Vanderbilt Journal of Transnational Law

Volume 50
Issue 5 *November 2017*

Article 6

2017

# A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement

Emily Linn

# A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement


## ABSTRACT

*The trade relationship between the European Union and the United States, the largest cross-border data flow in the world, is in a state of uncertainty. Operating under different notions of what privacy should look like and divergent legal protections for personal data, the European Union and United States have struggled to reach a mutually acceptable agreement in the past. This Note analyzes their latest attempt, the EU-U.S. Privacy Shield, with specific emphasis on (1) the way it has improved upon its predecessor, the EU-U.S. Safe Harbor; (2) the weaknesses that still remain; and (3) the external factors that threaten the future success of the agreement. Without attempting to predict a specific outcome, this Note surveys the potential challenges to the Privacy Shield in the coming years and considers potential alternative frameworks. This Note proposes that the agreement should be restructured into a private-public EU-U.S. business arrangement, in which a Data Privacy NGO takes over the duties of the US government. By relying on corporate self-regulation, the Privacy Shield can preserve its basic framework and Privacy Principles, while minimizing the vulnerabilities that make the agreement susceptible to invalidation.*


## TABLE OF CONTENTS

## I. INTRODUCTION

Personal data is a currency of the modern age and a valuable commodity in an increasingly electronic world. However, unlike traditional forms of currency, personal data inherently relies on private information about real people, occupying a sacred space that

warrants heightened protection. The dominant exchange of this ubiquitous personal data currency occurs between EU member states and the United States. Despite this, the United States and the European Union historically have fallen short in reaching a consensus about the permissible process by which EU personal data can be transferred to the United States.[1]

On October 6, 2015, the Court of Justice of the European Union (CJEU) issued a decision invalidating Safe Harbor, the previous EU-U.S. privacy agreement that permitted data transfer between the European Union and the United States. In invalidating the agreement, CJEU explained that Safe Harbor was not compliant with the Data Protection Directive and US enforcement of the agreement prioritized US concerns over the Safe Harbor Principles.[2] Less than a year later, the European Commission (EC) approved a new data sharing agreement, the EU-U.S. Privacy Shield (Privacy Shield), which went into effect on August 1, 2016.[3] While the Privacy Shield is an improvement on the protection afforded to EU citizens and their personal data, the framework of the new agreement is not immune to challenge by the European Union and faces an uncertain future.

This Note investigates the range of possible outcomes that could result from the Privacy Shield. Part II examines the differing notions of privacy within the European Union and the United States, and analyzes the EU Data Protection Directive's impact on US collection, usage, and onward transfer of EU personal data. Part III outlines the predecessor agreement, EU-U.S. Safe Harbor, and discusses the rationale for its invalidation. Part IV introduces the new agreement, the EU-U.S. Privacy Shield, outlining its structure, identifying the improvements within the new framework, and recognizing the weaknesses that threaten its long-term success. Part V considers the potential challenges for the Privacy Shield in the upcoming years: joint annual review and review by the European Court of Justice. Next, it offers a synopsis of the alternative mechanisms for compliance if the Privacy Shield framework is invalidated. Part V concludes by recommending restructuring the Privacy Shield as a public-private arrangement, replacing the role of the US government with a Data Privacy non-governmental organization (NGO) to exploit the

---

1. *See* Case C-362/14, Schrems v. Data Protection Comm'r, 2015 E.C.R. § 106 (serving as the latest failure to reach a data sharing agreement that satisfies the EU Data Protection Directive's requirements).

2. *See id.* (holding that the Safe Harbor did not meet the Article 25 requirement for "an adequate level of protection" required to safeguard EU data subjects' fundamental right).

3. Press Release, European Commission, European Commission Launches EU-U.S. Privacy Shield (July 12, 2016), http://europa.eu/rapid/press-release_IP-16-2461_en.htm [https://perma.cc/DA6V-T5DK] (archived Sept. 21, 2017).

improvements in the Privacy Shield, while minimizing the risk of invalidation.

## II. BACKGROUND

This Note only concerns the transfer of EU personal data to the United States for collection, usage, or onward transfer. Examples of these transactions include the inter-workings of one company with branches in both the United States and the European Union, travel corporations or online retailers who require personal information to finalize transactions, online educational institutions that seek personal statistics, social media platforms, and human resource companies, to name a few.[4] While there is no universal definition of personal data, the European Union has defined it as any information that makes it possible to identify a person, including: names, phone numbers, birthdates, both home and email addresses, credit card numbers, national insurance numbers, IP addresses, employee information including number, login information, gender, and marital status, and biometric and genetic data.[5] Personal data includes aggregate data, which involves the aggregation of information from servers and personal online profiles in order to tailor online ads to the specific preferences of a targeted user.[6]

If the Privacy Shield fails, the consequences will be severe, impacting not only the EU member states' and the United States' economy, but global trade as well. The European Parliament recognized the importance of the EU-U.S. trade relationship, noting that cross-border data flows between the European Union and the United States are the highest in the world—50 percent higher than any other transfer—and acknowledging personal data as an essential component.[7] The Department of Commerce (DOC) noted that EU-U.S.

---

4. EUROPEAN COMM'N, GUIDE TO THE EU-U.S. PRIVACY SHIELD 7 (2016), http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf [https://perma.cc/N2NC-KXWR] (archived Sept. 21, 2017).

5. *Id.*; Svetlana Yakovleva, Researcher, Inst. for Info. Law at the Univ. of Amsterdam, Speech at Vanderbilt Law School: The Protection of Personal Data in International Transactions (Sept. 22, 2016) (noting that there is no uniform definition, which makes it harder to negotiate between EU-US, citing as an example the fact that IP address fall under the EU's definition of personal data but would not be considered so in the US).

6. Lior Abraham et al., *Scuba Diving in Data at Facebook*, FACEBOOK INC., http://db.disi.unitn.eu/pages/VLDBProgram/pdf/industry/p767-wiener.pdf [https://perma.cc/J85W-X6KJ] (archived Sept. 21, 2017); Thorin Klosowski, *How Facebook Uses Your Data to Target Ads, Even Offline*, LIFEHACKER.COM (Apr. 11, 2013), http://lifehacker.com/5994380/how-facebook-uses-your-data-to-target-ads-even-offline [https://perma.cc/Z3C3-C5G6] (archived Sept. 21, 2017).

7. European Parliament Resolution on Transatlantic Data Flows, 2016/2727 (RSP) (May 26, 2016) [hereinafter Resolution 2016/2727].

transatlantic trading is the largest trading relationship in the world, estimated to produce half a trillion dollars of commerce annually, representing half of all US investments abroad, and employing 3.5 million Americans.[8] Clearly, there is a lot at stake both for consumers and corporate entities in the United States and the European Union.[9]

The United States and the European Union not only have different notions of what personal data includes, but also operate under two very different definitions of privacy more generally, which impact their respective laws and public policies.[10] As a result, the European Union and the United States have opposing views of what data protection specifically looks like and how it should be implemented.[11] Despite these differences, the European Union and the United States have recognized the profound need for cooperation and consensus.

### A. *Differing Notions of Privacy in the United States and the European Union*

The historical notion of privacy in the United States differs from that of the European Union. To start, the word "privacy" is absent from the US Constitution.[12] American jurisprudence has recognized that a

---

8. Letter from Kenneth E. Hyatt, Deputy Under Sec. for Int'l Trade, U.S. Dep't of Commerce Int'l Trade Admin., to Věra Jourová, Comm'r for Justice, Consumers and Gender Equality, The Eur. Comm'n, (July 7, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0M [https://perma.cc/J2DF-28ZK] (archived Sept. 22, 2017); INFO. TECH. INDUS. COUNCIL, THE EU-US PRIVACY SHIELD: WHAT'S AT STAKE 1 (2016), http://www.itic.org/dotAsset/9/b/9b4cb3ad-6d8b-469d-bd03-b2e52d7a0ecd.pdf [https://perma.cc/2WYY-8Q4Y] (archived on Sept. 22, 2017).

9. INFO. TECH. INDUS. COUNCIL, *supra* note 8.

10. *See generally* Barbara Crutfield George et al., *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L. J. 735, 741–749 (2001) (detailing the conflicting definitions of privacy in the U.S. and EU).

11. *See generally id.* (detailing the conflicting cultural, legal, and political attitudes between the U.S. and EU countries concerning what is private and how privacy should be maintained).

12. The Supreme Court, in Griswold v. Connecticut, 381 U.S. 479 (1965), recognized that while a right to privacy could be found in the "penumbras, formed by emanations from those guarantees" in the First, Third, Fourth, Fifth, and Ninth Amendments, a right to privacy is not expressly mentioned in the text. The First Amendment right of association creates the right to freely meet and to have privacy in associations. The Third Amendment prohibition against the quartering of soldiers in the home creates a zone of privacy in the home. The Fourth Amendment right of people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, creates the right to privacy in the home and "privacies of life." The Fifth Amendment Self-Incrimination clause "enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment." The Ninth Amendment states "enumeration in Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people," suggesting that while a

right to privacy is implicit in the Fourth Amendment's prohibition against unreasonable search and seizure.[13] However, courts have historically limited this right to criminal matters, leaving lackluster constitutional protection for civil privacy rights.[14]

Beyond the Constitution, there is also a common law privacy tort in the United States: invasion of privacy.[15] However, the tort's protection is narrow in reach: once an individual publishes personal information, he or she waives the right to sue for the tort.[16] Statutory law in the United States has also failed to create a comprehensive set of privacy standards.[17] Instead, legislative enactment has taken a piecemeal approach, passing narrow laws that are scattered across specific target genres.[18] Often these pieces of legislation are reactive and narrow in scope, creating privacy rights in instances where highly publicized violations have engendered public concern.[19] Notably, the

---

right of privacy is not listed, it may exist. *See generally* U.S. CONST. amend. I, III, IV, V, IX; *see Griswold*, 381 U.S. at 484.

13. *See generally* U.S. CONST. amend. XIV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

14. Consider, for example, the broad power of court-enforced civil discovery with the Fourth Amendment's protections against unreasonable governmental searches and seizures.

15. *See generally* Olmstead v. United States, 277 U.S. 438, 483–485 (1928) (Brandeis, J., dissenting) (arguing that even if the governmental actor did not violate the petitioner's constitutional rights in wiretapping his telephone, the government can still be liable in tort for a common law invasion of privacy. *Olmstead's* substantive ruling was overturned in Katz v. United States, 389 U.S. 347 (1967), when the Court determined that wiretapping was a "search" for purposes of the Fourth Amendment and the defendant had a "reasonable expectation of privacy.").

16. Therefore, while U.S. law recognizes the potential for privacy concerns, the extent of this protection is limited to a very thin margin of cases that do not account for the personal data concerns addressed in this Note. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 216 (Dec. 15, 1890).

17. Chuan Sun, *The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective*, 2 NW. J. TECH. & INTELL. PROP. 99, 105 (2003).

18. *See id.; see also* Jasmine McNealy & Angelyn Flowers, *Privacy Law and Regulation: Technologies, Implications, and Solutions*, *in* PRIVACY IN A DIGITAL, NETWORKED WORLD 189, 194–196 (S. Zeadally & M. Badra eds., Springer International Publishing 2015) (examples of narrowly constructed laws include the Cable Communications Policy Act, requiring cable companies to protect the privacy of consumer records; the Video Privacy Protection Act, protecting the privacy of videotape rental information; the Telephone Consumer Protection Act, protecting consumers against telemarketers; the Health Insurance Portability and Accountability Act, upholding the privacy of medical records; and the Children's Online Privacy Protection Act, restricting internet providers' collection and use of personal information of children under age 13).

19. *See* McNealy & Flowers, *supra* note 18, at 195 (viewing anti-terrorism legislation like the USA Patriot Act which allowed for easier law enforcement acquisition of voicemails as a reaction to the terrorist attacks of September 11, 2001).

majority of legal privacy protections in the United States guard against government intrusion. When regulation of the private sector must occur, there is a strong presumption in favor of self-regulation as the "least intrusive and most efficient means," preferring soft laws that permit, but do not compel, private actors' participation.[20]

The European Union has a very different notion of privacy that is reflected in the protections afforded individuals. Rather than limiting privacy rights to instances of government intrusion, the European Union recognizes privacy and data protection as an express right that protects individuals from corporate data collection.[21] Privacy of one's personal data is a fundamental right that is guaranteed by the European Union Charter of Fundamental Rights.[22] This *sui generis* right, analogous to a constitutional right in the United States, is grounded in international human rights instruments.[23]

In addition to recognizing a right to privacy, the European Union also asserts that data protection is an essential mechanism for protecting EU citizens' fundamental rights.[24] The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines) were created by the Organization for Economic Co-Operation and Development (OECD), an intergovernmental organization with thirty-five participating members, including the European Union.[25] The OECD Guidelines provide suggestions on what should be taken into account when developing legislation on privacy and data protection and highlight principles to preserve individual rights while easing restrictions on the flow of information between nations.[26] The European Union's adoption of the OECD Guidelines, by

---

20. Sun, *supra* note 17, at 106.

21. McNealy & Flowers, *supra* note 18, at 203.

22. Charter of the Fundamental Rights of the European Union, art. 8, Dec. 18, 2000, 2000 O.J. (C 364) 10. ("1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.").

23. *See* Convention for the Protection of Human Rights and Fundamental Freedoms, arts. 8–11, Nov. 4, 1950, E.T.S. No. 005; *see also* Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108; Charter of the Fundamental Rights of the European Union, *supra* note 22, arts. 8, 12.

24. *See* McNealy & Flowers, *supra* note 18, at 198 (finding a right to privacy to be part of a body of rights considered to be both a human right and a fundamental freedom).

25. *See* Mike Ewing, *The Perfect Storm: The Safe Harbor and the Directive on Data Protection*, 24 HOUS. J. INT'L L. 315, 319–323 (2001).

26. *See* LEE A. BYGRAVE, DATA PRIVACY LAW 43 (Oxford Univ. Press 2014); Ewing, *supra* note 25, at 320–321 (listing the eight principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability).

virtue of its membership in the OECD, resulted in each EU member state largely enacting its own data protection rules from the OECD Guidelines, creating uncertainty and inconsistency in legislation throughout the European Union.[27] To remedy the confusion, EU member states voted to create a unified piece of legislation: The Data Protection Directive.

### B. *Standard for Transfer of EU Data: Data Protection Directive & General Data Protection Regulation*

Directive 95/46EC[28] of the European Parliament and of the Council of 24 October 1995, colloquially known as the Data Protection Directive (the Directive), aimed to harmonize data protection frameworks within the European Union by creating a more stable regulatory framework that required a uniform minimum standard of privacy protection across the European Union.[29] Specifically, the Directive sought to achieve two goals: 1) facilitating the free flow of personal data within the EU; and 2) ensuring an equally high level of protection within all countries in the EU for "the fundamental rights and freedoms of natural persons, and in particular their right to privacy."[30]

Of particular concern for this Note is Article 25 of the Directive, which specifies that personal data processed in the European Union can only be transferred to a party in a non-member state if the non-member state "ensures an *adequate* level of protection."[31] The EC assesses adequacy and reviews data protection legislation in the non-EU country and then makes a determination with the assistance of the Article 29 Data Protection Working Party's (WP29) non-binding opinion.[32] "The Directive does not define what creates an adequate

---

27. *See* Ewing, *supra* note 25, at 323 (noting that "disparities in national legislation could hamper the free flow of data across frontiers . . . caus[ing] serious disruptions in important sectors of the economy, such as banking and insurance. . . .") *see also id.* at 328–329 (highlighting EU member countries' calls for the "creation of a single, binding standard for all EU members.").

28. Directives are not immediately binding, but rather "harmonizing" instruments that require each member state to enact national legislation that reflects the principles inherent in the directive; the Data Protection Directive requires member states to enact common rules regarding information privacy. Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures,* 126 HARV. L. REV. 1966, 1971–72 (2013).

29. European Council Directive 95/46, art. 1, 1995 O.J. (L 281) 1, 2.

30. Schwartz, *supra* note 28, at 1972.

31. Council Directive 95/46, *supra* note 29, at art. 25.

32. *See* W. Gregory Voss, *The Future of Transatlantic Data Flows: Privacy Shield or Bust?*, 19 NO. 11 J. INTERNET L. 1, 8–9 (2016) (noting that the WP 29's opinion is "not binding, but may be persuasive"). The WP 29 "is an independent privacy advisory group made up of, inter alia, representatives of the EU Member States national data protection authorities." *Id.*

level of protection, but it indicates that all the circumstances surrounding the transfer, including the laws in force in the third country, must be considered by the supervising authority in making a determination about adequacy." [33]

Article 25 reflects the EC's intention that the "high level of protection within EU borders is not circumvented in cases where personal data originally collected or stored in a member state under the purview of the Directive is processed or transmitted outside the European Union."[34] In practice, this led many of the countries that interacted with the European Union to alter their domestic privacy laws to align with the Directive.[35]

Lacking an omnibus privacy protection regime, many US entities questioned the continuing legality of data transfers in light of Article 25's nebulous "adequacy" requirement.[36] The United States' sectoral approach to data protection, relying on a combination of legislation, regulation, and self-regulation, differed from the protections afforded by the Directive, and likely would have been deemed inadequate if a member state had requested an adequacy decision from the EC.[37] In practice, such a finding could impede transatlantic personal banking, brokerage transactions, hotel and airplane purchases, and credit card purchases involving EU citizens, as well as restrict multinational companies' ability to manage millions of employees with offices in the European Union.[38] To avoid a designation of inadequacy and the halting of data transfers from the European Union to the United States, the DOC initiated a two-year negotiation with the European Union, which resulted in the Safe Harbor Agreement.[39]

---

33. George et al., *supra* note 10, at 759.

34. Sun, *supra* note 17, at 104.

35. George et al., *supra* note 10, at 763–64; *see, e.g.* U.S. CHAMBER OF COMMERCE AND HUNTON & WILLIAMS, BUSINESS WITHOUT BORDERS: THE IMPORTANCE OF CROSS-BORDER DATA TRANSFERS TO GLOBAL PROSPERITY (2014), https://www.hunton.com/images/content/3/0/v2/3086/Business_without_Borders.pdf [https://perma.cc/R949-VJ2V] (archived Sept. 24, 2017) (citing countries outside the EU with laws that mimic the EU Directive, including Azerbaijan, Dubai International Financial Centre, Israel, Russia, South Africa, Argentina, Brazil, Columbia, Mexico, Peru, India, Malaysia, Singapore, Indonesia, Japan, South Korea).

36. Schwartz, *supra* note 28, at 1980 (noting that while the EU never formally ruled on the adequacy of U.S. data protection laws, "the EU consensus [wa]s that the United States lacks an adequate level of protection").

37. Voss, *supra* note 32, at 9 (noting that because this "sectoral approach" was viewed as inadequate, the U.S. and EU entered into the negotiations that would eventually result in the Safe Harbor Agreement).

38. George et al., *supra* note 10, at 738. *But see infra* Part V.C. (acknowledging that companies that used alternative compliance mechanisms such as BCRs, SCC, or consent could continue data transfer even if the EC ruled that U.S. data protections were inadequate).

39. McKay Cunningham, *Complying with International Data Protection Law*, 84 U. CIN. L. REV. 421, 441 (2016).

As a brief aside, on May 4, 2016, the EU Commission adopted EU Regulation 2016/679, known as the General Data Protection Regulation (GDPR), which replaces the Directive and goes into effect on May 25, 2018.[40] While this domestic change is significant for EU data protection requirements, for the purposes of this Note, the adequacy standard for non-member states under Article 25 is analogous to the new GDPR Article 45 requirement for permissible transfers, mandating "an adequate level of protection."[41]

## III. LEARNING FROM THE PAST

### A. *EU-U.S. Safe Harbor Agreement*

The Safe Harbor Agreement, effective November 1, 2000, allowed US organizations a voluntary mechanism by which to demonstrate the adequacy of their data protection under the Directive. Pursuant to the agreement, a company receiving personal data from the European Union must abide by the following Safe Harbor Privacy Principles:

---

40. *Id.* at 428–29 (noting that the new EU Data Protection Regulation "confirms the strictures of the Directive").

41. Commission Regulation 2016/679 of 4 May 2016 on The Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 61 ("A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, or territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection.").

notice,[42] choice,[43] onward transfer,[44] security,[45] data integrity,[46] access,[47] and enforcement.[48] These principles come from the Fair

---

42. Notice is defined as:

> An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

Commission Decision 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 Harbor Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215) 7.

43. Choice is defined as:

> An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party[] or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice. For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

*Id.*

44. Onward Transfer is defined as:

> To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote[], it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a

Information Practices developed by the Federal Trade Commission (FTC)[49] and track with many of the requirements found in the Directive.[50]

The FTC enforced this agreement, categorizing any violation of the Safe Harbor Privacy Principles as an unfair or deceptive practice pursuant to Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting

---

contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

*Id.* (internal endnote deleted).

45. Security is defined as:

> Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

*Id.*

46. Data Integrity is defined as:

> Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

*Id.*

47. Access is defined as:

> Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

*Id.*

48. Enforcement is defined as:

> Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

*Id.*

49. Sun, *supra* note 17, at 107.

50. Voss, *supra* note 32, at 9.

commerce."[51] Only US organizations within the jurisdiction of the FTC or the Department of Transportation (DOT) were eligible for self-certification under the Safe Harbor Agreement, thus excluding financial institutions from certifying under the Safe Harbor.[52]

To self-certify, an organization had to take the following steps: (1) confirm it was subject to the jurisdiction of the FTC or the DOT; (2) develop a binding privacy policy that mirrored the Safe Harbor Privacy Principles; (3) post the policy referencing Safe Harbor compliance so it was visible to the public; (4) develop an independent recourse mechanism for complaints; and (5) designate a contact person within the organization to receive any complaints.[53] The benefits of the Safe Harbor attached on the date of self-certification with the DOC. This occurred upon the submission of a letter from the corporate officer (1) containing the organization's contact information; (2) explaining the extent of the company's processing of EU data; (3) describing the privacy policy created to protect that data; and (4) stating the company's claim of self-certification.[54] Submission of this letter gave rise to a "presumption of adequacy" under the Directive.[55] To ensure continued adherence to the agreement, organizations were required to re-register yearly with the DOC, which housed a list of all the organizations compliant with Safe Harbor.[56]

While the EC issued a decision stating that the Safe Harbor agreement "ensure[d] an adequate level of protection for personal data transferred from the community to organizations established in the United States," [57] not everyone was pleased with the protections provided. Some critics of Safe Harbor argued that the agreement was only a "minimalist solution," and that the United States never intended to follow through on its commitment to strengthen protections over time. [58] Others pointed to the absence of actual enforcement by the FTC—which until 2009 had not brought a single enforcement action under the agreement. [59] Many believed these

---

51. *Id.* at 14; *see also* Federal Trade Commission Act, 15 U.S.C. § 45 (prohibiting "unfair or deceptive acts or practice in or affecting commerce").

52. Cunningham, *supra* note 39, at 443 (based upon this limitation, in actuality "only U.S. organizations subject to the jurisdiction of the FTC as well as U.S. air carriers and ticket agents subject to the jurisdiction of the DoT could participate in Safe Harbor. Many organizations that deal in foreign commerce were not eligible for the Safe Harbor program, including certain financial institutions–like banks, investment houses, and credit unions, telecommunication common carriers, labor associations, non-profit organizations, and agricultural co-operatives").

53. *Id.* at 444.

54. *Id.*

55. *See* Ewing, *supra* note 25, at 338.

56. *Id.* at 340.

57. Sean D. Murphy, *U.S.-EU "Safe Harbor" Data Privacy Arrangement*, 95 AM. J. INT'L L. 156, 159 (2001).

58. Voss, *supra* note 32, at 10.

59. *See* Cunningham, *supra* note 39, at 446.

weaknesses highlighted the current agreement's inability to provide real protection for EU personal data.[60] The Snowden revelations served only to further diminish the European Union's trust in cross-border data flows with the United States.[61]

### B. *Safe Harbor Invalidated: The Schrems Holding*

While talks of revisions to the Safe Harbor were in the works, the CJEU issued a ruling that invalidated Safe Harbor, prematurely determining the status of the agreement.[62] Maximillian Schrems, an Austrian law student and privacy advocate, brought a complaint against the Irish Data Protection Authority (DPA)[63] for failing to consider his twenty-three complaints against Facebook's Irish subsidiary for transferring Schrems' personal data to its US parent company.[64] Schrems originally brought the case in the High Court of Ireland, which referred the questions concerning the continued adequacy of the Safe Harbor to the CJEU.[65] Schrems argued that, in light of the National Security Agency (NSA) revelations concerning US intelligence authorities' practice of accessing personal data without court approval, his personal data lacked the adequate protection required by the Directive.[66]

The CJEU, which interprets and reviews EU law, holds the sole power to invalidate EU legal actions and determine the compatibility of international agreements with EU law.[67] In its holding invalidating the EU-U.S. agreement, the CJEU highlighted several fatal flaws in

---

60. *Id.* at 447 (noting that a 2008 study found that of 1,597 companies that self-certified, only "348 complied with the enforcement and dispute resolution principle").

61. *See* Alan S. Gutterman, *U.S. Companies Need to Prepare for Requirements of Privacy Shield to Continue Data Transfer from European Union*, 7 BUS. COUNSELOR UPDATE (July 2016) (noting that following the Snowden leaks, it was clear "that the original Safe Harbor Agreement would need to be revised or replaced in light of the questions regarding surveillance and personal data protection in the U.S."); *see also* Voss, *supra* note 32, at 3 (noting that the Snowden leaks sent an "electroshock" across the EU "encourag[ing] the advancement of EU data protection law reform and negatively impacting trust in cross-border data flows with the United States").

62. *See* Case C-362/14, Schrems v. Data Protection Comm'r, 2015 E.C.R. 26 (noting that the ruling was issued on October 6, 2015); *see also* Voss, *supra* note 32, at 3 (noting the same and providing background information on the case).

63. KRISTINA IRION, SVETLANA YAKOVLEVA & MARIJA BARTL, TRADE AND PRIVACY: COMPLICATED BEDFELLOWS? 13 (2016), https://www.ivir.nl/publicaties/download/1807 [https://perma.cc/8ZJA-2XHW] (archived Oct. 8, 2017) (explaining that national DPAs in each member state are charged with "implementing and enforcing" the national data protection laws).

64. Voss, *supra* note 32, at 3.

65. *Id.*

66. *Schrems*, 2015 E.C.R. § 28.

67. *See* IRION ET AL., *supra* note 63, at 11–12 (discussing the authority of the CJEU to review Privacy Shield based on the supervisory opinion procedure provided for in Article 218(11) of the TFEU).

Safe Harbor, which are instructive when hypothesizing about the future of the successor, Privacy Shield. These include the lack of protection from US surveillance,[68] the absence of any mechanism to hold the US government accountable for its promises under the agreement,[69] and the lack of accessible redress mechanisms for EU citizens.[70]

Article 25 instructs the EC to assess the non-EU member country's level of protection by looking at "the circumstances surrounding a data transfer operation . . . [including] the rules of law, both general and sectoral, in force . . . and the professional rules and security measures."[71] The CJEU noted that the EC, in deeming the Safe Harbor framework adequately protective, only considered the adequacy of the principles and implementation documents, and failed to consider the larger scope of applicable US laws. The fact that US domestic concerns regarding national security, public interest, or law enforcement requirements had primacy over the Safe Harbor Principles deeply troubled the CJEU, and the reality that Safe Harbor permitted interference with EU citizens' fundamental right to privacy was unacceptable to the Court.[72]

Additionally, the CJEU found that while self-certified US companies were legally obligated to provide "adequate" protection to EU personal data, US government authorities were not similarly bound to follow through on their commitments.[73] Finally, the CJEU highlighted the absence of "administrative or judicial means of redress"

---

68. *See Schrems*, 2015 E.C.R. § 86 (explaining that US "national security, public interest, or law enforcement requirements have primacy over the safe harbor principles").

69. *See id.* § 82 (expressing concern regarding the fact that US public authorities are not required to comply with the Safe Harbor principles).

70. *See id.* § 90 (discussing the lack of administrative or judicial redress for EU citizens); NATASCHA GERLACH, JAMES DALEY & CLEARY GOTTLIEB, FROM SAFE HARBOR TO THE EU-US PRIVACY SHIELD (2016), https://www.americanbar.org/content/dam/aba/events/cle/2016/05/ce1605edv/ce1605edvcor.authcheckdam.pdf [https://perma.cc/MXC7-DZML] (archived Sept. 20, 2017) ("The lack of legal remedies for non-US citizens/legal residents violates the right to effective judicial protection.").

71. European Council Directive 95/46, art. 25, § 2, 1995 O.J. (L 281) 31.

72. *See Schrems*, 2015 E.C.R. §§ 86–87 (rejecting the Safe Harbor because it interfered with "the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States"); MARTIN A. WEISS & KRISTEN ARCHICK, CONG. RES. SERV., U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 7 (2016), https://fas.org/sgp/crs/misc/R44257.pdf [https://perma.cc/23WT-DS9X] (archived Sept. 20, 2017) (explaining that the CJEU found that the Safe Harbor scheme interfered with fundamental privacy rights of EU citizens); Nora Ni Loirdean, *The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law*, 19 NO. 8 J. INTERNET L. 1, 1 (2016) (discussing the CJEU's decision to strike down the Safe Harbor scheme for failing to provide adequate protection for fundamental privacy rights of EU citizens).

73. *Schrems*, 2015 E.C.R. § 82.

for EU data subjects.[74] Without a mechanism for EU citizens to have their complaints assessed and remedied, the Court found US promises to be illusory in the eyes of the Court and insufficient to protect citizens' fundamental rights required under the Directive.[75] Following the invalidation of Safe Harbor, there was even more political pressure on both sides of the Atlantic to reach a new agreement.[76]

## IV. ANALYSIS OF THE PRESENT: EU-U.S. PRIVACY SHIELD AGREEMENT

On February 2, 2016, the European Union and the United States announced the successor agreement to Safe Harbor, the EU-U.S. Privacy Shield, and released a draft adequacy decision to the public shortly thereafter. Many in the European Union criticized the draft, including the WP29,[77] the European Parliament[78] and the European

---

74. *Id.* § 90.

75. *Id.* § 95.

76. *See* Voss, *supra* note 32, at 11 (discussing "other bases for adequacy in transatlantic data flows" following the *Schrems* decision). Negotiations had been going on since late 2013 in response to EU suspicion about NSA surveillance and its impact on EU data. Other critics pointed out that the original agreement was established in the late 1990s, and since then major technological advancements have occurred, which implicate new issues that weren't perceived in the original negotiation. WEISS & ARCHICK, *supra* note 72, at 8–9.

77. Opinion 01/2016 of Article 29 Data Protection Working Party, April 13, 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf [https://perma.cc/4D5N-DAAZ] (archived Oct. 8, 2017) (the EU Article 29 Working Party acknowledged that the Privacy Shield was a "great step forward" but highlighted that there were still areas that were unacceptable, including its lack of explicit denial of "massive and indiscriminate bulk" collection by US authorities, concerns regarding commercial parts of the decision: including data retention, data integrity and purpose limits, and assessing the law enforcement guarantees under the Privacy Shield) [hereinafter Opinion 01/2016]; *see also Privacy Shield – Rejected. GDPR – Accepted: What This Means to Your Organization and What You Should Consider Doing Now*, FOLEY (April 16, 2016), https://www.foley.com/Privacy-Shield--Rejected-GDPR--Accepted-What-This-Means-to-Your-Organization-and-What-You-Should-Consider-Doing-Now-04-15-2016/ [https://perma.cc/4QPP-65MR] (archived Oct. 17, 2017) (outlining the WP29's primary concerns with the proposed Privacy Shield framework agreement); Gary Roboff, *EU's GDPR and the EU-U.S. Privacy Shield: Where Are We and Why Are We There?*, THE SHARED ASSESSMENTS BLOG (May 31, 2016), http://sharedassessments.org/2016/05/eus-gdpr-and-the-eu-us-privacy-shield-where-are-we-and-why-are-we-there/ [https://perma.cc/3NZR-DBD6] (archived Sept. 21, 2017) (explaining that the WP29's issues with the Privacy Shield "involved both commercial entities and access by public authorities to data transferred under the Shield, especially in areas related to national security").

78. *See* Resolution 2016/2727, *supra* note 7 (this non-binding resolution included the following areas of concern and alteration: potential for bulk collection still impermissibly being possible under draft calling for clarification on written assurances from the US; asks for redress mechanisms that are "procedure user-friendly and effective"; requests a sufficiently independent ombudsperson; and calls for the Commission to implement fully the recommendations of Article 29 Working Party); *Privacy Shield and the General Data Protection Regulation: More Key Developments,*

Data Protection Supervisor, Giovanni Buttarelli.[79] They all expressed concerns regarding whether the new agreement provided the requisite protection for EU data subjects. While this early dissonance was nonbinding, many felt that "the Commission [was] obligated to take up necessary adjustments to the adequacy decision in its negotiations with the US," and that if these concerns were not addressed prior to implementation of the Privacy Shield, the agreement would face challenges before the CJEU.[80]

Taking many of the criticisms into consideration, the EC and DOC amended the original draft. This updated version was then approved by the Article 31 Committee (which is comprised of representatives of each of the EU member states and has binding authority)[81] and formally adopted by the full EC.[82] The Privacy Shield went into effect on July 12, 2016.[83] The agreement not only created the potential for a more stable and efficient compliance mechanism for US companies, but also showed the strong force of transatlantic cooperation.[84] The European Union and the United States recognized the need for an

---

SIDLEY (July 2, 2016), http://www.sidley.com/news/2016-06-02-privacy-update (highlighting deficiencies in the current draft of the Privacy Shield identified by the European Parliament).

79. *See* SIDLEY, *supra* note 78 (On May 30, 2016, Giovanni Buttarelli of the EDPS issued his opinion on the EC's draft adequacy decision on the Privacy Shield citing the need for more specific language concerning: data retention, automated processing, purpose limits, explicit wording on exceptions, onward transfers, right to access and right to object, and the right of redress and oversight).

80. Catherine Stupp, *EU Privacy Watchdogs Demand Improvements to 'Privacy Shield'*, EURACTIV.COM (Apr. 13, 2016, 11:08 AM), http://www.euractiv.com/section/digital/news/eu-privacy-watchdogs-demand-improvements-to-privacy-shield/ [https://perma.cc/4YTY-FA8Z] (archived Sept. 21, 2017).

81. WEISS & ARCHICK, *supra* note 72, at 12.

82. While the Commission approved the Privacy Shield, making the agreement final, there were four out of the twenty-eight EU diplomats that abstained from voting. The identities of which countries did not vote in the final approval have been kept secret, so as to present a unified front of support by member states for Privacy Shield. *See* Stupp, *supra* note 80 (noting that "a group of representatives from EU member states does not get to hold a binding vote on the agreement").

83. *Privacy Shield Program Overview*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Program-Overview (last visited Oct. 8, 2017) [https://perma.cc/T2F3-HEGX] (archived Sept. 21, 2017); *see EU-US Privacy Shield Becomes Operational with the GDPR on the Horizon*, BIRD & BIRD (Sept. 12, 2016), https://www.twobirds.com/en/news/articles/2016/uk/eu-us-privacy-shield-becomes-operational-with-gdpr-on-the-horizon [https://perma.cc/YY88-Y5M2] (archived Oct. 8, 2017) ("The new regime relies on a similar approach of self-certification and external verification against seven privacy principles.").

84. *See* John Frank, *EU-U.S. Privacy Shield: Progress for Privacy Rights*, EU POL'Y BLOG MICROSOFT (July 11, 2016), https://blogs.microsoft.com/eupolicy/2016/07/11/eu-u-s-privacy-shield-progress-for-privacy-rights/ [https://perma.cc/9VEE-GXV6] (archived Sept. 21, 2017) ("The successful and rigorous negotiations also demonstrate progress between Europe and the United States on a vital issue for transatlantic coordination.").

agreement that honors the fundamental rights of EU citizens while still providing a realistic standard by which companies can comply—the EU-U.S. Privacy Shield is their latest attempt at striking this proper balance.

### A. *How the EU-U.S. Privacy Shield Framework Operates*

The Privacy Shield operates in a similar fashion to Safe Harbor, allowing companies to opt into the requirements of the Privacy Shield by self-certifying to the DOC that they will abide by seven privacy principles.[85] These principles possess similar titles to Safe Harbor but represent more demanding requirements from participating companies. [86] The Privacy Shield Framework also includes supplemental principles that create a wide range of obligations for the companies implicated. [87] While entry into the Privacy Shield framework is voluntary, once a company joins and publicly certifies its commitment to the Privacy Shield Principles, its compliance under the Principles is mandated.[88]

To self-certify, a company must create a "Privacy Shield-compliant privacy policy" in line with the Privacy Shield Principles to be posted on the company's public forum so it is accessible to EU citizens. The Privacy Shield program is administered by the International Trade Administration (ITA)[89] and enforced by the FTC. [90] ITA is an agency

---

85. *See* European Commission Implementing Decision 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, C(2016) 4176 (Dec. 7, 2016), http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf [https://perma.cc/62VS-D3XJ] (archived Sept. 21, 2017) (listing the privacy principles: Notice, Choice, Accountability for Onward Transfers, Security, Data Integrity and Purpose Limitations, Access, Recourse Enforcement and Liability); *see also EU-U.S. Privacy Shield Framework Principles,* U.S. DEP'T OF COMMERCE, https://www.privacyshield.gov/EU-US-Framework [https://perma.cc/9X34-BXRQ] (archived Sept. 21, 2017) (the Commerce Department released the Privacy Shield Principles pursuant to 15 U.S.C. § 1512, which gives the Department the "authority to foster, promote, and develop international commerce").

86. Commission Implementing Decision, *supra* note 85; *see also* Daniel J. Solove, *GDPR, BCR, and Privacy Shield Training Requirements FAQ*, TEACH PRIVACY, https://www.teachprivacy.com/gdpr-privacy-shield-training-requirements-faq/ (last visited Oct. 8, 2017) [https://perma.cc/K6RU-5DN4] (archived Sept. 21, 2017) ("The principles have been made stricter, especially the parts about accountability, redress, and enforcement."); BIRD & BIRD, *supra* note 83.

87. *See EU-U.S. Privacy Shield Framework Principles*, *supra* note 85, at III.1–16 (list of Privacy Shield Supplemental Principles).

88. *Id.* at I. § 2. ("While decisions by organizations to enter the Privacy Shield are entirely voluntary, effective compliance is compulsory.").

89. *Administration of Privacy Shield,* PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=Administration-of-Privacy-Shield (last visited Oct. 8, 2017) [https://perma.cc/5FBS-QZJW] (archived Sept. 21, 2017).

90 *See* Enforcement of Privacy Shield, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=Enforcement-of-Privacy-Shield (last visited

within the DOC responsible for verifying that companies that opt into the Framework satisfy their requirements for self-certification.[91] Accordingly, ITA is charged with maintaining the Privacy Shield List—the public list of all US organizations that have declared their commitment to adhere to the principles—which includes adding those that have successfully certified and removing organizations that have voluntarily withdrawn, have failed to recertify, or have shown a pattern of failure to comply. Along with the Privacy Shield List, the ITA has a working list of those companies that have been removed and the reasons for their removal—all of which is available to the public.

Self-certification with the ITA is an annual process for companies that wish to stay protected under the Privacy Shield. Companies should be aware that even if they decide to withdraw from the Privacy Shield list,[92] the requirement to act in accordance with the Privacy Shield Principles still attaches to any data retained as a result of participation in the program.[93] As of October 19, 2017, a total of 2,517 companies had certified under the Framework, including major corporations like Google, Facebook,[94] and Microsoft.[95] US companies have been quick to praise this new deal, saying that it protects user privacy while allowing for the continuation of economically significant transatlantic trade.[96] Microsoft's Vice President of EU Government

---

Oct. 23, 2017) [https://perma.cc/8BH8-VJDB] (archived Oct. 23, 2017) (the FTC can challenge as a deceptive practice under the Federal Trade Commission Act, 15 U.S.C §45, §5(a) the failure in full or in part of companies who certify under Privacy Shield. The FTC enforcement is achieved through administrative orders or by seeking court orders that carry penalties if violated).

91. *See Administration of Privacy Shield,* PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=Administration-of-Privacy-Shield (last visited Oct. 8, 2017) [https://perma.cc/5FBS-QZJW] (archived Sept. 21, 2017) (detailing the ITA's verification process for companies that opt-in to the framework).

92. *See Withdrawal from Privacy Shield,* PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=Withdrawal-from-Privacy-Shield [https://perma.cc/H42Y-944T] (archived Sept. 21, 2017) (detailing the Privacy Shield Framework withdrawal process).

93. *See id.* ("Your organization must continue to apply the Privacy Shield Principles . . . otherwise, your organization must return or delete the information or provide 'adequate' protection for information by another authorized means.").

94. James Titcomb, *Facebook Signs Up to Privacy Shield Data Treaty*, THE TELEGRAPH (Oct. 16, 2016, 8:15 PM), http://www.telegraph.co.uk/technology/2016/10/15/facebook-signs-up-to-privacy-shield-data-treaty/ [https://perma.cc/7BW8-46KB] (archived Sept. 21, 2017) (significant since the prior EU-US agreement, Safe Harbor, was invalidated as a result of a complaint brought before the CJEU against Facebook).

95. *See Privacy Shield List,* PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/list (last visited Oct. 8, 2017) [https://perma.cc/7ZQP-LXRJ] (archived Sept. 21, 2017) (list of companies certified under the framework).

96. Amar Toor, *EU-US Privacy Shield Agreement Goes Into Effect: Tech Companies Welcome New Data Transfer Agreement, But Activists Say it Doesn't Do Enough to Protect Privacy*, THE VERGE (July 12, 2016, 5:03 AM), http://www.theverge.com/2016/7/12/12158214/eu-us-privacy-shield-data-transfer-

Affairs believes the Privacy Shield properly meets the EU's data protection rules.[97]

### B. *Improvements in the Privacy Shield*

Even those most critical of the Privacy Shield concede that it is an improvement in many respects over its predecessor.[98] The EU-U.S. Privacy Shield provides enhanced protections to EU data subjects through three general avenues: comprehensive data protection, user-friendly redress mechanisms that are accessible to EU citizens, and hands-on oversight by US authorities to ensure compliance and enforcement.

#### 1. Data Protection Mechanisms

The Privacy Shield provides for more restrained processing and usage of EU data, specifically via more strenuous requirements on data retention and minimization. Under the Privacy Shield, US companies are constrained by two principles: (1) data retention, which prohibits the retention of personal data for an excessive time, and (2) data minimization, which permits companies to receive and process data only for a specifically stated purpose and bars them from retaining such data for any longer than needed for that specific purpose.[99] If a company does keep data longer than specified, there must be a legitimate reason, like "archiving for public interest, journalism, literature and art, scientific or historical research, or for statistical analysis."[100]

Another area of added protection under the Privacy Shield concerns the onward transfers of EU data to third parties that may or may not have independently opted in to the Framework.[101] Under the old agreement, a US business did not have to provide notice and choice to EU data subjects if the transfer was to an agent of the company.[102]

---

privacy [https://perma.cc/Y93V-96AP] (archived Sept. 21, 2017) ("Tech companies have welcomed the new deal, saying that it protects user privacy while allowing for trans-Atlantic trade.").

97. Frank, *supra* note 84.

98. *See* Opinion 01/2016, *supra* note 77, at 2 (WP29 admitted that Privacy Shield was better than old Safe Harbor agreement).

99. *See EU-U.S. Privacy Shield Framework Principles*, *supra* note 85, at II.5 (describing data integrity and purpose limitations under the framework).

100. *See id.* (noting that if your data is kept for an extended purpose for any of the listed reasons the company is still required to comply with the Privacy Principles).

101. *See id.* at II.3 (describing accountability for onward transfer principal under the new Privacy Shield).

102. *How Does Safe Harbor Compare to the EU-US Privacy Shield?*, ONLINE TECH, http://www.onlinetech.com/resources/references/how-does-safe-harbor-compare-

Organizations participating in the Privacy Shield conversely must ensure that any transfer of data to another company is properly protected.[103] If the third party cannot adequately protect the data, the transfers must cease.[104] Whether the onward transfer is to a third party acting as a controller[105] or as an agent,[106] a Privacy Shield company must contract with the third party and ensure that they provide the same level of protection as the original self-certified entity.[107]

In addition to its impact on US companies, the Privacy Shield grants EU data subjects with new affirmative rights concerning the protection of their data. First, if a company under the Framework wishes to use the data for a purpose different than the one originally intended, EU citizens have the right to opt out of the continued usage of their data.[108] Additionally, EU citizens now have the right to amend misstatements in their personal data—the data subject can request

---

to-the-eu-us-privacy-shield (last visited Oct. 8, 2017) [https://perma.cc/VTU7-89PE] (archived Sept. 21, 2017).

103. *See Final Privacy Shield: How it Changed and What It Means for Businesses*, LEXOLOGY (July 19, 2016), http://www.lexology.com/library/ detail.aspx?g=f403d783-6396-4508-8eed-da1b165fc56e [https://perma.cc/7BDL-ZGA9] (archived Sept. 21, 2017) (explaining that companies transferring data to third parties under the Privacy Shield framework will have to include more specific contractual obligations than previously required by the Safe Harbor).

104. *See id.* (discussing the tightened conditions for third party data sharing).

105. GUIDE TO THE EU-U.S. PRIVACY SHIELD, *supra* note 4, at 11 (defining a controller as a company that itself decides how to use the data). Data controllers are required to give notice and choice to a data subject and enter into a contract with the third party ensuring that the processing of EU personal information will be limited and for specific purposes in line with the consent given and that the third party will abide by the Privacy Principles. The contract should also require the third party to notify the Privacy Shield organization if it can no longer meet such requirement, at which time processing of EU data must cease. *EU-U.S. Privacy Shield Framework Key New Requirements*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Key-New-Requirements (last visited Oct. 8, 2017) [https://perma.cc/D8VM-M937] (archived Sept. 21, 2017).

106. GUIDE TO THE EU-U.S. PRIVACY SHIELD, *supra* note 4, at 11 (explaining that an agent is often needed to fulfill a service contract with a sub-processor). A Privacy Shield company faces stricter requirements to ensure that an agent transfers for limited purposes, provides at least equivalent protection as that required by the principles, notifies the Privacy Shield company in case of inability to provide requisite protection and takes reasonable steps to remediate. If the agent fails to properly protect data subjects, the Privacy Shield company can be liable. *EU-U.S. Privacy Shield Framework Key New Requirements*, *supra* note 105.

107. *See* GUIDE TO THE EU-U.S. PRIVACY SHIELD, *supra* note 4, at 11 (including that third parties ensure their usage and processing of data is limited and that they provide notice and cease usage of the data if they are unable to provide the requisite protection).

108. *See Safe Harbor Replacement EU-US Privacy Shield Approved*, THE NAT'L L. REV. (July, 12, 2016), http://www.natlawreview.com/article/safe-harbor-replacement-eu-us-privacy-shield-approved [https://perma.cc/2QNX-KLEP] (archived Sept. 22, 2017) (recognizing that often EU data will be processed for the primary purpose of a business and then additionally used in direct marketing purposes).

that a company amend or remove personal data that is inaccurate, outdated, or being handled in a way that violates the Privacy Shield.[109] Further, under the new Framework, data subjects have a right to know if their information is being processed—if a data subject makes contact with a company, the company is obligated to confirm whether or not they possess the individual's data within a reasonable time frame.[110]

2. Redress Mechanisms

The CJEU cited the lack of accessible modes of redress for EU data subjects as a rationale for striking down Safe Harbor in *Schrems v. Data Protection Commission*. The DOC and EC acknowledged this weakness and instituted multiple venues in which EU citizens may file complaints and seek remedy under the Privacy Shield.[111] Companies that want to certify under the Privacy Shield are required to provide free and user-friendly dispute resolution.[112] EU citizens may choose whether to bring a complaint and in what form to file their claim.[113] If a complaint is brought directly to the US company, the company must respond promptly to the individual, providing an independent recourse mechanism by which the EU data subject's complaint can be fairly investigated and resolved.[114] If an EU citizen prefers to submit her complaint to the DPA within the EU, the ITA assumes the responsibility for review and facilitation of a resolution.[115]

---

109. *See EU-US Privacy Shield Framework Principles*, *supra* note 85, at II.6 (explaining that EU data subjects "must have access to personal information about them . . . and be able to correct, amend, or delete that information where it is inaccurate"); *see also* GUIDE TO THE EU-U.S. PRIVACY SHIELD, *supra* note 4, at 11 (detailing that U.S. companies have to respond to data subject's access request "within a reasonable time frame," but a limit to this requirement might be if access would "breach professional privilege or conflict with legal obligations").

110. GUIDE TO THE EU-U.S. PRIVACY SHIELD, *supra* note 4, at 11.

111. *See EU-US Privacy Shield Framework Principles*, *supra* note 85, at II.7 (Recourse, Enforcement and Liability Principles); GUIDE TO THE EU-U.S. PRIVACY SHIELD, *supra* note 4, at 10, 12 (detailing several means of lodging a complaint under Privacy Shield).

112. *See EU-US Privacy Shield Framework Principles*, *supra* note 85, at III.11 (Dispute Resolution and Enforcement).

113. An individual has several possibilities to lodge a complaint, including: with the company itself, through an independent resource mechanism like Alternative Dispute Resolution, review by a national Data Protection Authority (DPA), through the DOC, FTC, or Privacy Shield Panel (after other redress options have been attempted). *See* GUIDE TO THE EU-U.S. PRIVACY SHIELD, *supra* note 4, at 15.

114. *Id.*

115. *Id. But see* Article 29 Working Party Statement on the Decision of the European Commission on the EU-U.S. Privacy Shield (July 26, 2017), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf [https://perma.cc/V58A-76U8] (archived Oct. 8, 2017) [hereinafter *WP 29 Statement*] (noting that a major concern for the EU is that U.S. enforcement is not mandated by any binding transnational legal source).

If these recourse mechanisms prove insufficient, a company must commit to binding arbitration, the process for which is explicitly laid out in an annex to the Framework.[116] The Privacy Shield not only greatly expands the explicit remedial rights of EU citizens, but importantly provides clear guidance for all involved on how to go about the exercise of redress actions.[117]

Another grievance the CJEU voiced when striking down Safe Harbor was the lack of restraint on US surveillance of EU data. While this issue is still a source of contention in the new Privacy Shield, the agreement does provide EU citizens with the possibility of redress.[118] This may be available in situations where an individual's personal data is accessed for a purpose beyond what is necessary for pursuing public interest objectives like national security or law enforcement.[119] This new protection was made possible by President Obama's adoption of the Judicial Redress Act, which extended protections under the 1974 Privacy Act to citizens of the European Union.[120] Additionally, the determination of necessity is judged by a newly created ombudsperson.[121] This is a significant addition to the Privacy Shield

---

116. *See EU-U.S. Privacy Shield Framework Principles*, *supra* note 85, at Annex I (Binding Arbitration) §§ A–H (details scope, available remedies, pre-arbitration requirements, binding nature, review and enforcement, the arbitration panel, procedures and costs).

117. *See* GUIDE TO THE EU-U.S. PRIVACY SHIELD, *supra* note 4, at 15–16 (noting all the ways that a data subject can lodge a complaint: (1) U.S. Privacy Shield Company; (2) Independent ADR body; (3) National Data Protection Authority; (4) Department of Commerce; (5) Federal Trade Commission; (6) Privacy Shield (Arbitral) Panel).

118. Though the Privacy Shield ensures US authorities will have limited access to EU citizen's data, letters from the Office of the Director of National Intelligence and Department of Justice outline the safeguards and limitations applicable to guard EU data from US national security authorities and law enforcement. *See* Letter from Robert S. Litt, Office of the Dir. of Nat'l Intelligence, Office of Gen. Counsel, to Justin S. Antonipillai, Counselor, U.S. Dep't of Commerce & Ted Dean, Deputy Assistant Sec'y, Int'l Trade Admin. (Feb. 22, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1F [https://perma.cc/T5QC-LRLV] (archived Sept. 22, 2017); Letter from Bruce C. Swartz, Deputy Assistant Attorney Gen. and Counselor for Int'l Affairs, Dep't of Justice, to Justin S. Antonipillai, Counselor, U.S. Dep't of Commerce & Ted Dean, Deputy Assistant Sec'y, Int'l Trade Admin. (Feb. 19, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0W [https://perma.cc/G8RH-JHWZ] (archived Sept. 22, 2017).

119. *See* Litt, *supra* note 118; Swartz, *supra* note 118 (discussing access limitations on data obtained for law enforcement or public interest purposes).

120. Allison Callahan-Slaughter, *Lipstick on a Pig: The Future of Transatlantic Data Flow Between the EU and the United States*, 25 TUL. J. INT'L & COMP. L. 239, 254 (2016); Voss, *supra* note 32.

121. U.S. DEP'T OF STATE, ANNEX A: EU-U.S. PRIVACY SHIELD OMBUDSPERSON MECHANISM REGARDING SIGNALS INTELLIGENCE, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g (last visited Oct. 8, 2017) [https://perma.cc/6VN4-ZDDR] (archived Oct. 8, 2017) ; *see* Letter from John F. Kerry, Sec'y of State, to Věra Jourová , Comm'r for Justice, Consumers and

framework in that a new entity was created to ensure that the US government is keeping its pledge to not excessively use EU citizens' data, which has been a major concern for many in the European Union following the Snowden revelations.[122] Though a step in the right direction, it remains to be seen whether this remedial action alone will be sufficient to pacify the concerns of the EC and to withstand a challenge by the CJEU.

3. Oversight Mechanisms

With commitments from the DOC,[123] the FTC,[124] the DOT,[125] the Office of National Intelligence,[126] the Department of State,[127] and the Department of Justice,[128] the United States is going to great lengths to convince the EC of its intent to ensure US companies' compliance with the Framework and its principles. While the FTC's role in enforcing Privacy Shield is largely identical to its role in Safe Harbor, the agency appears to be taking its enforcement role more seriously. On September 8, 2017, the FTC released a statement that it settled charges against three US companies that had represented to consumers that they were participating in the EU-U.S. Privacy Shield despite their respective failures to complete the certification process.[129]

---

Gender Equality, European Comm'n (July 7, 2016) (memorializing the agreement reached regarding the EU-U.S. Privacy Shield and the ombudsperson mechanism).

122. *See* GUIDE TO THE EU-U.S. PRIVACY SHIELD, *supra* note 4, at 13 (discussing the Privacy Shield Framework's implementation of the Ombudsman mechanism). *But see WP 29 Statement*, *supra* note 115, at 1 (recognizing that this independent review mechanism is still a component of the US government, there is no true binding component).

123. *See* Letter from Penny Priztker, Sec'y of Commerce, to Věra Jourová , Comm'r for Justice, Consumers and Gender Equality, European Comm'n (July 7, 2016) (transmitting the Privacy Shield Package).

124. *See* Letter from Edith Ramirez, Chairwoman, Fed. Trade Comm'n, to Věra Jourová, Comm'r for Justice, Consumers and Gender Equality, European Comm'n (July 7, 2016) (describing its enforcement of Privacy Shield).

125. *See* Letter from Anthony R. Foxx, Sec'y of Transp., Dep't of Transp., to Věra Jourová, Comm'r for Justice, Consumers and Gender Equality, European Comm'n (Feb. 19, 2016) (describing its enforcement of the Privacy Shield).

126. *See* Litt, *supra* note 118 (detailing PPD-28 and U.S. surveillance law).

127. *See* Kerry, *supra* note 121 (describing the new "Ombudsperson mechanism through which authorities in the EU will be able to submit requests on behalf of EU individuals regarding U.S. signals intelligence practices").

128. *See* Swartz, *supra* note 118 (noting DOJ outline of safeguards and limitations on U.S. Government access for law enforcement and public interest purposes).

129. *See* Press Release, Federal Trade Commission, Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework (Sept. 8, 2017), https://www.ftc.gov/news-events/press-releases/2017/09/three-companies-agree-settle-ftc-charges-they-falsely-claimed?utm_source=govdelivery [https://perma.cc/G3J5-KMPB] (archived Oct. 19, 2017) (the three companies, Decusoft LCC, Tru Communications, Inc. (operating under the name TCPrinting.net), and Md7, LLC, are prohibited from misrepresenting their

Many view this enforcement action during Privacy Shield's infancy as "highlighting the FTC's commitment to aggressively enforcing the Privacy Shield . . . ."[130]

The new agreement creates a more hands-on role for the ITA in motioning and supervising compliance under the agreement. [131] Beyond the annual recertification process created originally in Safe Harbor, the ITA will now conduct *ex officio* compliance reviews via detailed questionnaires and will investigate companies that leave or fail to recertify under the Privacy Shield.[132] While this represents a significant commitment of US government resources to the enforcement of the EU-U.S. Privacy Shield, it is important to recognize that these new commitments are not compulsory and do not provide the same motivational capital for compliance that might encourage US companies to certify and abide by the privacy principles.

Another novel feature of the new EU-U.S. Privacy Shield is annual joint review by both the DOC and the EC.[133] This revisionary meeting ensures the Framework is working properly and allows for amendments if necessary. The ability to continually evolve the agreement as technology and the political climates of the European Union and the United States change is a dexterous addition.[134] It should be stressed that the first annual joint review in September 2017 provided more information concerning whether the Privacy Shield will endure as a lasting transnational agreement or face a similar fate to Safe Harbor.[135]

---

compliance under any government data or privacy programs and must comply with FTC reporting requirements as conditions of their settlement).

130. *See id.* (Acting FTC Chairman Maureen K. Ohlhausen further emphasized that "[c]ompanies that want to benefit from these agreements must keep their promises or [FTC] will hold them accountable").

131. *See Administration of Privacy Shield*, PRIVACY SHIELD PROGRAM, https://www.privacyshield.gov/article?id=Administration-of-Privacy-Shield [https://perma.cc/P4NF-SBT8] (archived Sept. 24, 2017) (explaining ITA's role under the Privacy Shield program).

132. Sotirios Petrovas & Cynthia J. Rich, *Privacy Shield vs. Safe Harbor: A Different Name for an Improved Agreement?*, MORRISON FOERSTER (Mar. 3, 2016), https://www.mofo.com/resources/publications/privacy-shield-vs-safe-harbor-a-different-name-for-an-improved-agreement.htmlhttp://www.onlinetech.com/resources/references/how-does-safe-harbor-compare-to-the-eu-us-privacy-shield [https://perma.cc.KG4X-XQMV] (archived Sept. 22, 2017).

133. *See* European Commission Implementing Decision EU 2016/1250, 2016 O.J. (C 207) 1 (detailing how the Annual Joint Review will be performed and who will participate).

134. *Safe Harbor Replacement EU-US Privacy Shield Approved*, *supra* note 108.

135. *See infra* Part V.A (discussing the Annual Joint Review).

### C. *Remaining Weaknesses and Potential Issues Threatening the Privacy Shield*

Though the improvements discussed above address some of the concerns cited by the CJEU, they by no means immunize the Privacy Shield from challenge or from the threat of invalidation. Looking critically at the new framework, not only is there still a strong threat that EU data will be subjected to US surveillance, but there are additional external variables in the backdrop that serve to threaten the vitality of the Privacy Shield.

#### 1. Lack of Protection from US Surveillance

Many in the European Union are still concerned that the EU-U.S. Privacy Shield does not provide sufficient restrictions on US surveillance actions. Following the CJEU's invalidation of Safe Harbor, the WP29 issued guidance on the extent of permissible interference with a data subject's fundamental right to privacy in the name of surveillance when transferring data. [136] The European Essential Guarantees are domestic EU standards established by the WP29 to help define what permissible interferences should look like in a democratic society.[137] Although these principles do not directly apply to the United States, the WP29 used the European Essential Guarantees for data transfers in their Opinion 01/2016 to assess the adequacy of the Privacy Shield protections. [138] While the WP29 acknowledges the increased transparency offered by the US Administration and the verbal commitment of the Office of the Director of National Intelligence (ODNI) to not indiscriminately collect personal data, it still highlights the absence of any concrete assurance within the Privacy Shield text that the practice will not take place.[139] The

---

136. *See generally* Opinion 01/2016, *supra* note 77, at 11 ("The WP29 stresses that any interference with the fundamental rights to private life and data protection need to be justifiable in a democratic society.").

137. The Four European Essential Guarantees: 1. Processing should be clear, precise and accessible rules; 2. Necessity and proportionality with regard to the legitimate objectives pursued needs to be demonstrated; 3. An independent oversight mechanism should exist; 4. Effective Remedies need to be available to the individual. *See* Article 29 Data Protection Working Party, Working Document 01/2016 (European Essential Guarantees) (Apr. 13, 2016), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf [https://perma.cc/9BT2-P6FM] (archived Sept. 22, 2017).

138. Opinion 01/2016, *supra* note 77, at 4.

139. *See id.*; *WP 29 Statement*, *supra* note 115, at 1; Danny O'Brien & Rainey Reitman, *The Privacy Shield is Riddled with Surveillance Holes*, ELECTRONIC FRONTIER FOUNDATION (Mar. 3, 2016), https://www.eff.org/deeplinks/2016/03/privacy-shield-riddled-surveillance-holes [https://perma.cc/9KAU-M2YX] (archived Sept. 22, 2017) (arguing that the Privacy Shield does not actually prevent the collection of EU data by U.S. intelligence agencies).

WP29's long-standing position has been that such massive and indiscriminate surveillance can never be proportionate or strictly necessary in a democratic society, which the European Essential Guidelines require to properly protect fundamental rights.[140] It is unclear if the CJEU will follow the WP29's rationale and hold that the verbal commitment to stop indiscriminate and bulk collection of data by the ODNI is insufficient.

While the EU-U.S. Privacy Shield did create a new redress option for EU data subjects, satisfying the remedies element of the European Essential Guarantees, the efficacy of this mechanism remains to be seen.[141] The WP29 celebrated the creation of an ombudsperson to evaluate when US surveillance goes beyond what is necessary for legitimate purposes, but it remained skeptical whether the position can be both independent and vested with significant power to provide adequate redress.[142] The WP29 expressed the wish that the Privacy Shield had included more explicit guarantees concerning the independence and authority of the ombudsperson.[143] Only time will show the efficacy and autonomy of the ombudsperson and whether the presence of a redress mechanism will be sufficient to appease the CJEU without more explicit corresponding limitations on bulk collection.

2. External Factors

Looking outside the four corners of the agreement, an additional examination of external factors in both the United States and the European Union exposes further weaknesses in the new Framework.

i. US Political Climate: Trump Administration

The 2016 US presidential election has created additional uncertainty about the future of the Privacy Shield, with some critics concerned about the new administration's intent to honor US promises. One of President Trump's first executive orders, "Enhancing Public Safety in the Interior of the United States," directed US agencies to "ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."[144] While this caused a frenzy of speculation about the future of the

140. Opinion 01/2016, *supra* note 77, at 4.
141. *Id.* at 3–4.
142. *Id.* at 4.
143. *See WP 29 Statement*, *supra* note 115, at 1 (stating that the WP29 would have expected stricter guarantees concerning the independence and the powers of the Ombudsperson mechanism).
144. Exec. Order No. 13,768, 82 Fed. Reg. 8799, § 14 (Jan. 25, 2017).

Privacy Shield, the EC has asserted that the executive order should not impact the current agreement.[145] The EU-U.S. Privacy Shield and U.S. Privacy Act implicated within Trump's Executive Order are not mutually dependent instruments, and the Privacy Shield "does not rely on the protections under the U.S. Privacy Act."[146] Rather, the EC asserts that the Privacy Shield is based on the combination of "U.S. domestic law, international commitments, the Privacy Shield Principles, and an EC Decision of Adequacy."[147]

It remains unclear whether the Executive Order will directly impact the Privacy Shield. However, the Order reflects the new administration's position on transnational data privacy and suggests that the administration may take action that could jeopardize the data transfer agreement in the future.[148] The contrast between this executive order and those signed by President Obama[149] suggests that the two administrations have different approaches to transatlantic data transfers. In response, EU Commissioner for Justice, Consumers, and Gender Equality Věra Jourová has stated that she intends to ensure that the United States upholds a "culture of privacy" and that it follows through on commitments regarding US law enforcement and surveillance activities.[150] Only time will tell if the new Trump administration is committed to the Privacy Shield.

---

145. *See* Jan Phillip Albrecht (@JanAlbrecht), TWITTER (Jan. 26, 2017, 1:45 AM), https://twitter.com/JanAlbrecht/status/824553962678390784 [https://perma.cc/CJX8-FFTY] (archived Sept. 23, 2017) ("If this is true [Trump's Executive Order] @EU_Commission has to immediately suspend #PrivacyShield & sanction the US for breaking EU-US umbrella agreement. #CPDP2017.").

146. Natasha Lomas, *Trump Order Strips Privacy Rights from Non-U.S. Citizens, Could Nix EU-US Data Flows*, TECH CRUNCH (Jan. 26, 2017), https://techcrunch.com/2017/01/26/trump-order-strips-privacy-rights-from-non-u-s-citizens-could-nix-eu-us-data-flows/ [https://perma.cc/HW9H-9ZMZ] (archived Sept. 23, 2017).

147. Phil Bradley-Schmieg & David Bender, *European Commission Dismisses Privacy Shield Concerns Over Trump Executive Order*, INSIDE PRIVACY COVINGTON (Jan. 27, 2017), https://www.insideprivacy.com/international/european-union/european-commission-dismisses-privacy-shield-concerns-over-trump-executive-order/ [https://perma.cc/N73Z-BVP9] (archived Sept. 23, 2017).

148. *See* Phil Muncaster, *Trump Order Sparks Privacy Shield Fears*, INFOSECURITY MAGAZINE (Jan. 27, 2017), https://www.infosecurity-magazine.com/news/trump-order-sparks-privacy-shield/ [https://perma.cc/KFJ6-BGMD] (archived Sept. 23, 2017) (predicting that the Trump administration's 'America First' policies could jeopardize the data sharing agreement).

149. *See* Lomas, *supra* note 146 (noting that Obama's E.O. called for the limiting of U.S. agencies' surveillance to protect the privacy and civil liberties of all persons, whatever their nationality, and regardless of where they might reside).

150. *See EU Commissioner Plans to Assess U.S. Privacy Shield Commitments*, THE NAT'L L. REV. (Jan. 14, 2017), http://www.natlawreview.com/article/eu-commissioner-plans-to-assess-us-privacy-shield-commitments [https://perma.cc/7ZF4-2H56] (archived Sept. 23, 2017) ("Jourová indicated that she would seek to ensure that the U.S. maintains a 'culture of privacy' under the new administration, and that the U.S. government would continue to adhere to its commitments with regard to U.S. law

Another concern in the wake of the Trump election is whether President Obama's 2014 Presidential Policy Directive 28 (PPD-28) will be preserved.[151] PPD-28 is "a keystone underlying support for the Privacy Shield," and has a binding effect on US intelligence agencies.[152] It requires that intelligence agencies' collection and access to EU personal data be "as tailored as feasible," rather than "generalized."[153] This Directive legitimately limits such agencies' ability to engage in bulk collection, which is a source of major concern of the CJEU and EU citizens surrounding the adequacy of the Privacy Shield.[154] However, the new CIA Director, Mike Pompeo, has spoken directly against such limitations on US surveillance powers.[155] This,

---

enforcement and surveillance activities that were included within the Privacy Shield framework.").

151. *See* Press Release, Office of the Press Sec'y, Presidential Policy Directive–Signals Intelligence Activities, Policy Directive/PPD-28 (Jan. 17, 2014), http://go.wh.gov/WWipZM [https://perma.cc/PD9Q-RVTV] (archived Sept. 23, 2017) (stating that PPD-28 holds that signals intelligence activities must be conducted in such a way that ensures all persons [are] treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interest in the handing of their personal information); EU and U.S. Release Terms of Privacy Shield 5, Jones Day (Mar. 2015), http://www.jonesday.com/files/Publication/9dc75607-8e9b-4358-822d-0bfe2d72438d/Presentation/PublicationAttachment/ad1b7032-29bc-418a-8579-24e75b8b3de1/EU%20and%20US%20Release%20Terms%20of%20Privacy%20Shield.pdf [https://perma.cc/CXK9-VFFM] (archived Oct. 8, 2017) (noting the concerns of EU citizens regarding potential breaches of binding commitments by the U.S. government).

152. *See* Jones Day, supra note 151 (the Privacy Shield incorporates Presidential Policy Directive 28 ("PPD-28")'s binding effect on U.S. intelligence agencies); Cameron Kerry & Alan Charles Raul, The Economic Case for Preserving PPD-28 and Privacy Shield, LAWFARE (Jan. 12, 2017), https://lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield [https://perma.cc/V6CL-DSKB] (archived Sept. 23, 2017) (acknowledging that PPD-28 protects the privacy interests of innocent foreigners whose electronic communications are scooped up by NSA merely as incidental collections to the agency's actual targeting of malicious individuals).

153. *See* Press Release, Office of the Press Sec'y, *supra* note 151 ("In determining whether to collect signals intelligence, the [U.S.] shall consider availability of other information . . . appropriate and feasible alternatives to signals intelligence should be prioritized."); *see also* Jones Day, *supra* note 151 ("PPD-28 requires collection and access to EU personal data by U.S. intelligence agencies to be 'as tailored as feasible' rather than carried out on a 'generalized basis.'").

154. *See* Jones Day, *supra* note 151 (explaining that PPD-28 has a binding effect on U.S. intelligence agencies); *supra* Part III.B (examining CJEU concerns about Safe Harbor included lack of surveillance protections); *supra* Part IV.C.1 (recognizing that one weakness that still remains in new Privacy Shield agreement is access to EU Data by U.S. Intelligence authorities); *see also* Kerry & Raul, *supra* note 152 (predicting that a revocation of PPD-28 would undercut the Privacy Shield Framework and likely lead to its suspension).

155. *See* Adam Klein, *Surveillance Policy in a Trump Administration*, LAWFARE (Dec. 22, 2016, 11:00 AM), https://www.lawfareblog.com/surveillance-policy-trump-administration [https://perma.cc/TH5K-3W95] (archived Sept. 23, 2017) (pointing out that Mike Pompeo challenged Obama-era surveillance policy in several ways, but also emphasized the importance of building enduring public support for surveillance activities on a bipartisan basis).

paired with recent executive orders, shows a diminished concern for data privacy.[156]

In late March, Commissioner Jourová visited Washington D.C. to speak with US authorities about the state of the Privacy Shield, seeking reassurances that despite concerning US policy, the new administration was committed to the transatlantic agreement.[157] Meetings included sit-downs with U.S. Secretary of Commerce Wilber Ross and Attorney General Jeff Sessions, as well as discussions with various US companies and privacy NGOs.[158] Following her meetings, Commissioner Jourová spoke at the Center for Strategic & International Studies, stressing the need to limit government access to personal data and to ensure adequate oversight of companies' compliance.[159] Despite Commissioner Jourová's positive tweets regarding her US travels,[160] not all European regulators were convinced.[161]

Privacy Shield critics became even more apprehensive on April 4, 2017, when President Trump signed a Congressional Resolution rescinding an Obama-era rule that required internet service providers

---

156. *See id.* (noting that Pompeo and Jeff Sessions have both supported bulk collection of communications metadata).

157. *See* Stephanie Bodoni, *If Trump Spoils Privacy Pact, We'll Pull It, EU Official Warns*, BLOOMBERG TECH. (Mar. 2, 2017), https://www.bloomberg.com/news/articles/2017-03-02/if-trump-spoils-privacy-pact-we-ll-pull-it-eu-official-warns [https://perma.cc/EJA5-7MJR] (archived Sept. 23, 2017) (Commissioner Jourová stated prior to her trip that "If there is a significant change, we will suspend . . . I will not hesitate to do it. There's too much at stake").

158. *See* Li Zhou et al., *EU antitrust, privacy regulators visit D.C.*, POLITICO (Mar. 29, 2017), http://www.politico.com/tipsheets/morning-tech/2017/03/eu-antitrust-privacy-regulators-visit-dc-219486 [https://perma.cc/KS6Z-SYVB] (archived Sept. 23, 2017) (tracking Jourová's meetings during her visit).

159. Věra Jourová, European Comm'r for Justice, Speech at the Center for Strategic and International Studies (Mar. 31, 2017), https://ec.europa.eu/commission/commissioners/2014-2019/jourova/announcements/speech-commissioner-jourova-event-organized-center-strategic-and-international-studies_en [https://perma.cc/23G6-ZDB8] (archived Sept. 30, 2017).

160. *See* Věra Jourová (@VeraJourova), TWITTER (March 30, 2017), https://twitter.com/VeraJourova/status/847451968067047424 [https://perma.cc/8KDL-F5WW] (archived Sept. 23, 2017) ("Good first meeting w/ @USAGSessions Attorney General of the United States. EU – US cooperation is crucial, especially on criminal justice"); Věra Jourová (@VeraJourova), TWITTER (March 30, 2017), https://twitter.com/VeraJourova/status/847540721360015360 [https://perma.cc/5JA6-YUM5] (archived Sept. 23, 2017) ("good meeting w/ @SecretaryRoss, U.S. Secretary of Commerce to discuss #PrivacyShield. #dataprotection creates trust for data flows #EU to #US").

161. *See* Catherine Stupp, *MEPs want Commission to toughen up Privacy Shield under Trump*, EURACTIV.COM (Apr. 6, 2017), https://www.euractiv.com/section/data-protection/news/meps-want-commission-to-toughen-up-privacy-shield-under-trump/ [https://perma.cc/Q99M-GP88] (archived Sept. 23, 2017) (acknowledging that Commissioner Jourová's Washington visit didn't calm all anxiety surrounding the Trump Administration, evident by the MEPs resolution on April 6, 2017).

(ISPs) to seek customer permission before using their browsing history for marketing purposes.[162] While the repeal has no direct impact on the Privacy Shield or on EU data subjects, the resolution added to concerns generally about the United States' commitment to privacy.[163] Two days later, on April 6, 2017, the European Parliament passed a resolution on the adequacy of Privacy Shield protection, formally expressing concern about the Trump administration's commitment to upholding the Privacy Shield Principles.[164]

The Resolution lists a number of lingering concerns from MEPs and includes an agenda for the EC with talking points for the September 2017 Annual Review.[165] MEPs' criticisms include the voluntary nature of the agreement,[166] the unclear scope of the right to object,[167] the lack of explicit principles addressing the Privacy Shield's application to processors or agents,[168] and the small number of US companies that use an EU DPA for the dispute resolution mechanism.[169] Further, the MEPs noted that bulk collection is still possible so long as it is "as tailored as feasible" and "reasonable," which is more lax than the necessity and proportionality requirements mandated in the EU Charter.[170] The Resolution also "deplores" that bulk surveillance is still permissible for law enforcement purposes under the Privacy Shield without any explicit mode of judicial redress.[171]

---

162. *See* George Lynch, *FCC Rule Repeal Darkens EU View of U.S. Privacy Commitments*, BLOOMBERG L.: PRIVACY & DATA SECURITY (Apr. 27, 2017), https://www.bna.com/fcc-rule-repeal-n57982087235/ [https://perma.cc/28GY-7R66] (archived Sept. 23, 2017) (noting that, practically, the repeal of the rule means that ISPs can continue to sell customers' data without their consent).

163. *See id.* ("The new concerns over the commitment of the U.S. to privacy come during the ramp-up to the first annual review of the EU-U.S.").

164. *See* Resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-U.S. Privacy Shield, EUR. PARL. DOC. 2016/3018 (RSP); *see also* Press Release, European Union, Privacy Shield: MEPs alarmed at undermining safeguards in the US (Apr. 6, 2017) (noting that the resolution was introduced by the Committee on Civil Liberties, Justice & Home Affairs and passed 306 votes to 240 votes with 40 abstentions).

165. *See* Resolution of 6 April 2017, *supra* note 164 (reiterating the call on the Commission to seek clarification on the legal status of the 'written assurances' provided by the US and to ensure that any commitment or arrangement foreseen under the Privacy Shield is maintained following the taking up of office of a new administration in the United States).

166. *Id.* ¶ 3.

167. *Id.* ¶ 12.

168. *Id.* ¶ 15.

169. *Id.* ¶ 14.

170. *See id.* ¶ 16 (calling for a uniform definition of bulk surveillance linked to the European understanding of the term, where evaluation is not made dependent on selection).

171. *See id.* ¶¶ 19, 26 ("Deplores the fact that neither the Privacy Shield Principles nor the letters of the U.S. administration providing clarifications and assurances demonstrate the existence of effective judicial redress rights for individuals in the EU whose personal data are transferred to a US organisation under the Privacy

Additionally, the Resolution specifically addresses troubling US domestic policy. It characterizes the repeal of the Federal Communications Committee rule discussed above as "yet another threat to privacy safeguards in the United States."[172] Further, it "[expresses] great concern" over the NSA's "Procedures for the Availability or Dissemination of Raw Signals Intelligence Information," which permits sharing of private data without warrants amongst sixteen US agencies.[173] It also challenges the independence of the ombudsperson[174] and calls on the EC to assess the impact of President Trump's Executive Order on European citizens.[175]

The Resolution outlines points of clarification to be addressed during the Annual Review. These include: (1) confirming that the Privacy Shield will comply with the GDPR, EU 2016/679, which takes effect May 2018,[176] (2) seeking reassurances from US authorities that their written assurances will be maintained under the new administration, [177] and (3) ensuring that all mechanisms and safeguards touted by the US administration are being implemented and adequately protect data subjects.[178]

ii. EU Political Climate: Brexit

The political climate in the European Union further complicates the future of the Privacy Shield. Notably, there is uncertainty within the European Union surrounding Brexit's impact on the Privacy Shield

---

Shield Principles and further accessed and processed by US public authorities for law enforcement and public interest purposes.").

172. *Id.* ¶ 22.

173. *See id.* ¶ 23 (stating concern that an individual affected by a breach of the rules can apply only for information and for the data to be deleted and/or for a stop to further processing, but has no right to compensation).

174. *See id.* ¶ 27 (stating that the Ombudsperson mechanism set up by the U.S. Department of State is not sufficiently independent and is not vested with sufficient effective powers to carry out its duties and provide effective redress to EU individuals).

175. *See id.* ¶ 25 (calling on the Commission to assess the impact of the Executive Order on 'Enhancing Public Safety in the Interior of the United States', and in particular its Section 14 on the exclusion of foreign citizens from the protections of the Privacy Act regarding personally identifiable information, contradicting the written assurances that judicial redress mechanisms exist for individuals in cases where data was accessed by the US authorities).

176. *See id.* ¶ 31 ("Calls on the Commission to take all the necessary measures to ensure that the Privacy Shield will fully comply with Regulation (EU) 2016/679, to be applied as from 16 May 2018, and with the EU Charter.").

177. *See id.* ¶ 8 ("Reiterates its call on the Commission to seek clarification on the legal status of the 'written assurances' provided by the US and to ensure that any commitment or arrangement foreseen under the Privacy Shield is maintained following the taking up of office of a new administration in the United States.").

178. *See id.* ¶ 35 (calling on the Commission to evaluate meticulously whether the mechanisms and safeguards indicated in the assurances and clarifications by the US administration are effective and feasible).

and on data transfers coming from the United Kingdom.[179] Article 50 was triggered on March 29, 2017, which started the two-year clock for the United Kingdom to negotiate an exit deal.[180] If all goes according to plan, the United Kingdom will exit the European Union and cease to be covered under the EU-U.S. Privacy Shield. An expert in data protection from the United Kingdom postulated that the existence of the "Privacy Shield in the UK post-Brexit is largely dependent on the model adopted by the UK in its departure from the EU."[181] Some have speculated that the United Kingdom will follow Switzerland and adopt a new privacy agreement with the United States independent from the European Union.[182] Alternatively, the United Kingdom may choose to continue to act under the EU-U.S. Privacy Shield as a non-member of the European Union.[183] Under this option, US companies would be expected to comply with UK law when dealing with the personal data of UK citizens and would no longer receive a presumption of adequacy under the Privacy Shield, creating confusion about requisite compliance.[184] Thus, while Brexit is unlikely to directly impact the continuing existence of the Privacy Shield, it creates another source of uncertainty in the transatlantic data transfer arena.

---

179. *See* HM GOVERNMENT, THE EXCHANGE AND PROTECTION OF PERSONAL DATA: A FUTURE PARTNERSHIP PAPER (2017), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf [https://perma.cc/KZ56-M36N] (archived Sept. 23, 2017) (addressing UK's post-Brexit intentions to work with the EU to ensure continued data flows; notably, this paper does not mention anything about data transfers from between the UK and U.S.).

180. *See 'No turning back' on Brexit as Article 50 triggered,* BBC NEWS (Mar. 30, 2017), http://www.bbc.com/news/uk-politics-39431428 [https://perma.cc/3S2X-MHRQ] (archived Oct. 23, 2017) (noting that Prime Minister Theresa May wrote in a letter to EC President Donald Tusk of UK's intention to withdraw from the EU); Michael Wilkinson & Robert Midgley, *What is Article 50? The Only Explanation You Need To Read,* THE TELEGRAPH (Feb. 25, 2017), http://www.telegraph.co.uk/news/0/what-is-article-50-the-only-explanation-you-need-to-read/ [https://perma.cc/3DF8-UZK2] (archived Sept. 23, 2017) ("Triggering Article 50 starts the clock running. After that, the Treaties that govern membership no longer apply to Britain.").

181. Michael Nesheiwat, *Doing Business Abroad? Brexit and Its Implications On Your Data Practices*, 34 NO. 7 WESTLAW J. COMPUTER AND INTERNET 1, 2–3 (Sept. 9, 2016).

182. *See id.* (following the example of Iceland, Liechtenstein and Norway).

183. *See* McCann FitzGerald, *Brexit: Data Protection and EU-UK Data Flows*, LEXOLOGY (Feb. 23 2017), http://www.lexology.com/library/detail.aspx?g=dff5c8b6-a024-4e8d-8d0a-9bc417942efa [https://perma.cc/Q5CV-BD6R] (archived Sept. 23, 2017) ("[T]he UK Government publicly stated that its Brexit goals include ensuring that, from the Exit Date, crossborder flows of personal data between the UK and the EU could continue on an 'unhindered' and 'uninterrupted' basis.").

184. *See* Nesheiwat, *supra* note 181, at 2–3 ("[M]any U.S. companies that do some business in the EU, or otherwise interact with EU customers, must comply with EU data privacy laws.").

## V. LOOKING TOWARD THE FUTURE: THE POSSIBLE OUTCOMES FOR THE EU-U.S. PRIVACY SHIELD

Unfortunately, advocates and opponents of the Framework have no crystal ball to help predict the ultimate fate of the Privacy Shield. The agreement has faced opposition every step of the way. Yet that opposition has coexisted with a universal understanding of the importance of transatlantic trade between the European Union and the United States. Rather than providing an unsubstantiated guess as to the outcome, this Note recognizes the challenges the agreement may face in coming years and explores potential alternatives to the Framework as it exists today.

### A. *First Privacy Shield Challenge: Annual Joint Review*

On September 18 and 19, 2017 in Washington, D.C., EU regulators had the opportunity to challenge the Privacy Shield for the first time during the inaugural annual joint review by the EC and the DOC. [185] In addition to the members of the EC and the DOC, participants from the EU included: members of the WP29 and the European Data Protection Supervisor; and from the US: representatives from the FTC, the DOT, the Department of State, the ODNI, and the DOJ, as well as the acting Privacy Shield ombudsperson.[186]

Prior to the inaugural review, the EC surveyed the public opinion to identify concerns and discussion points to address during the September meeting. [187] The EU Commissioner circulated questionnaires to companies that have certified under the Privacy Shield, trade associations, and other interest groups, setting a July 5,

---

185. David J. Bender, *First Annual Privacy Shield Review Will Comprehensively Assess Framework*, THE NAT'L L. REV. (May 17, 2017), https://www.natlawreview.com/article/first-annual-privacy-shield-review-will-comprehensively-assess-framework [https://perma.cc/Y2L6-B89Z] (archived Oct. 8, 2017).

186. Report from the Commission to the European Parliament and the Council on the First Annual Review of the Functioning of the EU-U.S. Privacy Shield, at 3, COM(2017) 611 final (Oct. 18, 2017) [hereinafter Report on First Annual Review]; *see also id.* (noting that regulators both in the U.S. and EU are expected to closely scrutinize the first year of Privacy Shield operation).

187. *EU Commission Issues Questionnaire in Preparation for Annual Review of Privacy Shield*, HUNTON & WILLIAMS LLP: PRIVACY AND INFO. SECURITY L. BLOG (June 5, 2017), http://www.lexology.com/library/detail.aspx?g=4313223e-c6a7-4b9a-bf8a-32a3d6d73c20 [https://perma.cc/ZC3C-DURA] (archived Sept. 23, 2017); *see also* Bender, *supra* note 185 (noting that regulators plan to solicit information from Privacy Shield stakeholders, including companies that certify under the Framework and others interested parties).

2017 submission deadline for responses.[188] Prior to the review, the agreement's execution has effectively been stayed for a year, thus the September meeting was the first opportunity for invalidation.[189]

Following the review, the EC and the DOC issued a joint statement stating that the two "share an interest in the Framework's success and remain committed to continued collaboration to ensure it functions as intended."[190] On October 18, 2017, the EC issued its conclusion that the United States "continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield," meaning that the Privacy Shield provides the requisite level of protection for EU data under the Directive.[191] This is a significant holding considering many privacy experts in the European Union and the United States assumed the contrary.[192] However, this adequacy holding does not necessarily mean that the Privacy Shield is a perfect framework in the eyes of the EC or the United States. Rather, the decision likely stands as recognition that invalidation of the Framework entirely would be more harmful than working within the current arrangement and editing areas of continued concern. The Commission conceded this in its report listing a number of recommendations that would ensure the continuing vitality of the Framework.[193] Implicit in the EC's holding is the recognition that

---

188. *See EU Commission Issues Questionnaire in Preparation for Annual Review of Privacy Shield*, *supra* note 187 (stating that questionnaires include a variety of questions sought to gather information about how the certification process has gone for Privacy Shield certified companies, as well as gauge sentiments surrounding upholding of US commitments and US domestic law impact on the vitality of the agreement).

189. *See* Aaron Souppouris, *EU Will Watch Privacy Shield For a Year Before Challenging*, ENGADGET (July 27, 2016), https://www.engadget.com/2016/07/27/eu-data-protection-privacy-shield-annual-review/ [https://perma.cc/ZE7D-LUSV] (archived Sept. 23, 2017) ("European regulators have announced that Privacy Shield will not be challenged until its first annual review.").

190. Press Release, U.S. Sec'y of Commerce and EU Comm'r for Justice, Consumers and Gender Equality, Joint Press Statement on the EU-U.S. Privacy Shield Review (Sept. 21, 2017) (recognizing that the "Privacy Shield raised the bar for transatlantic data protection by ensuring that participating companies and relevant public authorities provide a high level of data protection for EU individuals").

191. Report on First Annual Review, *supra* note 186.

192. *See US Surveillance Makes Privacy Shield Invalid*, HUM. RTS. WATCH (July 26, 2017 12:01 AM EDT), https://www.hrw.org/news/2017/07/26/us-surveillance-makes-privacy-shield-invalid [https://perma.cc/5YXX-B6EX] (archived Oct. 20, 2017) (Co-Director of the U.S. Program at Human Rights Watch urged the EC to "take a ... hard look at the realities of US surveillance and take action to make sure no one's rights are sacrificed in the name of political or economic convenience."); Natasha Lomas, *Europe's DP Chiefs Fire Warning Shots Ahead of First EU-US Privacy Shield Review*, TECH CRUNCH (June 13, 2017), https://techcrunch.com/2017/06/13/europes-dp-chiefs-fire-warning-shots-ahead-of-first-eu-us-privacy-shield-review/ [https://perma.cc/9HFA-9QA8] (archived Oct. 22, 2017) (WP29 concerns included commercial aspects and law enforcement and national security issues); *see also WP 29 Statement*, *supra* note 115, at 1 (WP29 expressed a number of concerns about the adequacy of Privacy Shield).

193. Recommendations include:

while the Privacy Shield today is sufficient under EU law, absent changes in the future taking heed of the recommendations, the Framework may not survive future reviews. In a press release issued with the Report, the EC stated that it will collaborate with US authorities to ensure that the recommendations are followed and that the EU-U.S. Privacy Shield continues to work effectively.[194]

Ultimately, while the annual review and the EC's holding of adequacy is a positive development for the EU-U.S. Privacy Shield, it does not immunize the Framework from future challenge. The transatlantic data sharing agreement will face continued scrutiny during future annual reviews between the EC and DOC, as well as the threat of review by the CJEU.[195]

### B. *Upcoming Privacy Shield Challenge: Judicial Action by the CJEU*

The CJEU itself may speak on the adequacy of the Privacy Shield, as it did with the predecessor Safe Harbor. Over the past few years, the CJEU has become intimately involved in questions of security and data protection.[196] At the time of this Note's submission, opponents

---

- 2.1 Companies should not be able to publicly refer to their Privacy Shield certification before the certification is finalized by the DOC.
- 2.2 Proactive and regular search for false claims by the DOC
- 2.3 Ongoing monitoring of compliance with the Privacy Shield Principles by the DOC
- 2.4 Strengthening of awareness raising
- 2.5 Improve coordination between enforcers
- 2.6 Study on automated decision-making
- 2.7 Enshrine the Protections of the PPD-28 in the Foreign Intelligence Surveillance Act
- 2.8 Swift appointment of the Privacy Shield Ombudsperson
- 2.9 Swift appointment of the members of the PCLOB and release of the PCLOB report on PPD-28
- 2.10 More timely and comprehensive reporting of relevant developments by U.S. Authorities

*See* Report on First Annual Review, *supra* note 186 (in conjunction with their holding of adequacy, the EC also recognizes that the "practical implementation of the Privacy Shield framework can be improved in order to ensure that the guarantees and safeguards provided therein continue to function . . . .").

194. Press Release, European Commission, EU-U.S. Privacy Shield: First review shows it works but implementation can be improved (Oct. 18, 2017), http://europa.eu/rapid/press-release_IP-17-3966_en.htm [https://perma.cc/SP93-F6JW] (archived Oct. 23, 2017).

195. *See* David Spencer, *Privacy Shield Passes First Annual Review But Its Long-Term Future Remains Uncertain*, VPN COMPARE (Sept. 25, 2017), https://www.vpncompare.co.uk/privacy-shield-passes-first-annual-review-but-its-long-term-future-remains-uncertain/ [https://perma.cc/HS8W-ZGSN] (archived Oct. 20, 2017) (recognizing that the future of Privacy Shield is unknown and that is a significant consideration for why many companies are reluctant to certify under the Framework).

196. *See* Lauren Cerulus & Nicolas Hirst, *Europe's Gavel Comes Down Hard on Tech*, POLITICO (Oct. 9, 2016), https://www.politico.eu/article/european-court-of-justice-

have filed two legal challenges to the Privacy Shield's adequacy. First, Digital Rights Ireland, the privacy advocacy group that helped bring the suit that invalidated Safe Harbor, has brought a complaint in the Luxembourg General Court (a lower court of the CJEU).[197] It asserts that the Commission's adequacy decision, which approved and adopted the Privacy Shield, should be invalidated because the agreement fails to protect the privacy rights of EU citizens.[198] The second complaint is by La Quadrature du Net, a French civil liberties campaign group, asking for a similar annulment of the Privacy Shield.[199] Both groups must prove that the Privacy Shield is "of direct and individual concern" to the groups in order to have standing to bring their complaints.[200] Since both complaints are brought by civil liberties organizations, this may be challenging.

Assuming that these organizations satisfy standing and other procedural requirements, it may still take several years before the question of the adequacy of the Privacy Shield reaches the CJEU.[201] Further, even if the CJEU does hear such a case, there is no guarantee that the court will invalidate the Privacy Shield. The CJEU could

---

tech-cases-uber-airbnb/ [https://perma.cc/3W9U-4Z6Y] (archived Sept. 23, 2017); *see, e.g.*, Case T-738/16, La Quadrature du Net and Others v. Comm'n, 2017 E.C.R. 006/49; Case C-203/15, Tele2 Sverige AB v. Post- och telestyrelsen, 2017 E.C.R 053/13; Case T-670/16, Digital Rights Ireland v. Comm'n, 2016 E.C.R. 410/37; Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, et al. 2013 E.C.R.

197. *See Privacy Shield Challenged,* WHITE & CASE (Nov. 2, 2016), http://www.whitecase.com/publications/alert/eu-us-privacy-shield-challenged [https://perma.cc/C8VN-GWFL] (archived Sept. 23, 2017) ("Digital Rights Ireland ("DRI") has filed the challenge (case number T-670/16) with Europe's second highest court, the Luxembourg-based General Court, which is the lower court of the CJEU."); Lauren Cerulus, *Privacy Shield Data Agreement Challenged Before EU Court Digital Advocacy Group Attempts to Get Agreement Annulled,* POLITICO (Oct. 27, 2016), http://www.politico.eu/article/privacy-shield-data-agreement-challenged-before-ecj/ [https://perma.cc/CCZ7-6DLP] (archived Sept. 23, 2017) ("Privacy advocacy group Digital Rights Ireland has challenged the EU-U.S. data transfer agreement 'privacy shield' before the EU's General Court.").

198. Digital Rights Ireland, 2016 E.C.R. 410/37 ("[A]lleging that the contested decision is not in accordance with Article 25(6) of Directive 95/46, read in light of Articles 7, 8, 47 of the Charter of Fundamental Rights of the European Union."); *see also Privacy Shield Challenged*, *supra* note 197; Cerulus, *supra* note 197.

199. *See* La Quadrature du Net and Others, 2017 E.C.R. 006/49 ("declaring Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 to be contrary to Articles 7, 8, and 47 of the Charter of Fundamental Rights of the European Union"); Peter Sayer, *A Second Privacy Shield Legal Challenge Increases Threat to EU-US Data Flows*, PCWORLD (Nov. 3, 2016), https://www.pcworld.com/article/3138196/cloud-computing/a-second-privacy-shield-legal-challenge-increases-threat-to-eu-us-data-flows.html [https://perma.cc/6QF3-DF68] (archived Sept. 24, 2017).

200. Justine Brown, *Second Group Seeks to Annul Privacy Shield*, CIO DIVE (Nov. 4, 2016), https://www.ciodive.com/news/second-group-seeks-to-annul-privacy-shield/429745/ [https://perma.cc/3X35-6Z7J] (archived Sept. 24, 2017); Sayer, *supra* note 199.

201. *Privacy Shield Challenged*, *supra* note 197.

accept the framework, which would confirm and strengthen the European Union's adequacy decision, or issue guidance regarding any aspects it finds problematic.[202] While the CJEU is unlikely to invalidate the framework in the immediate future, the fact that there are already two challenges against it suggests an uncertain future for transatlantic personal data transfers between the European Union and the United States. In light of the weaknesses this Note has identified in the Privacy Shield and the propensity of the CJEU to invalidate it, the Privacy Shield is not a secure mechanism for trade in its current state.[203]

### C. *Alternative Mechanisms to the Privacy Shield*

While the focus of this Note has been the Privacy Shield, it is not the only mechanism by which transatlantic transfer of personal data between the European Union and the United States can be achieved. If the Privacy Shield is invalidated via Annual Joint Review or by the CJEU, or if the European Union and the United States decide that a blanket adequacy framework is unattainable, there are alternative contrivances available to US companies.[204] Absent a framework like the Privacy Shield, data transfers can still validly occur between the European Union and the United States through three mechanisms: (1) unambiguous consent by the data subject to the transfer;[205] (2) Standard Contract Clauses (SCCs), which are standard form, non-negotiable agreements that impose contractual obligations for data protection and are available on the EC's website;[206] and (3) Binding Corporate Rules (BCRs), which are binding self-governance rules for multinational corporate groups that may be approved by national DPAs upon a finding that the group's protection policy is sufficient and applies to all group members worldwide.[207] Notwithstanding the availability of these alternative mechanisms, many US companies still

---

202. *See* IRION ET AL., *supra* note 63, at 11–12 (detailing the powers of the CJEU).

203. *See supra* Part IV.C (explaining the weaknesses that still remain within the Privacy Shield).

204. *See* Jeff Stone, *Privacy Shield Seems Safe, but Have a Backup Plan*, WALL ST. J. (Mar. 22, 2017) https://www.wsj.com/articles/privacy-shield-seems-safe-but-have-a-backup-plan-1490214214 [https://perma.cc/APH7-C8QR] (archived Oct. 27, 2017) (recommending that companies that certify under the Privacy Shield also use model contract clauses as a back up plan).

205. *See* Lisa Mays, *The Trickle Down Effect of Privacy Shield Uncertainty: Fluctuating Lines for Anti-Bribery Compliance*, 19 No. 10 J. INTERNET L. 1, 9 (2016) (explores the various ways that absent a data sharing agreement, companies can permissible transfer and use EU data, including "a company [can] obtain consent to the transfer").

206. Neal Cohen, *The Public Follies: A Look Back at the CJEU's Invalidation of the EU/US Safe Harbor Framework*, Case Notes, 1 EUR. DATA PROT. L. REV. 240, 243 (2015); Gutterman, *supra* note 61, at 1.

207. Cohen, *supra* note 206, at 243; Gutterman, *supra* note 61, at 1.

prefer a comprehensive approach that allows certification under the Privacy Shield.[208]

While unambiguous consent would grant US companies greater flexibility in negotiating with EU data subjects, it would come at a high administrative cost.[209] Each data subject must fully and knowingly acquiesce to the transfer on an individual basis, which is much more taxing than simply requiring one-time self-certification and annual recertification that deems all of a company's EU data transfers permissible.[210] The Directive defines consent as a "specific and informed indication of a person's wishes for data to be processed," which is "unambiguously" and "freely given," without "compulsion or an act of deceit."[211] In certain circumstances, like data transfers for the purpose of human resources or employment related activities, it is presumed that consent may not be properly given in light of the power imbalance of the parties.[212] Further, according to the WP29, a data subject's consent "is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfer for the processing in question."[213]

While SCCs do not suffer from the administrative costs of attaining individual data subjects' consent, they lack the flexibility required to negotiate in practice.[214] SCCs are presumed permissible because the EC has issued explicit language for contracts that meet

---

208. *See* WEISS & ARCHICK, *supra* note 72 (stating that many US industries maintain that the US approach to data privacy is more nimble than the EU's policy and thus urge comprehensive data protection legislation).

209. Lothar Determann, Brian Hengesbaugh & Michaela Weigl, *The EU-U.S. Privacy Shield Versus Other EU Data Transfer Compliance Options*, BLOOMBERG BNA (Sept. 12, 2016), https://www.bna.com/euus-privacy-shield-n57982076824/ [https://perma.cc/4WC6-8KCQ] (archived Sept. 24, 2017).

210. *Id.*

211. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, art. 2, 1995 O.J. (L 281) 31.

212. *See* Commission Regulation 2016/679 of April 27, 2016, General Data Protection Regulation, 2016 O.J. (L 119) 2 (noting that under GDPR consent is held out to be valid only "if freely given, specific, informed and unambiguous, and can be revoked at any time"); Determann et al., *supra* note 209 (stating it is harder to ensure uniform consent in the human resources context because the lack of direct contact between parties does not induce data subjects to grant consent); The Honorable Julie Brill, U.S. Fed. Trade Comm'n, Presentation to the European Institute: Safe Harbor: The Schrems Case and What Comes Next (Oct. 20, 2015) (GDPR requires that companies expressly disclose the risks of international data transfers; note that human resource-related companies comprise 50% of the Safe Harbor participants).

213. Article 29 Data Protection Working Party, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* 11 (European Comm'n Directorate, General of Justice, Freedom, and Security, Working Paper No. 114, 2005), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf [https://perma.cc/ZX4V-7BBY] (archived on Sept. 24, 2017).

214. *Id.*; GERLACH ET AL., *supra* note 70, at 6.

the requisite standards to protect EU data subjects.[215] For businesses to receive the presumption of adequacy, they cannot amend the SCC's provisions regarding data subjects' privacy rights in any significant manner.[216] While, technically speaking, companies have the right to edit the SCC as they wish, such alterations would be subject to review by every EU member state and may trigger additional requirements to notify or seek further approval from local EU authorities—requirements that are not only costly, but eliminate the advantages of using the SCC in the first place.[217] Conversely, certification under a framework like the Privacy Shield enables companies to tailor a privacy policy to their specific purpose without sacrificing efficiency.

BCRs cover all direct and onward data transfers within a company, including those to its subsidiaries or affiliates, and thereby provide intragroup coverage.[218] However, BCRs do not protect onward data transfers to unaffiliated entities outside the company in question, including customers, suppliers, distributers, service providers, civil litigants, and government agencies.[219] This is troublesome because continued compliance is contingent upon companies either having those entities agree to BCRs or implementing other compliance mechanisms to protect the data—a requirement more burdensome on US companies than the self-certification process and onward transfer requirements under the Privacy Shield.

Further, the implementation process can take up to two years, and the BCR specification requirements compel companies to include many details about (1) the company's desire to transfer (including its location, contact information, and business structure), (2) the data transfers or set of data transfers in which the company wishes to engage (including what kind of EU data will be implicated and what type of data subjects), and (3) the type and purpose of processing.[220] Because of the onerous approval process, BCRs are very expensive to put in place—only one hundred companies globally and thirty in the United States have implemented this mechanism.[221] Again, compared

---

215. Determann et al., *supra* note 209; WEISS & ARCHICK, *supra* note 72, at 14.

216. *See* Commission Regulation 2016/679 of 27 April 2016, *supra* note 212 at 6 (Presumption of adequacy under the SCC when do not alter).

217. Presumptively use SCC because don't want to have to seek out approval of every EU member state, but if amendment to SCC in way implicates data subject privacy right have to effectively do what you were avoiding.

218. GERLACH ET AL., *supra* note 70, at 6; WEISS & ARCHICK, *supra* note 72, at 14; Determann et al., *supra* note 209.

219. *See* Commission Regulation 2016/679, *supra* note 212, at 2 (explaining in Art. 47, paragraph 2 that a company might want to engage in onward transfer of data to an entity that is not an affiliate of the company covered under the BCR); Determann et al., *supra* note 209.

220. WEISS & ARCHICK, *supra* note 72, at 14; Determann et al., *supra* note 209.

221. Philip L. Gordon & Tahl Tyson, *What Does the European Court of Justice's Invalidation of the U.S.-EU Safe Harbor Framework Mean for U.S.-Based Multinational*

to the Privacy Shield's annual self-certification process, BCR authorization is much more taxing.[222]

Further, there is a question as to the continuing adequacy of both SCCs and BCRs as alternative mechanisms for compliance. [223] Following the Schrems case, the Irish Data Protection Commissioner (DPC) noticed that Facebook was continuing to transfer personal data in reliance on SCCs.[224] The Irish DPC announced its intention to initiate a direct challenge to the validity of EU SCCs, arguing that SCCs suffer from the same weaknesses that led to the invalidation of Safe Harbor.[225] The hearing before the Irish High Court lasted over five weeks, from February 7, 2017 to March 15, 2017, with the Irish DPC asking the High Court to seek a referral to the CJEU on the issue of the validity of SCCs.[226] After closing arguments on March 15, 2017, the High Court reserved judgment for a later date. On October 3, 2017, High Court Judge Justice Caroline Costello agreed with the Irish DPC about the questionable status of SCCs, referring the issue of SCCs' validity to the CJEU. [227] Some scholars have noted that this rationale for challenging SCCs may call the adequacy of the BCRs into question

---

*Employers?*, LITTLER INSIGHT (Oct. 7, 2015), https://www.littler.com/publication-press/publication/what-does-european-court-justices-invalidation-us-eu-safe-harbor [https://perma.cc/HT5L-UA22] (archived Sept. 24, 2017).

222. *See supra* Part III.A (detailing how a U.S. company must comply under the Safe Harbor Agreement).

223. *See* Determann et al., *supra* note 209 (noting that these alternative mechanisms could be updated with more specificity or could be complexly eliminated under the GDPR. It is speculated that SCCs applicable to both processors and controllers, which prior to GDPR contained more generalized descriptions, will be updated for specific in reaction to the new data protection regime).

224. *Explanatory Memorandum, Update on Litigation Involving Facebook and Maximilian Schrems*, DATA PROTECTION COMMISSIONER (March 16, 2017), https://www.dataprotection.ie/docs/01-02-2017-Update-on-Litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm [https://perma.cc/8RVW-KF83] (archived Sept. 24, 2017).

225. *See* SIDLEY, *supra* note 78 (discussing the complaint and suggesting that "invalidation of model contracts could cause a huge shake up of global data transfers because following the invalidation of Safe Harbor, model contracts are the most popular international data transfer tool").

226. *See Update on Litigation Involving Facebook and Maximilian Schrems*, *supra* note 224 (listing the 5 expert witnesses on U.S. law that testified during the hearing); Natasha Lomas, *Legal Challenge to Facebook EU-US Data Transfer Mechanism Kicks Off In Ireland*, TECHCRUNCH (Feb. 7, 2017), https://techcrunch.com/2017/02/07/legal-challenge-to-facebook-eu-us-data-transfer-mechanism-kicks-off-in-ireland/) [https://perma.cc/9C6T-YCTL] (archived Sept. 24, 2017).

227. *See* Case 2016 No. 4809 P., Data Protection Comm'r v. Facebook Ireland Limited and Maximillian Schrems, §333 (Oct. 3, 2017), https://iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf [https://perma.cc/3CBQ-9RB2] (archived Oct. 19, 2017) (Justice Costello cited the need for "consistency and clarity" in the application of the Directive).

as well.[228] Irrespective of the ultimate holding, it is clear that SCCs and BCRs are not more stable mechanisms than the Privacy Shield framework.

Ultimately, while alternatives to the Privacy Shield framework do technically exist, closer analysis of these alternatives suggests that they may not offer measurable advantages that would justify abandoning the self-certification framework. Additionally, certification under the Privacy Shield framework provides unique benefits for companies, undermining arguments for abandoning the framework altogether. Not only does certification provide a presumption of adequate privacy protection that satisfies the EU Data Protection Directive, [229] but this presumption is universally binding on all member states. Member states are obligated to honor the adequacy decision of the EC. Thus, no matter where in the European Union the personal data originates, US companies are able to legally use the data.[230] An additional benefit for companies is the explicit nature of the compliance regime: the conditions under the Privacy Shield are transparent and cost-effective in comparison to the alternative mechanisms for compliance (e.g., consent, BCRS, and SCCs).[231]

### D. *Privacy Shield Reimagined: EU-U.S. Business Privacy Shield*

Rather than discarding the framework entirely, this Note proposes that the basic integrity of the Privacy Shield should remain intact, but the role of the US government within the framework should be removed. By keeping the basic self-certification structure and the Privacy Shield Principles, this approach would allow the European Union and the United States to maintain the progress that the Privacy

---

228. *See* Stewart Room, *The Challenge to Safe Harbour- A Totem For Something Much More Fundamental*, PWC (Oct. 1, 2015), http://pwc.blogs.com/data_protection/2015/10/the-challenge-to-safe-harbour-a-totem-for-something-much-more-fundamental-.html [https://perma.cc/NCV4-DFSQ] (archived Sept. 24, 2017) (criticizing the notion that BCRs provide a greater assurance of adequacy that Safe Harbor and predicting that BCRs are "vulnerable" to challenge).

229. *See supra* Part II.B. (while it still remains to be seen if this same presumption of adequacy applies now that Directive will be replaced in 2018, with the General Data Protection Regulation, their extraterritorial provisions both require an "adequacy" standard).

230. *See Benefits of Participation*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=Benefits-of-Participation (last visited Oct. 8, 2017) [https://perma.cc/CT6Q-97V6] (archived Sept. 24, 2017) (this implicitly does away with EU Member State requirements for prior approval of data transfers).

231. *Id. But see* Determann, et al., *supra* note 209 (noting that the Privacy Shield Framework still lacks real stability for US Businesses, as the Framework can be changed annually and data subjects are permitted to revoke consent at any time).

Shield has achieved, including more stringent data protections, greater redressability for EU data subjects, and oversight mechanisms.[232]

1. Regulatory Examples: Fair Labor Association and Worker's Rights Consortium

The concept of transnational regulation vis-á-vis a public-private arrangement is not novel in other areas of international and transnational law—examples in other industries include investor–state arbitration,[233] public-private infrastructure partnerships,[234] and corporate self-regulation. [235] Corporate self-regulation within the garment and apparel industry provides two prominent examples of private-public regulatory schemes that have accomplished what this Note suggests for the EU-U.S. Privacy Shield.

The first example is the Fair Labor Association (FLA), a collaborative cohort of universities, civil rights organizations, and companies that are committed to safeguarding workers' rights globally. [236] The organization requires companies who join the organization to commit to upholding the FLA Workplace Code of Conduct and to establish monitoring processes to insure internal

---

232. *See supra* Part IV.B (referencing the improvements in Privacy Shield from its predecessor).

233. Many of the reasons that diplomatic protection is inadequate to investors, similarly describe issues involving the US Government's participation in Privacy Shield: the investor is dependent on the political discretion of investor's government (just as US businesses and the EU are dependent on the enforcement and administration of Privacy Shield by US agencies); the government may refuse to help the investors (US intelligence agencies can push EU data subjects rights aside in the name of public safety or the public interest); and diplomatic protection can be discontinued at any time (just as US agencies can abandon their commitments in Privacy Shield without any legal repercussion). In just the same way that international investment law enabled investors to more efficiently protect their foreign investments by giving them a mechanism for redress, the proposed re-structuring of the Privacy Shield to eliminate the dependency on government enforcement to protect EU data subject rights allows for a more effective protection of EU data subjects by US businesses. *See* C.L. Lim & Jean Ho, *International Investment Arbitration*, OXFORD BIBLIOGRAPHIES (last modified April 28, 2016), http://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0135.xml [https://perma.cc/Z2WX-XV8Y] (archived Sept. 24, 2017).

234. *What are Public Private Partnerships?* WORLD BANK GROUP, http://ppp.worldbank.org/public-private-partnership/overview/what-are-public-private-partnerships [https://perma.cc/A73T-9SYF] (archived Sept. 24, 2017).

235. *See generally* Rhys Jenkins, *Corporate Codes of Conduct: Self Regulation in a Global Economy*, UNRISD (April 1, 2001), http://www.unrisd.org/80256B3C005BCCF9/search/E3B3E78BAB9A886F80256B5E00344278 [https://perma.cc/ALY8-X5JT] (archived Sept. 24, 2017) (discussing the proliferation of corporate codes of conduct and the increased emphasis on corporate responsibility in both the U.S. and abroad during the 1990s).

236. *See About Us*, FAIR LABOR ASS'N, http://www.fairlabor.org/about-us (last visited Oct. 8, 2017) [https://perma.cc/TFL3-5LPP] (archived Sept. 24, 2017) (detailing the organizational structure and purpose of the Fair Labor Association).

compliance.[237] The threat of random factory inspection and publication of all factory audits provides accountability for companies that opt in to the FLA.[238] These features force participating companies to uphold the Workplace Code of Conduct in order to continue doing business in the market.[239] Beyond ensuring compliance, FLA focuses on creating innovative solutions for labor issues, allowing all interested parties to participate.[240]

Another example of corporate self-regulation is the Worker Rights Consortium (WRC), an independent labor rights organization that specializes in global monitoring of factory working conditions.[241] The organization includes 186 colleges and universities in the United States and abroad that are committed to making sure that university apparel is produced in factories that respect the labor rights of their workers.[242] The WRC's responsibilities include investigating and documenting violations, and reporting violations to universities.[243] The threat of losing university and collegiate clients motivates apparel manufacturers to comply; by this process, the WRC uses market forces to ensure compliance.[244]

---

237. *See generally FLA Workplace Code of Conduct and Compliance Benchmarks*, FAIR LABOR ASS'N, http://www.fairlabor.org/our-work/labor-standards (revised Oct. 5, 2011) [https://perma.cc/PN99-XV6D] (archived Sept. 24, 2017) (detailing the specific terms of the FLA Workplace Code of Conduct); FAIR LABOR ASS'N, CHARTER DOCUMENT 21–29 (last modified Feb. 12, 2014), http://www.fairlabor.org/sites/default/files/fla_charter_2-12-14.pdf [https://perma.cc/ATK4-ZPQD] (archived Sept. 24, 2017).

238. CHARTER DOCUMENT, *supra* note 237, at 16, 24.

239. *See Accreditation*, FAIR LABOR ASS'N, http://www.fairlabor.org/accreditation (last visited Oct. 8, 2017) [https://perma.cc/LD8Y-TVWB] (archived Sept. 24, 2017) (currently, compliance programs of 25 affiliated companies are accredited by the FLA, including Nike, Patagonia, New Balance, Puma, and Gildan Activewear, Inc., to name a few).

240. FLA has supported various studies including hybrid corn production in Argentina, creation of the PREPARE project to encourage worker representation in Bangladesh, and the FLA Fashion Project which works to labor standards are being upheld in global supply chain. *See About Us*, *supra* note 236 (detailing goals of the Fair Labor Association).

241. *See* Don Wells, *The Workers Rights Consortium*, in BUSINESS REGULATION AND NON-STATE ACTORS 239 (Darryl Reed et al. eds., 2012) (explaining the Russell Athletic apparel closing of a Honduran Plant and WRC involvement in the investigation report on the plant); *Mission*, WORKERS RIGHTS CONSORTIUM, http://www.workersrights.org/about/ (last visited Oct. 8, 2017) [https://perma.cc/QF8V-F9GF] (archived Oct. 8, 2017) (explaining the organization structure and purpose of the Workers Rights Consortium).

242. *Mission*, *supra* note 241; *see also* Wells, *supra* note 241, at 240, 242 (noting that the WRC has been integral in raising "consumer awareness of global sweatshops").

243. *Mission*, *supra* note 241; Wells, *supra* note 241, at 240, 242.

244. *Mission*, *supra* note 241.

2. Replacement of US Government Role with a Data Privacy NGO

Following the example of both the FLA and the WRC, the administration and enforcement responsibilities within the Privacy Shield, previously filled by a variety of US agencies, would be delegated to a Data Privacy NGO. This public-private arrangement would maintain all of the substantive protections and processes of the Privacy Shield, but replace the US government with an NGO that would serve as a supervisory entity. The Data Privacy NGO would ensure companies' compliance with the Privacy Shield Principles and oversee the redress process for violations of EU data subjects' privacy rights, similar to the monitoring and investigation functions of the FLA and the WRC.[245] Just as corporations who opt into the requirements under the FLA and the WRC are held accountable by market forces, US businesses will commit to compliance, irrespective of the supervisory presence of US agencies, because of their self-motivated desire for reliable and sufficient access to EU data.

The Privacy Shield NGO's board should be diverse and should include more than just self-interested representatives of US businesses seeking EU personal data.[246] It should also include individuals who work in privacy NGOs, both in the European Union and the United States, and EU DPAs or other members of the EC.[247] This membership is important to preserve the lines of communication between the European Union and the United States and to provide for greater collaborative action to supplement the annual review required under the new Privacy Shield Framework. Board membership should also include technology experts within the data privacy field for two reasons: (1) to serve as a resource for determining whether standards for US corporations are reasonable, and (2) to ensure that the Privacy Shield Framework is evolving with current technology.

---

245. *See About Us*, *supra* note 236 (explaining the structure and role of the FLA); Wells, *supra* note 241 (explaining the role of the WRC in the closing of a Honduran Russell Athletic Plant).

246 *See* Wells, *supra* note 241, at 242 (stating that the WRC Board does not include corporate representatives for fear of capture by the apparel industry, a common criticism of the FLA's factory monitoring proposal, which would have allowed companies to have notice and choice of monitor prior to factory inspection). This Note proposes that the Privacy Shield NGO Board can and should include a small, minority corporate representation. However, the inclusion of EU and US privacy and technology experts will ensure that the Board considers all perspectives, creating workable standards.

247. To protect WRC capture by the apparel industry, governance is based on three constituencies (United Students Against Sweatshops, labor rights experts, and member universities), each electing five directors to sit on the Board. *See* Wells, *supra* note 241, at 242.

### 3. Advantages to Data Privacy NGO Enforcement of EU-U.S. Business Privacy Shield

Transforming the Privacy Shield into a public-private transnational agreement eliminates the weaknesses that could potentially invalidate the agreement. When looking at the weaknesses and the challenges that face the Privacy Shield, surveillance remains a cancerous element.[248] While the Privacy Shield places some limitations on US surveillance and collection of EU personal data,[249] it lacks any concrete assurance against indiscriminate collection and processing—especially within the context of a less privacy-protectionist administration.[250] This serves to critically threaten the future of the EU-U.S. Privacy Shield.[251]

Additionally, when it invalidated Safe Harbor, the CJEU expressed concern that nothing bound the US government to its promises under the Framework.[252] Jan Phillip Albrecht, a leading member of the European Parliament on data privacy issues, expressed similar concerns about the new Privacy Shield agreement, noting its lack of "legally binding improvements."[253] Restructuring the Privacy Shield as a public-private agreement that relies on corporate self-regulation provides a solution to both concerns of surveillance[254] and the lack of binding commitments[255] from US agencies: rather than attempting to "legally bind" US agencies to enforce privacy rules on private corporations, this framework would rely on market forces to naturally incentivize such corporations to comply.

Though some might criticize a public-private restructuring of the Privacy Shield for punting the surveillance issue to the side, it is out of necessity. Rather than let the problem of the permissible level of US surveillance poison the rest of the Privacy Shield, the solution proposed here chooses to write out the potential cause of invalidation. Thus, the question of US government surveillance on EU citizens should be

---

248. *See WP 29 Statement*, *supra* note 115 (emphasizing that surveillance is still an issue under Privacy Shield); *see generally supra* Part IV.C.1.

249. *See* Litt, *supra* note 118.

250. *See WP 29 Statement*, *supra* note 115 (noting that surveillance is still a concern under Privacy Shield); *see generally supra* Part IV.C.1.

251. *WP 29 Statement*, *supra* note 115.

252. *See supra* Part III.B (noting that one of the CJEU's criticisms when invalidating the EU-U.S. Safe Harbor was the absence of a mechanism binding the U.S. government to uphold their side of the bargain).

253. Natasha Lomas, *Europe and US Seal 'Privacy Shield' Data Transfer Deal to Replace Safe Harbor*, TECH CRUNCH (Feb. 2, 2016), https://techcrunch.com/2016/02/02/europe-and-us-seal-privacy-shield-data-transfer-deal-to-replace-safe-harbor/ [https://perma.cc/U8K4-ZD4W] (archived Sept. 24, 2017).

254. *See supra* Part IV.C.1 (describing the continued issue of protections from surveillance by U.S. Intelligence Authorities under the EU-U.S. Privacy Shield).

255. *See supra* Part IV.C.2.i (describing how the lack of binding commitments from the U.S. is particularly troubling in the new Trump Administration).

handled separately and at a different time between the United States and the European Union. The data sharing agreement need not sink because of the periphery issue of surveillance.

While a public-private arrangement eliminates the need to directly tackle the surveillance issue, the Privacy Shield NGO could take other remedial actions to indirectly address surveillance.[256] First, the Privacy Shield NGO can work with US businesses to reduce opportunities for US government surveillance, including tightening up the data retention principle so that US companies do not possess EU data for long stretches of time.[257] This would reduce the chance that US intelligence authorities could compel production. [258] Further, appointing data protection experts to the NGO's Board would encourage innovation with regard to protections against indiscriminate surveillance by intelligence authorities.[259]

A common complaint about corporate self-regulation is that it is industry-funded.[260] A Privacy Shield NGO will not be immune to this critique. But this Note proposes that the combination of US businesses' desire to engage in the market of EU personal data and the checks on self-interested action by a diverse board would limit the risk that the NGO will become an agent of the industry rather than remain an independent supervisory entity.

Ultimately, an EU-U.S. Business Privacy Shield agreement would allow the surveillance issue to be dealt with in other capacities and would protect against the threat of political instability both under the current administration and in the future. By eliminating the US government's role in enforcement, this arrangement would be limited to self-interested participants: US businesses that seek EU data and the EC, which is concerned about protecting its citizens' fundamental right to privacy.

---

256. *Protecting Workers' Rights Worldwide*, FAIR LABOR ASS'N, http://www.fairlabor.org/our-work (last visited Oct. 8, 2017) [https://perma.cc/45S8-DEKZ] (archived Sept. 24, 2017) (noting that the FLA allows "CSOs [civil society organizations] to engage with companies and other stakeholders to find viable solutions to labor concerns").

257. *See id.* (just as the FLA helps to create creative solutions for global labor issues, the Data Privacy NGO can work together to more efficiently protect EU data subjects' fundamental right to data privacy).

258. *See id.*

259. *See* Steven Greenhouse, *Critics Question Record of Monitor Selected by Apple*, N.Y. TIMES (Feb. 13, 2012), http://www.nytimes.com/2012/02/14/technology/critics-question-record-of-fair-labor-association-apples-monitor.html [https://perma.cc/6QA8-36ER] (archived Sept. 24, 2017) (explaining that Nike testified to fact that FLA had a significant impact on "leading multi-stakeholder innovation and engagement on core labor standards").

260. *Id.*

## VI. CONCLUSION

The transatlantic trade of personal data between the European Union and the United States is of critical importance. The EU-U.S. Privacy Shield is the most recent attempt by the trading partners to reach a mutually satisfactory agreement allowing for the transfer of EU personal data to the United States. When compared to its predecessor, the EU-U.S. Safe Harbor, the Privacy Shield Framework features numerous upgrades including improved data protection mechanisms, more thorough redress, and increased oversight by the US government. However, despite these developments, shortcomings of the EU-U.S. Privacy Shield still exist, including a lack of concrete protections from U.S. surveillance and external factors in both the European Union and the United States that threaten the future of the Framework.

As it stands, today's data privacy landscape is filled with uncertainty. While the EU-U.S. Privacy Shield is by no means a perfect settlement between trading partners, the need for an efficient mechanism of trade is of paramount concern for all involved. By restructuring the current framework into a public-private EU-U.S. business arrangement and forming a Data Privacy NGO to take over the administrative and enforcement role of US agencies, the framework has a chance at continued vitality and evolution.

*Emily Linn*

---

* B.A., University of Texas at Austin; Candidate for Doctor of Jurisprudence, 2018, Vanderbilt Law School. I would like to express my gratitude to Professor Ingrid Wuerth and Svetlana Yakovleva for their guidance and insight throughout the writing process. I would also like to thank the editorial staff of the Vanderbilt Journal of Transnational Law for their valuable contributions to this Note, as well as my family and friends for their unwavering support and love.