Behind the Curve: Schrems II and the Need for Increased U.S. Data Protections in a Global Economy

Micah Carlson

I. INTRODUCTION 198
II. BACKGROUND 199
A. Data as a Commodity 199
B. The Emergence and Evolution of Data Protections 200
C. The European/American Relationship 202
D. Schrems II and the Aftermath 204
III. ANALYSIS 204
A. Potential Solutions 204
B. A Privacy Shield Replacement 205
C. Standard Contractual Clauses 206
D. Derogations, Including Data Subject Consent and the Fulfillment of Contracts 208
E. Data Localization 209
F. GDPR-Esque Protections in the U.S. 210
IV. RECOMMENDATION 212
A. The Passage of Federal Legislation That Would Satisfy the EU's Adequacy Requirements is Exceedingly Unlikely 212
B. FISA Section 702 and EO12333 Must be Addressed 213
C. FISA Section 702 and EO12333 Would Still Retain their Effectiveness 117
D. Giving the Exemptions Legally Binding Force 213
V. CONCLUSION 214

I. INTRODUCTION

The United States (U.S.) and the European Union (EU) have long enjoyed a prosperous and peaceful relationship that has mutually benefitted both parties. With their shared Western values, their economic influence, and their cultural relevance, the American/European relationship has only rarely been tested throughout the 20th and 21st Centuries. Despite this, there is one area of the law where the two jurisdictions seem incapable of seeing eye-to-eye: data protections.

While the EU has served as the global leader in the realm of data protections, the U.S. has regrettably lagged behind.[1] While the EU has passed directives and legislation aimed at providing their citizens with strict data and privacy protections, the U.S. has failed to do so.[2] In order to facilitate legal data transfers between the two jurisdictions, the EU and the U.S. have been compelled to establish agreements where U.S.-based businesses can choose to adhere to European data law.[3] Through these legal mechanisms, U.S. businesses have been granted a legal avenue to import European data.[4] In an increasingly data-centric global economy, the ability to transfer data between two of the world's largest economic powerhouses is of the utmost importance.

In July of 2020, the EU's highest court struck down the legal mechanism that allowed data transfers between the EU and the U.S.[5] The court's reasoning was based on the U.S.'s ongoing surveillance programs; although U.S. businesses could bind themselves to adhere to European law, there existed no guarantee that U.S. intelligence would not collect, store, or handle European citizens' data.[6] Consequently, the framework was struck down as illegal under EU law.[7]

It is imperative that data transfers between the U.S. and the EU are granted a legal mechanism to resume. Today, the U.S. and the EU are negotiating a legal framework for data transfers to succeed the invalidated legal framework.[8] Despite this, any replacement will inevitably be short-lived if the new deal does not address the primary concerns of the European courts. To ensure the longevity of the EU-U.S. alliance and the economic future of the two jurisdictions, the new legal framework must address U.S. surveillance programs. Most notably, the participants of the new legal framework must be exempted from surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA Section 702) and President Reagan's Executive Order 12333 (EO12333), two legal bases

1. *See infra* Parts II.C, II.D (discussing the development of European and American data protections).
2. *Id.*
3. *E.g.*, Press Release, European Comm'n, Press Release, EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield (Feb. 2, 2016), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216 [https://perma.cc/255C-G3BG] [hereinafter *Transatlantic Data Flow Framework*] (announcing the second EU-U.S. framework for data transfers to the U.S.).
4. *Id.*
5. Data Prot. Comm'r v. Facebook Ir. Ltd. [2019] IESC 46 (H. Ct.) (Ir.).
6. *Id.*
7. *Id.*
8. Press Release, U.S. Dep't Com., Joint Press Statement from U.S. Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders (Aug. 10, 2020), https://www.commerce.gov/news/press-releases/2020/08/joint-press-statement-us-secretary-commerce-wilbur-ross-and-european [https://perma.cc/4H75-ERMS][hereinafter *Joint U.S./EU Press Release*].

for widespread U.S. surveillance that have been highlighted as especially problematic by EU courts.[9] To best achieve this, Congress should amend FISA Section 702 to exempt business participants of the new framework, and President Biden or Congress should amend or eliminate EO12333.

II. BACKGROUND

A. Data as a Commodity

Through the rapid globalization and technological advancements of the 20th Century, data has been established as a recognized commodity.[10] But why do companies desire consumer data? Why would a business allocate part of its resources to collecting and processing seemingly worthless masses of consumer information? Simply put, consumer data is not worthless; indeed, it has been estimated that the global market for data will be $229.4 billion in 2025.[11] Companies are willing to pay money for data because, among other benefits, consumer data can be invaluable when forming a marketing strategy.[12]

While collecting names, addresses, phone numbers, and email addresses has its obvious utility, data collection has become far more sophisticated and far-reaching.[13] Data collection now includes categories such as purchase patterns, gender, location, electronic devices used, driving history, and many more.[14] This sophistication has led to staggeringly accurate and effective marketing efforts. For example, in an unprecedented marketing objective, Target Corporation used data analytics professionals to develop a "pregnancy prediction score" for its customers.[15] This score purported to estimate the likelihood that a female shopper was pregnant, even predicting how far along the pregnancy was.[16] By catering their marketing strategies to such an individual, Target hoped to capture pregnant women as loyal pre-birth and post-birth customers.[17]

To acquire consumer data, companies like Target often purchase consumer data through so-called data brokers, entities that specialize in the realm of collecting and selling consumer data.[18] Data brokers' influence has become more far-reaching in recent years, as they have adapted from collecting data on a case-by-case basis to instead

---

9. Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–11, 1821–29, 1841–46, 1861–62, 1871; Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981).

10. *See generally* Alberto De Franceschi & Michael Lehmann, *Data as Tradeable Commodity and New Measures for Their Protection*, 1 ITALIAN L.J. (2015) (detailing the emergence of data as a commodity).

11. Press Release, MarketsandMarkets, Big Data Market Worth $229.4 Billion by 2025 (Mar. 13, 2020), https://www.marketsandmarkets.com/PressReleases/big-data.asp [https://perma.cc/3T3V-GNLJ].

12. *See generally* Charles Duhigg, How Companies Learn Your Secrets, N.Y. TIMES MAG., (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/97PU-9DVV] (detailing how companies retrieve consumer data and its marketing uses).

13. *See generally* Michael J. Becker, *The Consumer Data Revolution: The Reshaping of Industry Competition and a New Perspective on Privacy*, 15 J. DIRECT DATA & DIGIT. MKTG. PRAC. 213 (2014) (detailing the rapid expansion of data collection practices).

14. *Id.* at 215.

15. Duhigg, *supra* note 12.

16. *Id.*

17. *Id.*

18. Logan Danielle Wayne, *The Data-Broker Threat: Proposing Federal Legislation to Protect Post-Expungement Privacy*, 102 J. CRIM. L. & CRIMINOLOGY 253, 253 (2012).

collecting large pools of consumer data on many data subjects en masse.[19] Additionally, the market has experienced pressure to produce immediate results.[20] For example, suppose a company wishes to conduct a background check to determine whether a job candidate is fit to fill a newly vacant, essential position within the company. In this case, the company will likely demand the background check be completed as soon as possible. This desire for immediate results has led data brokers to continue growing their databases, rarely deleting any information previously collected.[21]

This mass collection of data has presented emerging risks to consumers. With more entities gathering greater masses of data from an ever-expanding list of data categories, the potential for data leaks, improper usage of consumer data, data breaches, and perpetual retention of consumer information has only increased. In an increasingly digital world where more data is collected, the number of contact points with such data has increased in tandem. Each employee with access to consumer data, each email containing consumer data, each server storing consumer data, and every single other contact point that interacts with consumer data is a potential point of failure in the chain that could ultimately harm consumers. A disgruntled employee could purposefully leak data, an email may be sent to the wrong person, or hackers could tap into a server. Throughout our digital revolution, the risks presented to consumers have increased exponentially, though American consumers' control over such risks has remained mostly stagnant.[22] Consequently, the potential for abuse and privacy violations has, understandably, lead many to conclude that data protections and increased regulations are needed.[23]

B. The Emergence and Evolution of Data Protections

With data collection growing in popularity while also possessing potential for abuse, some governments have sought to regulate the data market and recognize data subjects' rights to their data.[24] For example, the Canadian government passed the Personal Information Protection and Electronic Documents Act (PIPEDA) in 2000, which provides federal protections for Canadian residents' data when their province or territory does not provide substantially similar protections.[25]

On the other side of the Atlantic, the EU adopted the Data Protection Directive in 1995, which instructed EU states to provide data protections to their residents.[26] Most

19. *Id.* at 263.

20. *Id.*

21. *Id.*

22. *See infra* Parts II.B, IV.A (discussing the development of American data protections at the federal and state levels).

23. *See generally* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling 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/7QTN-PAR6] (discussing how Americans feel about data collection and protection in the U.S.).

24. Council Regulation 2016/679, 2016 O.J. (L 119) 1; *see also* Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.) (detailing Canada's primary data privacy law).

25. *PIPEDA in Brief*, OFF. PRIV. COMM'R CANADA, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ [https://perma.cc/259E-PJBQ].

26. Council Directive 95/46/EC, 1995 O.J. (L 281) 31; *see also* David Banisar & Simon Davies, *Global*

importantly, the Data Protection Directive directed EU states to only allow the export of European personal data to other jurisdictions when they knew the data would be protected by law.[27]

In 2016, the EU adopted the General Data Protection Regulation (GDPR) which sought to further enshrine protections for European residents' personal data, ultimately replacing the Data Protection Directive.[28] Most critically, this law defines "personal data" quite broadly:

> Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[29]

Any information that falls under this broad definition is subject to GDPR protections. Consequently, any "controller" or "processor" of such data must implement "appropriate technical and organi[z]ational measures."[30] These requirements apply to any entity wishing to control or process EU residents' personal information, regardless of their location.[31] This means that GDPR applies to foreign entities that process EU nationals' data.[32] Furthermore, the GDPR stipulates that personal data is not to be processed unless it is legitimized by one of six possible justifications: consent, contract, public task, vital interest, legitimate interest, or legal requirement.[33] If the justification is based on consent, the resident in question retains his or her right to revoke consent at any time.[34] Additionally, other requirements under GDPR include the appointment of a data officer and making proper public disclosures regarding data collection practices.[35]

The American approach to data privacy has been markedly different. Currently, the U.S. does not have a central federal privacy law.[36] Instead, the U.S. has elected to regulate data collection in specific, sensitive instances and markets.[37] Most notably, the

---

Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments, 18 J. MARSHALL J. COMPUT. & INFO. L. 1, 3–4 (1999) (analyzing how privacy rights are viewed and protected around the world).

27. *Id.*

28. Council Regulation 2016/679, 2016 O.J. (L 119) 1.

29. *Id.* at 33.

30. *Id.* at 36.

31. *See id.* at 101 (detailing Member States' obligations to ensure international transfers protect EU residents' data).

32. *Id.*

33. Council Regulation 2016/679, 2016 O.J. (L 119) 36.

34. *Id.* at 37.

35. *Id.* at 52, 55.

36. *See generally* Derek Hawkins, *The Cybersecurity 202: Why a Privacy Law Like GDPR Would be a Tough Sell in the U.S.*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/ [https://perma.cc/D7JL-TKU8] (discussing why a law GDPR or an equivalent would not be possible in the U.S.).

37. *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (detailing the regulation of websites that target or knowingly collect info from children 13 and under); Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (detailing the protection of private health related data

Health Insurance Portability and Accountability Act (HIPAA) prevents protected health information (PHI) from certain disclosures.[38] PHI is merely limited to "individually identifiable health information," meaning the information must be health information and capable of being used to identify the individual in question. Additionally, only "covered entities" and business associates of such covered entities are subject to HIPAA's regulations; covered entities only include health care providers, health plans, and health care clearinghouses.[39] Consequently, the scope of HIPAA is much more limited than GDPR.

The U.S. does have other federal data protection laws, though they are also limited in scope. These include the Privacy Act[40] (placing restrictions on the use of government-held data), the Gramm-Leach-Bliley Act[41] (protecting nonpublic financial information), and the Children's Online Privacy Protection Act[42] (granting protections to the personal information of those under 12 years of age). Regardless, even when considered as a whole, these laws do not rival the general applicability of GDPR.

C. The European/American Relationship

In the late 1990s and early 2000s, the EU and the U.S., despite being close allies and trade partners, were worlds apart in the realm of data protections.[43] The U.S. had yet to pass a comprehensive data protection law, while EU entities were barred from transferring data to jurisdictions with inadequate data protections.[44] To maintain trade relations and support both jurisdictions' economies, the EU and the U.S. needed to reach an agreement.

Such an agreement was reached under the EU–U.S. Safe Harbor Principles.[45] Under Safe Harbor, U.S. entities could choose to self-certify, where they would commit to incorporating policies that further the seven principles of Safe Harbor: notice, choice, onward transfer, security, data integrity, access, and enforcement.[46] To further these objectives, Safe Harbor entities were expected to provide notices about their collection practices, offer the opportunity to opt-out of information being disclosed to third parties or used for unexpected purposes, ensure that any third parties provide adequate data

---

held by health institutions); Gramm–Leach–Bliley Act, 15 U.S.C. §§ 6801–6809, 6821–6827 (codified in scattered sections of 12 and 15 U.S.C.) (detailing the regulation of private consumer financial information); 5 U.S.C. § 552A (1974) (detailing the handling of personal identifiable information by federal agencies).

38. Health Insurance Portability and Accountability Act, Pub. L. No. 104–191, 110 Stat. 1936 (1996).

39. *Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH AND HUM. SERV., https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [https://perma.cc/6VE3-ASC2].

40. 5 U.S.C. § 552A (1974).

41. Gramm–Leach–Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.).

42. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506.

43. *See supra* Part II.B (detailing the different approaches that the EU and the U.S. have taken in the realm of data security).

44. *Id.*

45. *U.S.-EU Safe Harbor Framework*, FED. TRADE COMM'N (July 25, 2016), https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework [https://perma.cc/U4Y3-UMQY].

46. *Information For EU Residents Regarding The U.S.-EU Safe Harbor Program*, FED. TRADE COMM'N (July 5, 2016), https://www.ftc.gov/tips-advice/business-center/guidance/information-eu-residents-regarding-us-eu-safe-harbor-program [https://perma.cc/4Y7Q-K3JW].

protections, take reasonable precautions to protect held data, use data only for its intended purposes, ensure the accuracy of held data, provide access to information to the relevant data subjects, and establish complaint and enforcement mechanisms.[47] Safe Harbor was largely dependent upon self-regulation for enforcement and maintained compliance.[48]

Safe Harbor remained relatively undisturbed until 2013. In 2013, Edward Snowden granted the world a peek at the domestic and international spying program clandestinely maintained by the U.S. government.[49] In the wake of the revelations, Max Schrems, an Austria-born attorney, began to question how the U.S. could be considered to provide "adequate" (as defined under EU law) data protections.[50] Schrems brought suit against Facebook Ireland Ltd. to attempt to bar them from transferring data to the U.S., asserting that such transfers violated European data protections.[51] Eventually, the Court of Justice of the European Union (CJEU) reviewed the case in 2015.[52] On October 6, 2015, the CJEU ruled Safe Harbor invalid; the ruling was primarily based on the conclusions that Safe Harbor did little to block U.S. government interference with the provided protections and Safe Harbor did not provide a remedy mechanism for individuals seeking access to their data.[53] This decision has since come to be known as *Schrems I*.[54]

Following *Schrems I*, the EU and the U.S. began work on a replacement.[55] By February 2, 2016, the European Commission and the U.S. had come to a preliminary agreement, which would be labeled as the EU-U.S. Privacy Shield.[56] Under Privacy Shield, U.S. entities could choose to self-certify, where they would bind themselves to comply with data protection standards that rise to the same level as EU protections.[57] The framework was immediately subject to scrutiny, notably from Max Schrems himself.[58] In a 2016 piece, Schrems predicted that the U.S. government's continued mass surveillance (which was even acknowledged by the European Commission) would inevitably lead to a similar ruling to *Schrems I*, with the new framework being struck down.[59]

---

47. U.S. Dep't of Com., *Safe Harbor Privacy Principles*, EXPORT.GOV (Jan. 30, 2000, 3:03 PM), https://2016.export.gov/safeharbor/eu/eg_main_018475.asp [https://perma.cc/35ZK-LRWP].

48. *Id.*

49. Barton Gellman et al., *Edward Snowden Comes Forward as Source of NSA Leaks*, WASH. POST (June 9, 2013), https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html [https://perma.cc/DEC7-ZWAG].

50. Tim Walker, *Max Schrems: The Austrian Law Graduate who Became a Champion of Facebook Users*, INDEPENDENT (Oct. 6, 2015), https://www.independent.co.uk/life-style/gadgets-and-tech/news/max-schrems-austrian-law-graduate-who-became-champion-facebook-users-a6683711.html [https://perma.cc/X524-MKY6].

51. *See generally* Case C-362/14, Schrems v. Data Prot. Comm'r, (*Schrems I*), ECLI:EU:C:2015:650 (Oct. 6, 2015).

52. *Id.*

53. *Id.*

54. Max Schrems, *The Privacy Shield is a Soft Update of the Safe Harbor*, 2 EUR. DATA PROT. L. REV. 148, 148 (2016).

55. *Transatlantic Data Flow Framework*, *supra* note 3.

56. *Id.*

57. *Id.*

58. Schrems, *supra* note 54.

59. *Id.*

D. Schrems II and the Aftermath

Ultimately, Schrems' prediction proved true. On July 16, 2020, the CJEU struck down Privacy Shield as invalid, in what has come to be known as the *Schrems II* decision.[60] In *Schrems II*, the court found that because a U.S.-based entity is always potentially subject to U.S. surveillance (specifically under provisions like Section 702 of FISA) and because EU residents are not always granted a method of redress for violations of their EU-guaranteed privacy rights within the U.S., the Privacy Shield framework violated EU law.[61] In other words, while U.S. entities can guarantee that they will hold themselves to "adequate" data protection standards, they cannot affirm the same for the U.S. government. Additionally, the U.S. government is mostly unaccountable in its handling of foreigners' information.[62] While the CJEU concedes that there are some instances in which a foreigner could seek redress for mishandled information, they are not exhaustive and do not cover every method that the U.S. government uses in its surveillance efforts.[63]

It should be noted, however, that the U.S. government was not violating any law by surveilling Safe Harbor and Privacy Shield entities; the U.S. is a sovereign nation, and under relevant U.S. law, specifically FISA Section 702 and EO12333, the U.S. government is wholly empowered to collect information from entities under its jurisdiction.[64] Safe Harbor and Privacy Shield did not bind the U.S. government to adopt any specific data protections, but allowed private entities to bind themselves to adopt higher data protection standards. Safe Harbor and Privacy Shield were struck down not because the U.S. was violating any legal obligation, but because U.S. surveillance laws made it impossible for EU data exporters to fulfill their legal obligations under EU law when exporting data to the U.S.[65]

III. ANALYSIS

A. Potential Solutions

Under EU law, there are three mechanisms provided for legal international data transfers.[66] First, the European Commission may find that the destination state ensures an 'adequate level of protection' of the data transferred to it.[67] Second, the transfer can be conducted with 'appropriate safeguards', including the use of published Standard Contractual Clauses (SCCs).[68] Third, the transfer could be legitimized through certain derogations including consent of the data subject, even in the absence of adequate

60. *See generally* Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. (*Schrems II*), (2020) ECLI:EU:C:2020:559.

61. *Id.*

62. *See id.* (detailing Privacy Shield's Ombudsperson system for redress and its shortcomings in meeting the requirements of a "tribunal" for redress).

63. *Id.*

64. Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1811, 1821–1829, 1841–1846, 1861–1862, 1871; Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981).

65. Case C-311/18, *Shrems II* (2020) ECLI:EU:C:2020:559

66. *Id.*

67. Council Regulation 2016/679, 2016 O.J. (L 119) 45.

68. *Id.* at 46.

protections or appropriate safeguards.[69] In *Schrems II*, the CJEU found that the European Commission's determination that the U.S. provides adequate protections to EU data through Privacy Shield was erroneous.[70] Because the basis of this inadequacy is based on the U.S.'s mass collection of subjects' data and the lack of avenues for redress for mishandling of that data, there have been several proposed solutions to resume data transfers between the EU and the U.S.[71] Most notably, a Privacy Shield replacement, SCCs, certain derogations such as garnering subject consent or direct subject contracts, data localization, and a revamping of U.S. data protections serve as potential solutions.

B. A Privacy Shield Replacement

A logical solution to consider would be to establish a Privacy Shield replacement. After all, Privacy Shield was a replacement itself, taking the place of the Safe Harbor Principles.[72] Indeed, the U.S. and EU have made clear that they plan to pursue a new framework for data transfers between the two jurisdictions in the aftermath of the *Schrems II* decision.[73]

While a Privacy Shield replacement may allow for legal transfers between the jurisdictions for a time, any replacement that fails to shield its participants from U.S. surveillance is likely to suffer the same fate as Safe Harbor and Privacy Shield, just as Max Schrems predicted for Privacy Shield.[74] This inevitability is because the CJEU's elimination of Privacy Shield is not based on the Privacy Shield framework itself, but U.S. data protections in general.[75] Most notably, the court pointed to FISA Section 702 and EO12333 as being especially problematic, as they permit the U.S. government to acquire personal data en masse.[76]

Under FISA Section 702, the U.S. government can compel "U.S. electronic communication service providers" to hand over data that they possess on foreign individuals.[77] In practice, "electronic communication service provider" is defined very broadly.[78] Additionally, under EO12333, "[i]nformation obtained in the course of lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation" is permitted to be collected, retained, and disseminated.[79] These two rules

69. *Id.* at 49.

70. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. (*Schrems II*), ¶ 73 (2020) ECLI:EU:C:2020:559.

71. *Id.*; *see also* Joshua P. Meltzer, *The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security*, VOXEU (Aug. 5, 2020), https://voxeu.org/article/impact-gdpr-data-flows-and-national-security [https://perma.cc/VNZ2-CM4G] (detailing the inadequacy of U.S. data protections and the consequences of that inadequacy).

72. *Transatlantic Data Flow Framework*, *supra* note 3.

73. *Joint U.S./EU Press Release*, *supra* note 8.

74. Schrems, *supra* note 54.

75. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. (*Schrems II*), ¶ 73 (2020) ECLI:EU:C:2020:559.

76. *Id.* at ¶ 354.

77. *Section 702 Overview*, DIR. NAT'L INTEL., https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf [https://perma.cc/TJT6-GVQP].

78. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114–15 (3d Cir. 2004) (finding that an entity's usage of an internal communication system was sufficient to label the entity as an electronic service provider).

79. Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (1981).

indicate an entire American framework that prioritizes the government's ability to collect information and protect against potential terrorist acts, as opposed to prioritizations of privacy.

Members of the U.S. intelligence community have asserted that such a prioritization of counterterrorism and surveillance is desirable.[80] In particular, the Office of the Director of National Intelligence (ODNI) has asserted that FISA Section 702 is "vital" to the security of the U.S.[81] Specifically, the ODNI asserts that FISA Section 702 is necessary for counterterrorism efforts, protecting U.S. military personnel, improving domestic cybersecurity, and preventing weapons proliferation abroad.[82] Despite this, the ODNI has been unable or unwilling to provide substantive examples of the successful usage of FISA Section 702 in these areas concerning national security.[83] In fact, evidence suggests that sweeping surveillance efforts are extremely ineffective at preventing terrorist attacks. In 2020, the 9th Circuit Court of Appeals found no evidence that the U.S.' widespread surveillance of American phone records led to any arrests of suspected terrorists.[84] Rather, some of the most infamous terrorist attacks that have occurred on American soil were successful not because of U.S. intelligence's lack of information, but because of a failure to properly share, analyze, and disseminate such information.[85] Regardless, as a matter of policy, the U.S. has decided to prioritize surveillance and information-gathering over privacy and data security.

Consequently, any ill-conceived replacement of Privacy Shield would be built on quicksand. As long as FISA Section 702 and EO12333 are operating in the background of American data law, the CJEU would likely take up a case challenging the hypothetical new framework and would strike it down as inadequate.[86]

C. Standard Contractual Clauses

One potential solution for the issues presented by the *Schrems II* decision is the usage and widespread adoption of SCCs. SCCs are standard contractual documents that have been pre-approved by the European Commission as methods to facilitate data

80. *Section 702 Overview*, *supra* note 77.

81. *Id.*

82. *Id.*

83. *See id.* (providing only one substantive example of a successful counterterrorism operation made possible by FISA Section 702: the killing of a high-ranking ISIS leader).

84. Aaron Holmes, *The NSA Phone-Spying Program Exposed by Edward Snowden Didn't Stop a Single Terrorist Attack, Federal Judge Finds*, BUS. INSIDER (Sept. 2, 2020, 7:23 PM), https://www.businessinsider.com/nsa-phone-snooping-illegal-court-finds-2020-9 [https://perma.cc/EG92-UB8F].

85. *See* Patrick G. Eddington, *No, Mass Surveillance Won't Stop Terrorist Attacks*, CATO INST. (Jan. 27, 2015), https://www.cato.org/commentary/no-mass-surveillance-wont-stop-terrorist-attacks [https://perma.cc/Y4RP-4V2D] (detailing both the 9/11 terrorist attacks and the Boston Marathon bombing as attacks where U.S. intelligence had all the information necessary to stop the attacks, but failures of sharing, analyzing, and disseminating the information allowed the attacks to happen).

86. *See* Schrems, *supra* note 54, at 148 (analyzing Privacy Shield's inadequacies and predicting its demise years before the CJEU struck it down); Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. (*Schrems II*), (2020) ECLI:EU:C:2020:559 (highlighting the particular issues with FISA Section 702 and EO12333).

transfers from the EU.[87] SCCs allow for data "controllers" and data "processors" to contract between themselves to ensure that the data being transferred will be adequately protected to the standard required under European law.[88] The alluring aspect of SCCs is that the language has already been approved and deemed to provide adequate protections by the European Commission when the parties adhere to the provided language.[89]

SCCs have become a popular proposed solution to the problem presented by *Schrems II*.[90] This is perhaps because the opinion of the Court explicitly allows for the continued use of SCCs as a method for granting "appropriate safeguards."[91] The Court states, "safeguards may be provided by standard data protection clauses drawn up by the Commission."[92] While at first blush, the Court's reluctance to eliminate SCCs grants some confidence that these clauses could serve as a permanent replacement for Privacy Shield, the Court quickly dashes such confidence. The Court makes clear that SCCs must be paired with a preliminary conclusion that the SCCs cannot be utilized when transferring to a jurisdiction in which they would be "impossible to honour."[93]

The Court implies that the U.S. is one such destination country that makes honoring the SCCs impossible.[94] Any European data exporters conducting a *bona fide* analysis of U.S. data law will inevitably come to the conclusion that they are incapable of honoring the SCCs and European data law when exporting data to the U.S; this is because many of the requirements that existed under Privacy Shield are similar to the requirements under the SCCs, and the CJEU has explicitly concluded that the Privacy Shield framework was wholly inadequate under EU law.[95] When paired with the court's implication that U.S. data laws make honoring SCCs impossible,[96] it becomes difficult to imagine any *bona fide* analysis that concludes with an assertion that data exporters can comply with both European data protections and American surveillance laws. By putting the ball in the data exporter's court, many exporters may be unwilling to play. Data exporters would risk being reprimanded under European law if they incorrectly concluded that it is possible for U.S.-based data importers to comply with the SCCs.

On June 4, 2021, the European Commission published new versions of the SCCs in response to the *Schrems II* ruling.[97] These updated SCCs notably require the contracting parties to perform a Schrems Privacy Impact Assessment, also known as a Transfer

87. *Standard Contractual Clauses (SCC)*, EUROPEAN COMM'N, (June 4, 2021), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en [https://perma.cc/PF2X-9N5X].

88. *Id*.

89. *See id.* (summarizing approvals in existence).

90. *See* Meltzer, *supra* note 71 (detailing the potential of SCCs in addressing the problems presented by *Schrems II*).

91. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. (*Schrems II*), ¶ 164 (2020) ECLI:EU:C:2020:559.

92. *Id.* at ¶ 128.

93. *Id.* at ¶ 137.

94. *See id* (implying that the U.S. makes it impossible for data controller to comply with standard clauses).

95. *Id*.

96. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. (*Schrems II*), (2020) ECLI:EU:C:2020:559.

97. *Standard Contractual Clauses (SCC)*, *supra* note 87.

Impact Assessment (TIA).[98] TIAs compel the data controller and processor to assess and document their conclusions as to whether the local laws of the destination country will compromise the protections afforded to the data through the SCCs and GDPR.[99] In reaching their conclusion, parties will likely be able to consider such factors as the data importer's history of receiving governmental requests for data, the consistency of enforcement of the relevant local data laws, and, in light of the data importer's industry, the probability that the data importer will receive a governmental request for the turnover of data.[100]

While the updated SCCs will compel parties to be more conscientious of their data transfers and the laws that affect them, the primary issues presented by *Schrems II* still remain. If the parties conclude that the laws of the destination country will compromise the security of the data being transferred, the parties must implement measures to adequately protect the data. If the parties are incapable of implementing such measures, the data transfer is not to occur.[101] Because parties will likely be incapable of concluding in good faith that U.S. law does not compromise the data being transferred, data exporters will be forced to choose between continuing their data exportation and risk punitive action or cease all data transfers to the U.S.

D. Derogations, Including Data Subject Consent and the Fulfillment of Contracts

Another of the three options for legal data transfers from the EU to other jurisdictions is a list of several derogations, with data subject consent and contract fulfillment being the most notable.[102] Beyond these two examples, Article 49 of GDPR provides for other derogations, including when the "transfer is necessary for important reasons of public interest."[103] While these other derogations are notable and have the potential to provide legal justification for data transfers in some scenarios, they are useful only in limited, niche situations. The applicability of these derogations is limited to the extent that data transfers between the EU and U.S. could not generally rely upon them; consequently, they will not garner analysis within this Note.

The derogation of consent seems to provide an adequate alternative to Privacy Shield, as Article 49(1)(a) of GDPR explicitly provides for data subject consent as a method for legal transfers of data, even in situations where the importing jurisdiction provides inadequate data protections.[104] Additionally, the CJEU made no indication in its *Schrems II* decision that consent should no longer be a legal justification for data transfers.[105] Consequently, one would be inclined to think that U.S. entities could rely on data subject consent in the wake of *Schrems II*. Despite this inclination, a closer

98. *Id.*

99. *Id.*

100. Tess Blair & Axel Spies, *New European Standard Contractual Clauses Are Not 'Set And Forget'*, MORGAN LEWIS (June 14, 2021), https://www.morganlewis.com/pubs/2021/06/new-european-standard-contractual-clauses-are-not-set-and-forget [https://perma.cc/QGW7-A4BF].

101. *Standard Contractual Clauses (SCC), supra* note 87.

102. Council Regulation 2016/679, 2016 O.J. (L 119) 49.

103. *Id.*

104. *Id.*

105. *See generally* Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. (*Schrems II*), (2020) ECLI:EU:C:2020:559.

examination reveals that there are some severe limitations surrounding the use of a data subject's consent when attempting to comply with European data law.

First, GDPR lays out specific requirements for consent regarding data transfers.[106] These requirements include that the consent is explicit and for the proposed transfer;[107] that the consent is provided after the data subject has "been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;"[108] and be "freely given, specific, informed and unambiguous."[109] As a result, the bare minimum requirements for consent are rather rigorous. For example, "freely given" can be a contentious phrase. In scenarios where one party has vastly more bargaining power than another, it may be determined that the consent was not freely given.[110] Another potential issue is the requirement that the data subject be informed of possible risks of the transfer. While many data subjects may simply glean over such warnings, some individuals may be (understandably) unwilling to provide consent after being informed that their transfer may result in U.S. surveillance collecting their personal data.

Beyond the textual requirements, consent as a means of sidestepping *Schrems II* comes with other serious drawbacks. For one, under the GDPR, consent may be withdrawn at any time.[111] While this undoubtedly benefits the data subject, it leaves the data controllers with little assurance of stability; the continued transfer of data from the EU to any recipient jurisdiction would be wholly reliant on the data subject's continued consent. Under business models that require a constant, uninterrupted stream of personal data, consent would prove an inadequate solution to *Schrems II*.

Alternatively, the necessity to fulfill a contract can be a legal basis for a data transfer.[112] Specifically, Article 49 of GDPR allows for data transfers when "the transfer is necessary for the performance of a contract between the data subject and the controller . . ."[113] However, under the European Data Protection Board's guidelines, this justification for data transfers should only be used occasionally and should not be relied on incessantly.[114] Thus, these derogations present roadblocks that are too numerous and too serious to use as a standard justification for data transfers from the EU.

E. Data Localization

Another proposed solution for *Schrems II* is data localization.[115] With data localization, European residents' data simply would not be exported to any country that

106. Council Regulation 2016/679, 2016 O.J. (L 119) 49.
107. *Id.*
108. *Id.*
109. *Id.* at art. 4.
110. Case C-453/99, Courage Ltd. v. Crehan and Inntrepreneur Pub. Co. v. Crehan, 2001 E.C.R. 1-06297.
111. Council Regulation 2016/679, 2016 O.J. (L 119) 7.
112. *Id.* at art. 49.
113. *Id.*
114. *Id.* (mandating that transfers justified by the necessity to fulfill a contract "take place only if the transfer is not repetitive, concerns only a limited number of data subjects . . .").
115. Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 J. INT'L ECON. L. 771, 771 (2020).

has not been deemed adequate.[116] This framework would effectively address the issue of legally justifying data exports, but the costs associated with such a strategy are steep.[117]

First, the strategy undermines the very goals of providing European data protections: increasing global trade and providing Europeans with more significant data security.[118] With a data localization strategy, the free flow of information is abruptly brought to a halt, and the global economy as a whole will suffer. Additionally, this economic harm would likely come at the cost of no additional security.[119] While the basis of the ruling in *Schrems II* is based on the U.S.'s surveillance operations, the U.S. is at its least restrained when surveilling foreign individuals.[120] The U.S. provides some limited data protections to its citizens but does not provide such niceties to foreign individuals; consequently, Europeans' data is at a higher risk of American surveillance when stored in Europe as opposed to the U.S.[121]

Second, data localization is patently expensive.[122] This is because an entity must completely localize all of its data operations.[123] If an entity had previously outsourced some of its data management processes, it would then be forced to find a way to conduct those processes in its home jurisdiction, which will likely be more expensive.[124] This is especially problematic for entities that do business in multiple jurisdictions but presently only store data in one central location; enforcement of data localization would force such entities to establish unique data centers in each of the jurisdictions in which they do business.[125]

F. GDPR-Esque Protections in the U.S.

A seemingly simple way to solve the problems of *Schrems II* would be for the U.S. to adopt data protections for its residents and regulate its domestic entities in the same vein as GDPR. This would, in theory, allow for the European Commission to determine that the U.S. is a jurisdiction that provides an adequate amount of protection to the data it houses. However, this is far easier said than done. The European Commission has found that only a few nations provide adequate protections, and the nations who have been granted such status are far further developed in their data protection law than the U.S.[126]

The U.S. is simply nowhere near the point to be considered a jurisdiction that provides adequate protection, and this is exceedingly unlikely to change anytime soon. Despite this, some states have taken it upon themselves to adopt data protections that far exceed the U.S.'s national standards. The California Consumer Protection Act (CCPA) is

116. *Id.* at 777.
117. *Id.* at 778–84.
118. *Id.*
119. *Id.*
120. Chander, *supra* note 115, at 778–84.
121. *Id. See supra* Part II.B (detailing some of the data protections that Americans are granted by the U.S. government).
122. Chander, *supra* note 115, at 778–84.
123. *Id.* at 782–84.
124. *Id.*
125. *Id.*
126. *Compare 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/HH8E-6YK9], *with* Hawkins, *supra* note 36.

a GDPR-esque California statute, but it is the exception, not the rule in the U.S.[127] Additionally, neither of the two biggest political parties in the U.S. have demonstrated that they will be prioritizing data protections for U.S. citizens anytime soon.

The Democratic Party published its platform for the 2020 election, and while the platform stated that the party is "committed to policies that will protect individuals' privacy and data rights," this statement is supported by little structure or form within the document.[128] In fact, the Democratic Party's commitment to data protections is seemingly undermined by the claims within the same document that the party "will ensure federal data collection and analysis is adequately funded and designed to allow for disaggregation by race, gender, sexual orientation, gender identity, geography, disability status, national origin, and other important variables . . .".[129] Depending upon the implementation of such a program, the data protection policies that Democrats claim to be prioritizing may be undermined, as it is unclear what security measures would be implemented to protect this newly collected, federally-held personal data. On the other hand, Republicans' 2020 platform failed to mention data protections at all.[130] Ultimately, this means that Americans are unlikely to be afforded any large-scale data protection legislation in the near future, let alone any substantive legislation that would be deemed to provide adequate protections under EU law.

While President Biden has issued limited executive orders that touched on data privacy issues by advancing actions such as protecting Americans' data from foreign governments and directing the Federal Trade Commission to adopt new regulations regarding data collection, these executive orders have not addressed the U.S. government's role in collecting data on Americans. One of these executive orders, designated an "Executive Order on Promoting Competition in the American Economy," is not even primarily focused on data privacy, and is instead mostly fixated on addressing perceived unfair and monopolistic business practices[131] These executive orders are illustrative of the fact that, thus far, the Biden administration has chosen to primarily focus on other issues besides data privacy, such as providing welfare and immigration reformation.[132] While data privacy may eventually become a core political issue in the U.S., it remains, at the U.S.'s continued peril, a largely ignored consideration.

---

127. Jedidiah Bracy, *With the CCPA now in Effect, Will Other States Follow?*, INT'L ASSOC. PRIV. PROS. (Jan. 2, 2020), https://iapp.org/news/a/with-the-ccpa-now-in-effect-will-other-states-follow/#:~:text=In%20addition%20to%20driving%20policy,pass%20more%20sectoral%20privacy%20laws [https://perma.cc/FD2W-6RV6].

128. DEMOCRATIC NAT'L COMM., 2020 DEMOCRATIC PARTY PLATFORM 25 (2020), https://democrats.org/wp-content/uploads/2020/08/2020-Democratic-Party-Platform.pdf [https://perma.cc/D9H6-G2YD].

129. *Id.* at 31.

130. *See generally* REPUBLICAN NAT'L COMM., RESOLUTION REGARDING THE REPUBLICAN PARTY PLATFORM (2020), https://prod-cdn-static.gop.com/docs/Resolution_Platform_2020.pdf [https://perma.cc/TBS3-8TRU] (lacking any mention of data privacy as a legislative priority).

131. *See* Exec. Order No. 14,036, 86 Fed. Reg. 36987 (July 14, 2021) (detailing the Biden administration's position that unfair business practices are stifling Americans' quality of life).

132. *The Biden-Harris Administration Immediate Priorities*, THE WHITE HOUSE, https://www.whitehouse.gov/priorities/ [https://perma.cc/7KG3-K267].

IV. RECOMMENDATION

With the European-American relationship in jeopardy, the relevant parties must reach a solution. While the EU and the U.S. have begun work on a potential Privacy Shield replacement, the details of such negotiations have not been made public.[133] Regardless, such a deal must include certain characteristics if it is to have any staying power. To achieve a robust trade framework that will survive scrutiny by European courts, the new framework must address the highlighted flaws in American data law: FISA Section 702 and EO12333.[134] If the new framework elects to simply ignore the problems with FISA Section 702 and EO12333 that the CJEU has emphasized in their *Schrems II* decision, the framework will likely be the target of litigation from the moment of its announcement. Consequently, this Note advocates for the adoption of a Privacy Shield framework that exempts the framework's participants from FISA Section 702 and EO12333.

A. The Passage of Federal Legislation That Would Satisfy the EU's Adequacy Requirements is Exceedingly Unlikely

First, it is important to recognize that the passage of a GDPR-esque piece of legislation in the U.S. remains nothing more than a pipedream. The passage of such legislation would be a herculean feat, as the U.S. simply has not prioritized such data protections.[135] Substantive change is possible, as CCPA's adoption in 2018 and subsequent state-level data protection laws have demonstrated that there is some political will to enact more strict data protections in the U.S.[136] Despite this, it must be reiterated that all substantive developments in this area of the law in the U.S. have been at the state level, not the federal level.[137]

As previously mentioned, there has been little movement from either political party on the national level to prioritize data protections.[138] This may be in part to the history of large-scale surveillance in the U.S., as FISA Section 702 and EO12333 are considered valuable tools by the U.S. intelligence community; there would likely be an unwillingness to part with them.[139] Thus, while the future may lead to a widespread domestic push for U.S. data protections, a solution to *Schrems II* cannot wait that long if the U.S.-EU trade relations are to thrive.

---

133. *Joint U.S./EU Press Release*, *supra* note 8.

134. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. (*Schrems II*), ¶¶ 56, 66 (2020) ECLI:EU:C:2020:559.

135. Hawkins, *supra* note 36.

136. Sarah Rippy, *US State Privacy Legislation Tracker*, INT'L ASS'N PRIV. PRO., https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/7A46-ZG65].

137. *See* Philip Bezanson et al., *The Battle of the Bills Begins: Proposed Federal Data Privacy Legislation Aims to End Patchwork Problem but Increases Enforcement*, NAT'L L. REV., Mar. 2021, at 2–3 (listing several federal data protection bills and acknowledging the poor chances of their passage).

138. DEMOCRATIC NAT'L COMM., *supra* note 128; REPUBLICAN NAT'L COMM., *supra* note 130.

139. *Supra* notes 80, 81, 82 and accompanying text.

B. FISA Section 702 and EO12333 Must be Addressed

Despite the potential for resistance among members of U.S. intelligence, it is important to acknowledge that FISA Section 702 and EO12333 must be addressed in Privacy Shield's successor, lest the new framework suffer the same fate as Privacy Shield. While comprehensive federal data privacy legislation remains unlikely to pass, a more narrowly tailored, surgical response to *Schrems II* would be more feasible.

Instead of fully adopting GDPR-esque legislation, the U.S. should take the small step of providing exemptions to FISA Section 702 and EO12333 to participants of Privacy Shield's replacement. This solution would serve as a practical middle-ground that would address the CJEU's primary complaints with U.S. data protections while also maintaining the effectiveness of FISA Section 702 and EO12333 as tools for the U.S. intelligence community.

C. FISA Section 702 and EO12333 Would Still Retain their Effectiveness

While there would perhaps be some concern within the intelligence community that exempting participants in an EU-U.S. data transfer framework would significantly handicap U.S. intelligence efforts, the data available does not suggest such a conclusion. At the time of its invalidation, Privacy Shield had just over 5,000 participating organizations.[140] While certainly nothing to scoff at, the program's enlistment pales when compared to the U.S. business sector as a whole. According to the U.S. Census Bureau, dozens of millions of businesses continue to operate within the U.S. every year.[141] Exempting a mere 5,000 from the list of intelligence sources would have a minor or negligible effect on the number of entities subject to U.S. surveillance. Many businesses would refrain from participating in a self-certification data transfer network in the same vein as Privacy Shield. These businesses could have various explanations for refraining from participating in a Privacy Shield replacement, but the most common reasoning would likely be that the business does not directly receive data from the EU. Thus, it is probable that U.S. surveillance would not lose their surveillance tools in their entirety.

D. Giving the Exemptions Legally Binding Force

Because FISA and EO12333 were acts of Congress and the President, respectively, a Privacy Shield replacement would have to legally exempt participants in a manner that complies with the hierarchy of U.S. law.[142] To exempt participants from FISA Section 702, the act would have to be amended by Congress. This would be no small task; Congress just amended and extended Section 702 in 2017, which will need to be reauthorized by 2023.[143] Consequently, amendments will likely be proposed once the

140. U.S. DEP'T COM., PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/list [https://perma.cc/FXB7-CQ6H].

141. U.S. CENSUS BUREAU, STATISTICS OF UNITED STATES BUSINESSES, https://www.census.gov/programs-surveys/susb.html [https://perma.cc/EP7G-GEQJ].

142. U.S. DEP'T JUST., The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801; Exec. Order No. 13740 (2008).

143. Press Release, The White House, Statement by the President on FISA Amendments Reauthorization Act of 2017 (Jan. 19, 2018), https://www.presidency.ucsb.edu/documents/statement-signing-the-fisa-amendments-reauthorization-act-2017 [https://perma.cc/6YUU-M5DM].

reauthorization deadline approaches, but nothing bars Congress from amending Section 702 now. If the political will can be mustered, Section 702 should be amended to exempt the participants of Privacy Shield's replacement as soon as a Privacy Shield replacement is unveiled.

Additionally, participants of Privacy Shield's replacement would require exemption from EO12333. There are several options to achieve this. First, Congress could choose to override EO12333 through a FISA amendment or any other piece of legislation passed into law. Alternatively, President Biden could choose to amend EO12333 to exempt the participants of the hypothetical program. It's possible that President Biden would be willing to issue such an amendment—he has taken some small, limited steps in the realm of American data privacy thus far.[144] In the short term, it would make little difference whether Congress or Biden was to revise or eliminate EO12333. An act of Congress would be preferred in the long-term as legislative acts are relatively more resilient when compared to Executive Orders.[145]

V. CONCLUSION

Despite enjoying decades of economic prosperity facilitated in part by a strong trade alliance, the U.S. and EU do not have any legal data transfer mechanism at present. This lack of cohesiveness will not exist indefinitely, as a replacement mechanism is forthcoming. However, it has yet to be seen whether this replacement will have the legs to survive the scrutiny of EU courts or if it will merely be a feeble attempt to kick the can down the road, leaving the trade relationship of the two jurisdictions in doubt once again.

To ensure the longevity of such a framework, the replacement must, at a minimum, address the U.S.'s widespread surveillance practices, with the most notable facilitators of such practices being FISA Section 702 and EO12333. Since the U.S. has demonstrated extreme reluctance in sacrificing its surveillance capabilities, anticipating a large overhaul of U.S. data protections that grants widespread privacy rights to U.S. residents, regulates U.S. entities, and restrains U.S. intelligence is unrealistic at best. Instead, a small step towards increased data protections may be enough to survive scrutiny within EU courts while simultaneously allowing U.S. intelligence to largely retain its surveillance tools.

By amending FISA Section 702 to exempt participants of Privacy Shield's replacement, Congress would provide those entities and the European data that they handle protection from U.S. surveillance. At the same time, because FISA Section 702 applies so broadly, there are so many total U.S. businesses, and there would be limited participants in Privacy Shield's replacement, U.S. surveillance would not be seriously crippled.

Most importantly, Congress should pass legislation to counter or eliminate EO12333. This would remove the other primary legal justification for surveilling participants in Privacy Shield's replacement. Alternatively, President Biden may amend

144. *See supra* note 131 and accompanying text.

145. *See* Eric Bradner et al., *Biden Targets Trump's Legacy with First-day Executive Actions*, CNN (Jan. 20, 2021, 8:48 PM), https://www.cnn.com/2021/01/20/politics/executive-actions-biden/index.html [https://perma.c c/F4DV-U69D] (outlining President Biden's multiple Inauguration Day executive actions which undid multiple Trump administration executive orders).

or eliminate EO12333. With these small, surgical changes to the new framework, the American/European trade relationship will be allowed to operate at its maximum potential for decades to come.