THE EU-U.S. PRIVACY SHIELD: AN UNCERTAIN FUTURE

Catherine Read†

TABLE OF CONTENTS

I. INTRODUCTION

In January 2018, President Donald J. Trump signed the renewal of Section 702 of the Foreign Intelligence Surveillance Act ("FISA") for a six-year period "following an overwhelming vote of approval in the Senate (65-34) and the House of Representatives (256-164)."[1] In short, the law permits the United States government to collect the communications of foreigners that are reasonably believed to be located abroad for foreign intelligence purposes.[2] While the

†J.D. Candidate, Class of 2020 at the Benjamin N. Cardozo School of Law. Staff Editor on the International Comparative, Policy & Ethics Law Review.

[1] Jonathan Keane, *What FISA Renewal Means for the U.S.-EU Privacy Shield Agreement*, THE DAILY DOT (Feb. 10, 2018, 6:00 AM), https://www.dailydot.com/layer8/fisa-renewal-us-eu-privacy-shield/.

[2] *Id.*

government may not directly target Americans, "wholly unrelated and purely domestic communications" are often swept up in the process.[3] Furthermore, once these communications are "incidentally" collected, the Federal Bureau of Investigation ("FBI") may search and use the data in unrelated criminal investigations, also known as "backdoor searches."[4]

Section 702's contentious renewal has sparked serious privacy concerns not only in the U.S., but in the European Union ("EU"), as well.[5] European data is stringently protected by the General Data Protection Regulation ("GDPR").[6] Under the GDPR, data transfers to non-EU countries are only permitted if personal data receives an "adequate level of protection" upon arrival in the destination country.[7]

The original framework governing transatlantic data transfers from the EU to the U.S. was known as Safe Harbor, adopted in July 2001.[8] However, following former National Security Agency ("NSA") Edward Snowden's revelation that the NSA was engaging in bulk data collection, the European Court of Justice ("ECJ") invalidated the agreement in October 2015 for failing to ensure an adequate level of protection for EU citizens' data.[9] As Irish High Court Justice Gerard Hogan noted, there were "gaping holes in contemporary U.S. data protection practice" that needed to be addressed.[10]

As a result, the European Commission ("EC") and the U.S. Department of Commerce ("DOC") renegotiated the framework and

[3] Michelle Richardson, *FISA 702: What Happened and What's Next*, CDT (Feb. 5, 2018), https://cdt.org/blog/fisa-702-what-happened-and-whats-next/.

[4] Sharon Bradford Franklin, *The House Intelligence Committee's Section 702 Bill is a Wolf in Sheep's Clothing*, JUST SECURITY (Jan. 9, 2018), https://www.justsecurity.org/50801/house-intelligence-committees-section-702-bill-wolf-sheeps-clothing/.

[5] Keane, *supra* note 1.

[6] Hayley Evan & Shannon Togawa Mercer, *Privacy Shield on Shaky Ground: What's Up with the EU-U.S. Data Privacy Regulations*, LAWFARE (Sept. 2, 2018, 2:31 PM), https://www.lawfareblog.com/privacy-shield-shaky-ground-whats-eu-us-data-privacy-regulations.

[7] Alston & Bird LLP, *Transferring Data from the EU: Privacy Shield and Data Transfer Under the GDPR*, https://files.alston.com/files/docs/Roadmap-to-the-GDPR-International-Data-Transfers.pdf (last visited Nov. 25, 2019).

[8] David Lowe, *The Implications of the Schrems Decision and Ending of the US-EU Safe Harbour Agreement*, THE NEW JURIST (Feb. 1, 2016), http://newjurist.com/the-implications-of-the-schrems-decision.html.

[9] *Id.*

[10] *Id.*

implemented the EU-U.S. Privacy Shield in July 2016.[11] The new data transfer agreement "includes limitations on data retention, accountability for onward transfers, an Ombudsperson for redress by EU individuals in relation to the transfer of their data to the U.S., and more regular and rigorous monitoring by the Department of Commerce."[12] Additionally, the EC and DOC jointly review Privacy Shield on a yearly basis.[13] Although the reviews thus far have concluded that Privacy Shield "ensure[s] an adequate level of protection"[14] for personal data transferred from the EU to the U.S., the fate of the agreement remains in question, particularly in light of the reauthorization of Section 702 and the U.S.'s delay in implementing the EC's annual proposals.[15]

Following Privacy Shield's initial review in September 2017, the U.S. disregarded the EC's recommendation to fully incorporate the Presidential Policy Directive-28 ("PPD-28")—which would recognize and strengthen privacy protections for non-Americans—in Section 702 when it reauthorized the law without PPD-28 in January 2018.[16] Consequently, any data transferred from the EU to the U.S. could be subject to surveillance by the National Security Agency ("NSA"), which sparked significant backlash from European privacy advocates.[17] As one critic stated: "The only concern in the U.S. has been the protection of U.S. persons from NSA spying and surveillance and while there was some effort to address this in the amended FISA bill, there was nothing there to address Europeans' and the EC's concerns."[18]

Additionally, the U.S. has been extremely slow to appoint new members to the depleted U.S. Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent agency tasked with advising the President and other executive branch officials on matters of U.S.

---

[11] *Id.*

[12] Evan & Mercer, *supra* note 6.

[13] David Bender & Calvin Cohen, *Privacy Shield Updates: Second Annual Review and Brexit Guidance*, INSIDE PRIVACY (Dec. 21, 2018), https://www.insideprivacy.com/international/european-union/privacy-shield-updates-second-annual-review-and-brexit-guidance/.

[14] *Id.*

[15] *Id.*

[16] Evan & Mercer, *supra* note 6.

[17] Keane, s*upra* note 1.

[18] *Id.*

privacy and civil liberties, at the EC's request.[19] For example, as of Privacy Shield's second annual review in October 2018, the U.S. had yet to appoint a permanent Privacy Shield Ombudsperson to handle data protection complaints from EU citizens, a key feature of the agreement.[20] The EC subsequently demanded that the U.S. identify and submit a nominee for the position by February 28, 2019, or else the Commission would "consider taking appropriate measures, in accordance with the General Data Protection Regulation."[21] Finally, on January 18, 2019, President Trump nominated Keith J. Krach for the position,[22] and on June 20, 2019, the U.S. Senate confirmed Mr. Krach to become the administration's first permanent Privacy Shield Ombudsperson—almost three years after the initial request.[23] This was not the first or only time that the U.S. had been threatened with sanctions for non-compliance with Privacy Shield. In July 2018, Members of the European Parliament ("MEPs") threatened to suspend Privacy Shield after a massive transatlantic data breach occurred in which Facebook transferred roughly 2.7 million EU citizens' data to Cambridge Analytica, a British political consulting firm.[24] The scandal indicated that certain U.S. signatories were not respecting the agreement, and that Privacy Shield needed greater supervision.[25] While the agreement was ultimately kept intact, the possibility of a temporary interruption or complete ban of data transfers from the EU

[19] Rebecca Hill, *Two Years Later and It Still Sucks: Privacy Shield Progress Panned*, THE REGISTER (Aug. 31, 2018, 12:05 PM), https://www.theregister.co.uk/2018/08/31/privacy_shield_progress_panned/.

[20] EUROPEAN COMMISSION, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL ON THE SECOND ANNUAL REVIEW OF THE FUNCTIONING OF THE EU-U.S. PRIVACY SHIELD (Dec. 19, 2018), https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf [hereinafter EUROPEAN COMMISSION, SECOND ANNUAL REVIEW OF THE FUNCTIONING OF THE EU-U.S. PRIVACY SHIELD].

[21] *Id.*

[22] Amanda Lee, *US to Appoint Permanent Privacy Shield Ombudsperson, As EU Pressure Tells*, EURACTIV (Jan. 23, 2019), https://www.euractiv.com/section/data-protection/news/us-to-appoint-permanent-privacy-shield-ombudsperson-following-eu-pressure/.

[23] Mark Young & Sam Jungyun Choi, *Privacy Shield Ombudsperson Confirmed by the Senate,* COVINGTON (June 25, 2019), https://www.insideprivacy.com/cross-border-transfers/privacy-shield-ombudsperson-confirmed-by-the-senate/.

[24] Fouad Khalil, *Breaking Down Privacy Shield: Will It Stay or Will It Go?*, SILICON REPUBLIC (Sept. 6, 2018), https://www.siliconrepublic.com/enterprise/privacy-shield-analysis.

[25] *Id.*

to the U.S. remains high if U.S. signatories continue to fail to comply with Privacy Shield's terms.[26]

This Note explores the implications of Section 702 of FISA on the EU-U.S. Privacy Shield, the importance of maintaining transatlantic data flow between the EU and the U.S., and the current geopolitical tensions existing between the EU and the U.S. with respect to the U.S. government's haphazard compliance with the agreement. As Alan Butler, senior counsel at the Electronic Privacy Information Center, indicates, "[t]he EU-US Privacy Shield is an agreement built on a delicate balance of commitments and assumptions made by both the Americans and the Europeans, and the tumultuous changes taking place now in the United States could well bring the entire structure crashing down."[27] This note argues that, in order to secure the future of Privacy Shield and the free flow of information from the EU to the U.S., the U.S. government should amend Section 702 to enshrine the PPD-28 protections for non-Americans, maintain a fully-staffed and functioning PCLOB board, and subject U.S. Privacy Shield signatories to more rigorous reviews and swift enforcement actions for non-compliance.

II. BACKGROUND

A. Section 702 of the FISA

Section 702 of FISA is largely a byproduct of the George W. Bush Administration's President's Surveillance Program ("PSP") implemented in the wake of the September 11th attacks.[28] Under one aspect of that program, known as the Terrorist Surveillance Program ("TSP"), President Bush authorized the NSA, without warrants, to intercept the contents of international communications of both U.S. and non-U.S. persons from within the United States as a means to detect and prevent future attacks on the United States.[29]

---

[26] Evan & Mercer, *supra* note 6.

[27] Alan Butler, *Whither Privacy Shield in the Trump Era*, 3 EUR. DATA PROTECTION L. REV. 111, 113 (2017).

[28] PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE ACT 86-97 (2014), https://www.pclob.gov/library/702-Report.pdf.

[29] OFFICES OF INSPECTORS GEN. OF THE DEP'T OF DEF. ET AL., REPORT NO. 2009-0013-AS, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 18 (2009), https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-I.pdf.

After the program was publicized by The New York Times in 2005,[30] the government sought to legitimize its practices by creating a statutory framework for its warrantless surveillance activities.[31] As a temporary measure, Congress adopted the Protect America Act ("PAA") in 2007.[32] The PAA modified FISA of 1978 by generating additional procedures for authorizing certain acquisitions of foreign intelligence information, and in turn, easing restrictions on the surveillance of foreigners where one or both parties were located abroad.[33]

1. The Law

Although the PAA expired shortly thereafter, its core values were preserved when Congress passed the FISA Amendments Act ("FAA") in 2008.[34] The FAA incorporated several new provisions including Section 702 of FISA, codified as amended at 50 U.S.C. § 1881(a).[35] The statute empowers the Attorney General ("AG") and Director of National Intelligence ("DNI") to jointly authorize surveillance targeting any non-U.S. person "reasonably believed to be located outside the United States to acquire foreign intelligence information."[36]

Unlike traditional FISA surveillance, Section 702 does not require the government to demonstrate probable cause that "the target of the electronic surveillance target is a foreign power or an agent of a foreign power," nor does it require that "each of the facilities or places at which the electronic surveillance is directed [be] used, or is about to be used, by a foreign power or agent of a foreign power."[37] Rather, the statute merely stipulates that a "'significant' purpose of the surveillance is to gather 'foreign intelligence information.'"[38] Such

[30] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

[31] Evan & Mercer, *supra* note 6.

[32] Protect America Act, Pub. L. No. 110–55, 121 Stat. 552 (2007).

[33] *Id*.

[34] FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436.

[35] *Id.*

[36] 50 U.S.C. § 1881a(a) (2012).

[37] 50 U.S.C. § 1805(a)(2) (2006).

[38] *Q & A: US Warrantless Surveillance Under Section 702 of the Foreign Intelligence Surveillance Act*, HUMAN RIGHTS WATCH (Sept. 14, 2017, 1:54 PM) (citing 50 U.S.C. § 1881a), https://www.hrw.org/news/2017/09/14/q-us-warrantless-surveillance-under-section-702-foreign-intelligence-surveillance.

data includes any information that relates to the United States' ability to protect against an "actual or potential attack or other grave hostile acts of a foreign power . . . ; sabotage, intentional terrorism, or the proliferation of weapons of mass destruction by a foreign power . . . ; or clandestine intelligence activities by an intelligence service or network of a foreign power . . . ."[39]

Section 702, however, attempts to curb the government's surveillance power by imposing the following six limitations on the acquisition of intelligence:

> (1) [surveillance] may not intentionally target any person known at the time of acquisition to be located in the United States; (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States; (3) may not intentionally target a United States person reasonably believed to be located outside the United States; (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; (5) may not intentionally acquire communications that contain a reference to, but are not to or from, a target of an acquisition authorized under subsection (a), except as provided under section 103(b) of the FISA Amendments Reauthorization Act of 2017; and (6) shall be conducted in a manner consistent with the fourth amendment of the Constitution of the United States.[40]

While the statute does not require the government to obtain individualized court authorization for the communications of each targeted person,[41] it does require the AG and DNI to adopt certain "targeting and minimization procedures."[42] These procedures are meant to help minimize the acquisition and retention of information concerning nonconsenting U.S. persons.[43] Further, prior to any interception, the AG and DNI must submit a written certification of the procedures to the Foreign Intelligence Surveillance Court ("FISC").[44] The FISC then reviews the procedures to ensure the

[39] 50 U.S.C. §1801(e)(1).
[40] 50 U.S.C. § 1881(a)(1-6).
[41] 50 U.S.C. § 1881(a).
[42] 50 U.S.C. § 1881(e).
[43] *Id.*
[44] 50 U.S.C. § 1881(a).

government targets only those "persons reasonably believed to be located outside the United States" (i.e., it does not purposefully target domestic communications).[45] Once the certification is approved, the FISC issues a court order permitting the surveillance for a period of up to one year.[46]

2. Incidental/About Collection

Despite these safeguards, however, the government inevitably sweeps up vast quantities of U.S. persons' international communications.[47] What is termed "incidental collection" can occur anytime an American communicates with a foreigner that is "targeted" under Section 702 surveillance, regardless of whether they are suspected of any wrongdoing.[48] This could even include a wholly innocent conversation that mentions, for example, a current event involving ISIS because it "relates to… the conduct of the foreign affairs of the United States." [49]

Under Section 702, there is "no standard of suspicion or limiting check on the government's power to determine that it is reasonable to incidentally collect a particular Americans' communications."[50] Thus, "broad foreign intelligence categories, targets and selectors that a judge does not approve and for which there is no probable cause coupled with broad-based collection means that the 'incidental' collection will be vast, arbitrary, and unnecessary for the cause."[51]

Included in incidental collection is the issue of "about" collection, which is where the government collects not only communications that are "to" and "from" a target, but also those that are "about" a target.[52] This type of collection could include emails between two non-targets that happen to mention a target's email address, phone number, or

[45] 50 U.S.C. § 1881(j)(2)(B)(i).

[46] 50 U.S.C. § 1881(j)(3)(A).

[47] Allyson Scher, *Stop Calling It "Incidental" Collection of Americans' Emails: The Gov't's Renewed Surveillance Powers*, JUST SECURITY (Jan. 22, 2018), https://www.justsecurity.org/51272/stop-calling-incidental-collection-americans-emails-govts-renewed-surveillance-powers/.

[48] *See id.*

[49] *Reducing "Incidental" Collection Under FISA Section 702: A Critical Protection for Americans*, BRENNAN CENTER FOR JUSTICE (Oct. 2017), https://www.brennancenter.org/sites/default/files/FISASection702ReducingIncidentalCollection.pdf.

[50] 50 U.S.C. § 1881(j)(2)(B)(i).

[51] *See id.* § 1881(j)(2)(B)(i).

[52] Franklin, *supra* note 4.

other "selector" in their communications.[53] "About" collection permits not only the gathering of "communications where no participating communicant is a target, but it [also] vastly increases the risks of collecting purely domestic communications."[54] The FISC, however, has found this type of collection to raise serious privacy concerns and recently forced the government to shut it down.[55]

3. Backdoor Searches

Additionally, once Americans' communications are incidentally gathered, the FBI is permitted to search and use the contents and metadata collected under Section 702 in unrelated criminal investigations.[56] "Backdoor searches," or "U.S. person queries," "occur when, without any judicial process or oversight, the government searches through its collected Section 702 database for information about a specific American—someone who could not be targeted for surveillance in the first place without an in individualized warrant . . . ."[57]

It has been reported that the NSA and the Central Intelligence Agency ("CIA") conduct these searches tens of thousands of times per year, and the FBI, who routinely sifts through this data, does not even attempt to track the number of queries it conducts.[58] According to a four-month investigation, and a sampling of over 160,000 communications collected under Section 702, the *Washington Post* found that nine out of ten account holders identified were not surveillance targets, but were "incidentally" intercepted.[59] Moreover, nearly fifty percent of the communications included names, email addresses, or other details belonging to U.S. citizens or residents.[60]

[53] *See id.*
[54] *See id.*
[55] *See id.*
[56] *See id.*
[57] *See id.*
[58] Franklin, s*upra* note 4.
[59] Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST (July 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html?utm_term=.423d95f1ae18 [https://perma.cc/EUC2-BQT7].
[60] *See id.*

These findings are also supported by judicial record.[61] For example, in 2015, a FISC judge who overseas Section 702 surveillance observed that "substantial quantities" of Americans' communications are intercepted under its authority.[62]

Despite Section 702's apparent constitutional issues, the program has been found to "make a substantial contribution to the government's efforts to learn about the membership, goals, and activities of international terrorist organizations, and to prevent acts of terrorism from coming to fruition."[63] Additionally, the program has "led the government to identify previously unknown individuals who are involved in international terrorism, and it has played a key role in discovering and disrupting specific terrorist plots aimed at the United States and other countries."[64] The question remains, however, whether the benefits of the program outweigh its costs.

In January 2018, Congress answered this question in the affirmative through the passing of the FISA Amendments Reauthorization Act, which reauthorized Section 702 until 2023.[65]

B. EU-U.S. Privacy Shield

1. Data Protection Directive and General Data Protection Regulation

International data transfers from the European Union to third party countries were initially governed by Article 25(6) of the Data Protection Directive ("DPD") 95/46/EC, adopted in 1995.[66] Under this Article, the European Commission was permitted to authorize transfers if "a third country ensure[d] an adequate level of protection… by reason of its domestic law or of the international commitment it has entered into."[67] A finding of adequacy "allow[ed]

---

[61] Robyn Greene, *How the Government Can Read Your Email*, POLITICO (June 22, 2017, 5:25 AM), https://www.politico.com/agenda/story/2017/06/22/section-702-surveillance-program-national-security-000463.

[62] UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT, MEMORANDUM OPINION AND ORDER (Nov. 6, 2015), https://www.intelligence.gov/assets/documents/702%20Documents/oversight/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

[63] PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 28, at 86-97, 104.

[64] *Id.* at 108.

[65] FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3.

[66] Council Directive 95/46, art. 25, 1995 O.J. (L 281) 6 (EC).

[67] *Id.*

the free flow of personal data from the EU without the EU data exporter having to implement any additional safeguards or being subject to further conditions."[68] Such a finding recognized that a non-EU country's level of data protection was "essentially equivalent" to the protection provided by the EU, considering its rules and procedures on access to personal data by public authorities for law enforcement, national security, and public interest purposes.[69] Although the DPD was phased out in May 2018 and replaced by the General Data Protection Regulation ("GDPR"), under the EU's new data privacy regime, the "essentially equivalent" standard continues to be the hallmark of adequacy decisions.[70]

2. Safe Harbor and the Schrems Decision

The EU and U.S. Department of Commerce ("DOC") first entered into an international data transfer agreement in July 2000, which was known as "Safe Harbor."[71] In October 2015, however, the ECJ invalidated the provision in response to growing concerns about U.S. surveillance programs.[72] Max Schrems, a privacy activist and Facebook user, filed a complaint with the Irish Data Protection Commissioner, "alleging that his Facebook data, which is transferred from Facebook's Irish subsidiary to servers in the United States, was inadequately protected."[73] Schrems based his allegations on news reports about the scope of NSA surveillance that resulted from the Snowden disclosures.[74] The Commissioner rejected the complaint on

---

[68] *See* EUROPEAN COMMISSION, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, EXCHANGING AND PROTECTING PERSONAL DATA IN A GLOBALISED WORLD (Oct. 1, 2017), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN [hereinafter EUROPEAN COMMISSION, EXCHANGING AND PROTECTING PERSONAL DATA IN A GLOBALISED WORLD].

[69] *Id.*

[70] Alston & Bird LLP, *supra* note 7.

[71] Ernst-Oliver Wilhelm, *A Brief History of Safe Harbor*, IAPP, https://iapp.org/resources/article/a-brief-history-of-safe-harbor/ (last visited Nov. 25, 2019).

[72] Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, 2015 EUR-Lex CELEX LEXIS 650 (Oct. 6, 2015).

[73] Ellen Nakashima, *Top E.U. Court Strikes Down Major Data-Sharing Pact between U.S. and Europe*, WASH. POST (Oct. 6, 2015), https://www.washingtonpost.com/world/national-security/eu-court-strikes-down-safe-harbor-data-transfer-deal-over-privacy-concerns/2015/10/06/2da2d9f6-6c2a-11e5-b31c-d80d62b53e28_story.html?utm_term=.48f14e920d15.

[74] *Id.*

the grounds that the Safe Harbor framework ensured that any data transferred between the EU and U.S. was adequately protected.[75] On review, the Irish High Court referred the matter to the ECJ for a preliminary ruling.[76] In October 2015, the ECJ ultimately invalidated the Safe Harbor framework, ruling that the agreement failed to adequately protect EU citizens' data, and that it placed "national security, public interest or law enforcement requirements" over privacy principles.[77]

3. Privacy Shield Framework

To address the concerns outlined in the Schrems decision, the European Commission ("EC") and the DOC renegotiated a revised agreement known as "Privacy Shield."[78] The new framework seeks to strengthen data privacy protections and more closely regulate commercial transatlantic data flow from the EU to the U.S.[79] Privacy Shield places stronger obligations on U.S. companies to protect EU citizens' data by including enhanced safeguards, such as "limitations on data retention, accountability for onward transfers, an Ombudsperson for redress by EU individuals in relation to the transfer of their data to the U.S., and more regular and rigorous monitoring by the Department of Commerce."[80] Privacy Shield also commits itself to an annual review by the EC to assess ongoing levels of data protection adequacy.[81]

With the necessary safeguards in place, Privacy Shield was adopted in July 2016.[82] The agreement "provides companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data" from the EU to the U.S.[83] Privacy Shield, like the GDPR, serves to protect EU citizens' data in the commercial context.[84] For example, "when shopping online or using social media in the EU, personal data may be collected in the

[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] Evan & Mercer, *supra* note 6.
[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] *Privacy Shield Overview*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Program-Overview (last visited Nov. 25, 2019).
[84] EUROPEAN COMMISSION, EXCHANGING AND PROTECTING PERSONAL DATA IN A GLOBALISED WORLD, *supra* note 68.

EU by a branch or business partner of a participating American company, who then transfers it to the U.S."[85] Or, "a travel agent in the EU may send names, contact details and credit card numbers to a hotel in the U.S. which has registered to the Privacy Shield."[86] Privacy Shield also ensures adequate levels of protection for European data in the law enforcement and national security context, as well.[87]

To effectuate data transfers under Privacy Shield, participating organizations are required to "self-certify" with the DOC, and "publicly commit to comply with the framework's requirements."[88] Organizations must adhere to "23 principles laying out the requirements for the use and treatment of personal data received from the EU, as well as access requests and recourse mechanisms for EU citizen complaints."[89] Once organizations are certified, they are "deemed to provide 'adequate' privacy protection to personal data transferred outside of the EU under the EU Data Protection Directive."[90] As mentioned, the DPD has since been superseded by the GDPR, which permits data transfers to international companies only when the relevant processor or controller has fully complied with the GDPR's privacy and data protection requirements.[91] To date, more than 4,000 companies have been certified with the DOC, including Facebook and Google.[92]

III. ANALYSIS

A. Domestic and International Implications of Section 702

Section 702 of FISA not only affects domestic laws and policies, but international ones, as well. First, in the U.S., critics argue that the passage of the FISA Amendments Reauthorization Act "contains no

[85] *EU-U.S. Privacy Shield: First Review Shows It Works but Implementation Can Be Improved*, EUROPEAN COMMISSION (Oct. 17, 2017), http://europa.eu/rapid/press-release_IP-17-3966_en.htm.

[86] *Id.*

[87] *See* EUROPEAN COMMISSION, EXCHANGING AND PROTECTING PERSONAL DATA IN A GLOBALISED WORLD, *supra* note 68.

[88] U.S. DEP'T OF COMMERCE, *The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks*, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdg (last visited Nov. 25, 2019).

[89] Evan & Mercer, *supra* note 6.

[90] *Id*.

[91] *Id*.

[92] *Id*.

meaningful reforms to Section 702, and in several respects, it expands surveillance authorities and codifies the worst intelligence community practices rather than reforming them."[93] For example, some claim that the Act codified, and actually expanded, the highly disputed, privacy-invasive "about" collection.[94] Robyn Greene, writing for New America, claims there is "a risk that the bill could be read to permit unintentional 'abouts' collection, and to permit the collection of communications that merely reference targets, but do not contain selectors of surveillance targets under Section 702. This would represent a drastic expansion of the most concerning form of Section 702 surveillance."[95]

The Act also codified "backdoor" searches for Americans' communications.[96] The statute "pretends to address this problem by requiring the FBI to obtain a warrant before accessing communications when conducting a search related to a 'predicated' investigation (i.e., once there [is] already a factual basis for the investigation)."[97] However, the FBI "would still be free to conduct unlimited warrantless searches before the 'predicated' investigation stage, such as before and during assessments, which require no factual basis whatsoever that the American was engaged in any wrongdoing."[98] By the time the investigation reaches this stage, "the FBI will have already warrantless search all of an investigative target's communication that were swept up in Section 702 surveillance."[99] Additionally, the Act permits several exceptions to the Fourth Amendment warrant requirement.[100] For example, no warrant is required for predicated investigations related to foreign intelligence, national security, or if a threat to life or serious bodily injury could be mitigated.[101] Taken together, it is clear that the FISA Amendments Reauthorization Act made no meaningful reforms to Section 702, and

[93] Robyn Greene, *Section 702 Bill is Surveillance Expansion and No Meaningful Reform*, NEW AMERICA (Jan. 12, 2018), https://www.newamerica.org/oti/blog/vote-no-s-139-cloture-section-702-bill-surveillance-expansion-and-no-meaningful-reform/.

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] Greene, *supra* note 93.

[100] *Id.*

[101] *Id.*

thus countless electronic communications of innocent Americans remain at risk of being collected.

The same privacy issues hold true in the EU. With Section 702 in place, Europeans' data is effectively subject to "indiscriminate mass surveillance," as the statute permits the U.S. government to collect any foreign intelligence target's electronic communications either stored by U.S. providers or in transit to them.[102] This type of broad collection was exactly what the ECJ was concerned with when it struck down Privacy Shield's predecessor, Safe Harbor, noting that surveillance must be "necessary and proportionate" to national security needs.[103] Section 702, as it currently stands, is contrary to the privacy values enshrined in the Privacy Shield and GDPR, and thus the ultimate fate of Privacy Shield is uncertain.

B. The Future of Privacy Shield

Although, to date, the annual reviews of Privacy Shield have concluded that the framework "continues to ensure an adequate level of protection" for personal data transferred from the EU to the U.S., the European Commission has called for further improvements.[104] The EC conducted its first annual review of Privacy Shield on September 18-19, 2017 and concluded that the agreement ensures an "adequate level of protection for the personal data transferred from the EU to participating companies in the U.S."[105] However, it also made several recommendations to improve Privacy Shield's functioning and ensure its continued existence.[106] For example, the EC suggested that the U.S. more fully incorporate into Section 702 the privacy protections offered for non-Americans by PPD-28, which safeguards personal information regardless of where the person resides[107] and is "a keystone underlying support for the Privacy Shield."[108] It also advised the swift appointment of a permanent Privacy Shield Ombudsperson and members of the depleted U.S. Privacy and Civil Liberties

---

[102] Richardson, *supra* note 3.

[103] *Id.*

[104] *EU-U.S. Privacy Shield*, *supra* note 85.

[105] *Id.*

[106] *See id.*

[107] *See id.*

[108] Cameron Kerry & Alan Charles Raul, *The Economic Case Preserving PPD-28 and Privacy Shield*, LAWFARE, (Jan. 17, 2017, 3:19 PM), https://www.lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield.

Oversight Board because of the important roles that each play in the framework's continued performance.[109]

However, the U.S. has been extremely slow to implement the EC's recommendations, if at all.[110] First, Congress failed to embed PPD-28 into Section 702 when it issued a six-year reauthorization of the Act without it in January 2018; and second, the appointment of the PCLOB members has been far slower than expected.[111] Moving forward, it will be important that the U.S. government implement and maintain these recommendations to ensure the continued existence of Privacy Shield and the free flow of data between the EU and the U.S.

Embedding PPD-28 into Section 702 is crucial to reforming U.S. surveillance authority with respect to non-Americans, and thus improving our relationship with the EU. Former President Obama's 2014 directive declares that "all persons should be treated with dignity and respect regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information."[112] In other words, PPD-28 extends the same privacy safeguards to foreigners as put in place for Americans (e.g., that targeted surveillance be for carefully defined and legitimate purposes).[113] Incorporating this directive into Section 702 would be vital to easing data sharing tensions and restoring global trust in U.S. privacy and surveillance policies. Therefore, Congress should amend Section 702 to include PPD-28 as soon as possible.

Furthermore, maintaining a fully staffed and functioning PCLOB will be imperative to the continued existence of Privacy Shield. As of the agreement's second annual review in October 2018, the U.S. had yet to appoint a permanent Privacy Shield Ombudsperson, who handles data protection complaints from EU citizens on U.S. surveillance practices, a key feature of the Privacy Shield.[114] Subsequently, the EC demanded that the U.S. identify and submit a nominee for the position by February 28, 2019, or else the Commission would "consider taking appropriate measures, in accordance with the General Data Protection Regulation."[115] Nearly three years after Privacy Shield's initial adoption, President Trump

[109] *See EU-U.S. Privacy Shield*, *supra* note 85.

[110] *See* Hill, *supra* note 19.

[111] *See id.*

[112] Kerry & Raul, *supra* note 108.

[113] *See id.*

[114] *See* EUROPEAN COMMISSION, SECOND ANNUAL REVIEW OF THE FUNCTIONING OF THE EU-U.S. PRIVACY SHIELD, *supra* note 20, at 4.

[115] *Id.* at 5-6.

finally nominated Keith J. Krach for the position. On June 20, 2019, Mr. Krach was confirmed by the U.S. Senate to become the Trump administration's first permanent Privacy Shield Ombudsperson, staffing the board's fifth and final seat.[116] While the PCLOB is now fully operational, past vacancies have seriously threatened the existence of Privacy Shield, and thus it will be important to maintain a fully staffed board moving forward. As PCLOB Chairman Adam Klein stated, "the emergence of the [PCLOB] as a visible, energetic, public-facing, and credible evaluator of key surveillance programs" is an important and positive step toward "rebuilding trust with the American people, the technology industry, and partners and publics abroad."[117]

In addition to making the above changes, it will be important that the U.S. government subject U.S. Privacy Shield signatories to more rigorous reviews and swift enforcement actions for non-compliance. In July 2018, the European Parliament ("EP") warned that it would indefinitely suspend the agreement unless the U.S. took greater action to protect the data transferred from the EU to the U.S.[118] This ultimatum was given because, along with failing to fully implement the EC's recommendations after Privacy Shield's first annual review, a massive transatlantic data breach occurred where Facebook transferred approximately 2.7 million EU citizens' data to British political consulting firm Cambridge Analytica.[119] Facebook's blatant noncompliance with Privacy Shield indicated that at least some U.S. signatories were not respecting the agreement.[120] Further, neither of the companies involved had their certifications revoked by the DOC[121] and the Foreign Trade Commission ("FTC") took 15 months to bring an enforcement against Facebook.[122] Further, the FTC has over 25,000 complaints with the EC about Facebook consumer privacy pending, yet it has not taken a single enforcement action against the

[116] Young & Choi, s*upra* note 23.

[117] Cameron Kerry, *It's Time for the Senate to Act on PCLOB Nominations*, LAWFARE (Aug. 27, 2018, 9:08 AM), https://www.lawfareblog.com/its-time-senate-act-pclob-nominations.

[118] *See id.*

[119] Khalil, *supra* note 24.

[120] *Id.*

[121] *See* Hill, *supra* note 19.

[122] ELECTRONIC PRIVACY INFORMATION CENTER, COMMENTS TO THE EUROPEAN COMMISSION ON THE PRIVACY SHIELD THIRD ANNUAL REVIEW 10 (July 15, 2019), https://epic.org/privacy/intl/Comments_Privacy_Shield_Review_3.pdf.

company.[123] Members of the European Parliament ("MEPs") declared this incident a "scandal," which significantly weakened trust across borders and discredited the Privacy Shield framework.[124] Reviewing U.S. signatory privacy practices on a more regular and rigorous basis, combined with bringing swifter enforcement actions for non-compliance, will be crucial to the future of Privacy Shield.

Thus, in light of the broad surveillance measures permitted under Section 702, the U.S government's haphazard implementation of Privacy Shield recommendations, and the lack of adequate review and enforcement of U.S. signatories for non-compliance, the future of Privacy Shield, and the free flow data that it protects, remains in a state of uncertainty.

IV. CONCLUSION

The ability to transfer data across borders has become increasingly vital to global commerce and communications networks.[125] The EU-U.S. Privacy Shield is a mutually agreed upon framework that allows for the free flow of personal data from the EU to the U.S. While Privacy Shield arguably contains significantly more privacy protections for Europeans than its predecessor, Safe Harbor, including more oversight possibilities and redress mechanisms, the European Commission remains concerned that the U.S is shirking its privacy duties to non-Americans and that the agreement fails to adequately protect EU citizens' personal data. For example, reauthorizing Section 702 of FISA without incorporating PPD-28 failed to ensure non-Americans the same level of privacy protections granted to Americans, taking more than three years to fully staff and appoint a Privacy Shield Ombudsperson impeded the Privacy Shield's functioning and weakened trust with the EU, and experiencing the impacts of the Facebook/Cambridge Analytica scandal discredited Privacy Shield's framework. These shortcomings, in combination, gravely threaten the future of the EU-U.S. Privacy Shield. Thus, it is recommended that the U.S. government amend Section 702 to enshrine the PPD-28 protections for non-Americans, maintain a fully staffed PCLOB board, and subject U.S. Privacy Shield signatories to more rigorous reviews and swift enforcement actions for non-compliance.

---

[123] *Id.*
[124] *Id.*
[125] Richardson, *supra* note 3.