U.S.-EU Privacy Shield and Transatlantic Data Flows

September 22, 2021

Congressional Research Service
https://crsreports.congress.gov
R46917

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

U.S.-EU Privacy Shield and Transatlantic Data Flows

SUMMARY

R46917

September 22, 2021

Kristin Archick
Specialist in European Affairs

Rachel F. Fefer
Analyst in International Trade and Finance

Differences in U.S. and European Union (EU) legal regimes and policy approaches on data privacy and protection have long posed challenges in U.S.-EU relations. To enable cross-border data flows amid EU concerns that the United States does not sufficiently protect personal data, the United States and the EU have concluded several data transfer agreements in both the commercial and law enforcement sectors. In 2013, widespread media reports of unauthorized disclosures of U.S. National Security Agency (NSA) surveillance practices and the alleged involvement of some U.S. internet and telecommunications companies intensified scrutiny in Europe of transatlantic data flows and prompted legal challenges to U.S.-EU commercial data transfer accords. Congress may be interested in better understanding the current state of play with these issues, as well as how a disruption to transatlantic data flows may impact the U.S. economy and the U.S.-EU partnership.

Transatlantic Data Flows and EU Court Rulings

The United States and the EU share an extensive trade and investment relationship and are each other's most important commercial partners for digitally-enabled services. According to the U.S. Bureau of Economic Analysis, U.S.-EU trade in information and communications technology (ICT) services and potentially ICT-enabled services was estimated to be over $264 billion in 2020. Transatlantic data flows enable people and companies to transmit information for online communication, track global supply chains, share research, provide cross-border services, and support technological innovation, among other activities.

Since the media leaks of the NSA programs, the Court of Justice of the European Union (CJEU, also known as the European Court of Justice, or ECJ) has invalidated two U.S.-EU commercial data transfer accords—the Safe Harbor accord in 2015 and its successor agreement, the Privacy Shield Framework, in 2020. In both rulings (known as *Schrems I* and *Schrems II*, respectively), the CJEU found that the data transfer arrangements did not meet EU data protection standards, given the breadth of U.S. data collection powers authorized in U.S. electronic surveillance laws and the lack of redress options for EU citizens. The CJEU's 2020 ruling also increased due diligence requirements for data exporters using another EU mechanism—standard contractual clauses (SCCs)—to transfer personal data to the United States.

At the time of the CJEU's judgment in July 2020, Privacy Shield had 5,380 participants, including U.S. businesses and other organizations, U.S. subsidiaries in the EU, and 250 entities headquartered in the EU. The CJEU ruling creates legal uncertainty for many firms engaged in transatlantic trade, both those that relied on Privacy Shield (over 75% of which are small and mid-sized firms, SMEs) and those using SCCs, including many multinational companies. The CJEU decision could raise operating costs, especially for SMEs, given the limited alternatives for U.S.-EU data transfers. Some experts suggest that the EU or member states may turn to data localization rules requiring local storage of EU citizens' personal data.

U.S.-EU Negotiations and Congressional Interests

The Biden Administration is negotiating with the EU on an enhanced successor accord to Privacy Shield. U.S. negotiators are reportedly seeking to provide the EU with greater assurances through executive orders and administrative action on how the United States safeguards EU citizens' personal data and to clarify how they can pursue redress in U.S. courts for any alleged misuse of their data. Some in the EU question whether such measures would satisfy EU regulators or, ultimately, the CJEU, and contend that legislative action may be necessary to address EU concerns.

Many Members of Congress have supported the Privacy Shield framework as vital to U.S.-EU trade and investment ties. Some in Congress express concerns that the EU approach to data protection creates unfair trade barriers and limits U.S. firms' access to the EU market. Some Members urge the quick conclusion of an enhanced Privacy Shield accord in light of U.S. business needs and because they view U.S.-EU cooperation as crucial to setting international data privacy standards and countering China's potential influence on the issue globally. Possible options for Congress to facilitate U.S.-EU data flows and a successor to Privacy Shield include exploring changes when authorizing and overseeing surveillance programs and considering whether comprehensive national privacy legislation with data protection provisions would help mitigate EU concerns. Congress also may examine how best to achieve broader consensus on data flows and privacy at the global level, including through potential common approaches with the EU in ongoing bilateral and multilateral digital trade negotiations.

Contents

Figures

Contacts

Overview

For decades, data privacy and protection issues have been sticking points in U.S. relations with the European Union (EU) because of differences in U.S. and EU data privacy approaches and legal regimes. The 27-member EU considers the privacy of communications and the protection of personal data to be fundamental rights, codified in EU law, and has established a comprehensive legal framework to protect citizens' personal data.[1] In the United States, respect for privacy is broadly enshrined in the Constitution and data privacy and protection laws are a mix of federal and state statutes that protect certain data on a largely sectoral basis. To address EU concerns that the U.S. approach does not protect personal data to the same extent as EU law, the United States and the EU have concluded agreements to allow for commercial transatlantic data flows (see **Figure 1**), as well as other accords for data transfers in the law enforcement sector.[2]

In 2013, widespread reports in the media of unauthorized disclosures of U.S. National Security Agency (NSA) surveillance programs and the alleged involvement of some U.S. internet and telecommunications companies intensified European concerns about U.S. government access to EU citizens' personal data. Since then, the Court of Justice of the European Union (CJEU, also known as the European Court of Justice, or ECJ) has invalidated two U.S.-EU commercial data transfer accords—the Safe Harbor accord in 2015 and its successor agreement, the Privacy Shield Framework, in 2020. In both the 2015 and 2020 CJEU rulings (known as *Schrems I* and *Schrems II*, respectively), the CJEU found that the U.S.-EU data transfer accords failed to meet EU data protection standards given the breadth of U.S. data collection powers authorized in U.S. electronic surveillance laws and the lack of redress options for EU citizens.

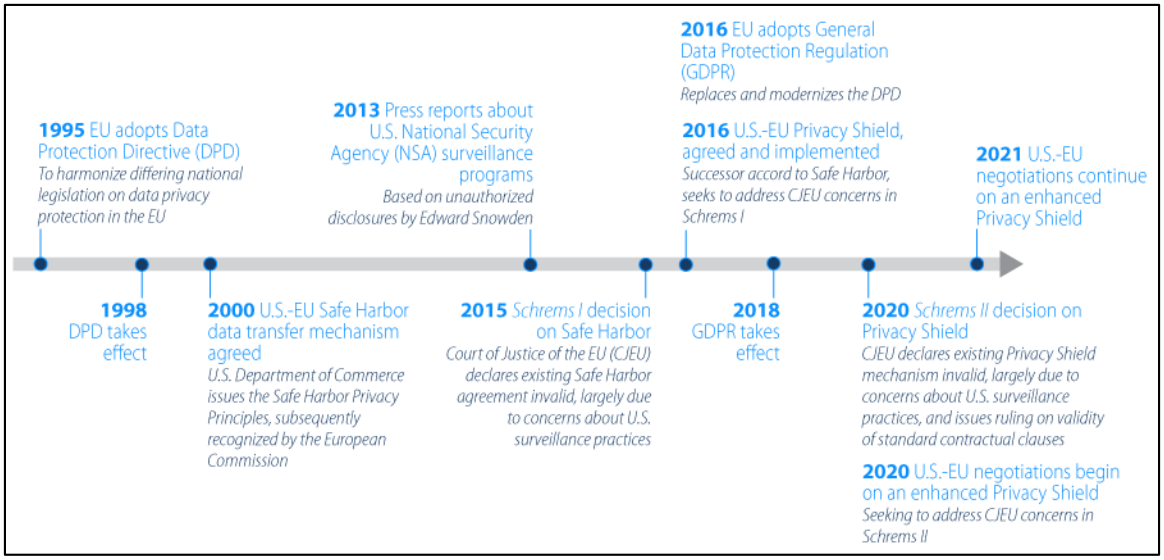
The CJEU's invalidation of Privacy Shield in 2020 leaves U.S. firms with limited options for cross-border data flows with the EU and threatens bilateral trade for many U.S. and EU businesses. The CJEU decision on Privacy Shield has increased congressional concerns that the EU approach to data protection creates unfair trade barriers and limits U.S. firms' access to the EU market. Like the former Trump Administration, the Biden Administration is negotiating with the EU on an enhanced successor accord to Privacy Shield. The Biden Administration have expressed hope that a new agreement will help bolster U.S.-EU relations and address U.S. business demands for durable, protected transatlantic data flows. Some Members of Congress urge the quick conclusion of an enhanced Privacy Shield in light of U.S. business and industry concerns and because they view U.S.-EU cooperation as crucial to setting international data privacy standards and countering China's potential influence on the issue globally.

This report provides background on the differences in U.S. and EU data privacy regimes, the development of Privacy Shield and the prospects for an enhanced successor accord, implications for U.S. interests, and issues for Congress. Also see CRS Report R46724, *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield*, by Chris D. Linebaugh and Edward C. Liu. For more information on the EU, see CRS Report RS21372, *The European Union: Questions and Answers*, by Kristin Archick.

[1] The current 27 members of the EU are Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden. In January 2020, the United Kingdom withdrew as a member of the EU.

[2] U.S.-EU agreements to allow the transfer of data for law enforcement purposes include the U.S.-EU Passenger Name Record (PNR) accord on sharing airline passenger data and the U.S.-EU Terrorist Finance Tracking Program (TFTP), also known as the U.S.-EU SWIFT agreement. For background on these and other U.S.-EU data-sharing accords in the law enforcement sector, see CRS Report RS22030, *U.S.-EU Cooperation Against Terrorism*, by Kristin Archick.

Figure 1. Timeline of Key Events for Commercial Transatlantic Data Flows



Source: CRS based on public sources.

Data Privacy and Protection in the EU and the United States

Both the United States and the EU assert they are committed to upholding individual privacy rights and ensuring the protection of personal data, including online data. Nevertheless, there are fundamental differences in the U.S. and EU approaches to data privacy and protection. EU concerns about how the United States handles personal data have posed challenges in U.S.-EU economic and security relations and, at times, have disrupted U.S.-EU data flows. At the same time, many U.S. stakeholders describe the EU's data privacy and protection regime as overly restrictive for efficient cross-border data flows.

EU Approach

The EU considers the privacy of communications and the protection of personal data to be fundamental rights. These rights are contained in Articles 7 and 8 of the 2000 Charter of Fundamental Rights of the European Union and made binding on all EU members through the 2009 Treaty of Lisbon (the EU's most recent institutional reform treaty). Furthermore, Article 52 of the Charter holds that any limitations on such rights must be subject to the principle of proportionality, while Article 47 provides the right to judicial redress for infringements. Europe's past history with fascist and totalitarian regimes informs the views on data privacy in many European countries and contributes to the demands from European politicians and publics for strict data protection measures, especially for personal data.[3]

[3] Thomas Shaw, "Privacy Law and History: WWII-Forward," International Association of Privacy Professionals, March 1, 2013; David Meyer, "How Europe Is Better at Protecting Data Than the U.S. – And What the Stasi and Nazis Have To Do With It," MarketWatch.com, March 21, 2018; Olivia B. Waxman, "The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History," *Time*, May 24, 2018.

The EU first sought to establish a comprehensive EU-wide framework to harmonize differing national legislation on data privacy protection with its 1995 Data Protection Directive (DPD), which took effect in 1998.[4] The DPD set out common rules for public and private entities in all EU member states that hold or transmit personal data. The DPD governed how information about European citizens may be collected and used across all industries, with each EU member state responsible for implementing the provisions of the DPD through its own national laws. The DPD also established that the transfer of personal data to a country outside of the EU could occur only if the European Commission (the EU's executive) determined that the country provided an adequate level of protection for personal data. The adequacy of the level of protection was assessed in light of all the circumstances surrounding the data transfer, with particular consideration given to the nature of the data, the purpose and duration of the proposed processing operations, the final destination of the data, and that country's laws, rules, and security measures.

In 2012, the European Commission proposed a new legislative package to modernize the DPD and introduce other data protection reforms to take into account the changes in data processing since 1995 brought about by the widespread use of the internet. After four years of contentious debate within the EU, including a process for EU and foreign stakeholders to provide input, the EU adopted the General Data Protection Regulation (GDPR) to replace the DPD. The GDPR became directly applicable in all EU members states in May 2018.[5]

The GDPR establishes a single set of rules for protection of personal data throughout the EU. It seeks both to strengthen individuals' fundamental rights in the digital age and to facilitate business by ensuring more consistent implementation of the rules in all EU countries. The GDPR sets out specific individual rights and company obligations regarding data collection and processing. It applies to all businesses and organizations that process the personal data of individuals in the EU, regardless of where the actual processing of the data takes place. Like the former DPD, the GDPR permits the transfer of personal data outside the EU only to those countries that the EU regards as having an adequate level of protection.[6]

U.S. Approach

Unlike in the EU, no single U.S. federal law comprehensively regulates the collection and use of consumers' personal data.[7] While the U.S. Supreme Court has interpreted the Constitution to provide individuals a right to privacy, this right generally guards only against government intrusions. The U.S. Privacy Act of 1974[8] governs how the federal government manages personal information in its possession, while the Electronic Communications Privacy Act of 1986[9]

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (Data Protection Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of National Persons with Regard to the Processing of Personal Data and the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1626568561070&from=EN.

[6] GDPR Articles 44-50. For more information on the GDPR, see CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick.

[7] For additional information on U.S. privacy law, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

[8] 5 U.S.C. §552a. The Privacy Act covers personal records maintained by federal agencies.

[9] 18 U.S.C. §2510 et seq.

extended government restrictions on telephone wiretaps to include computer transmissions of electronic data.

Congress has enacted a number of laws designed to provide statutory protections of individuals' personal information. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. For example, with a data-specific approach to regulating data privacy, U.S. laws protect specific information such as health care or financial data. The Federal Trade Commission (FTC) may bring enforcement actions against companies who mislead consumers about their privacy practices, but the FTC does not have the mandate to enforce broad online privacy protections. Some stakeholders see self-regulation through industry best practices, codes of conduct, and voluntary standards (among other possible measures) as advantageous in quickly evolving areas, such as artificial intelligence, because they may allow companies to readily adapt to changes in innovation and technology while providing a more market-oriented solution. Companies may use such mechanisms as a way to enhance their brand and build consumer trust, but this approach relies on self-policing rather than government authority for enforcement.[10]

Many U.S. officials and industry representatives maintain that the U.S. sectoral approach to data privacy is more nimble than what they view as the EU's "one-size-fits-all" regulatory approach. They also contend that the U.S. approach helps promote and sustain U.S. technological innovation.[11] Nevertheless, some U.S. privacy advocates argue that there are gaps in the U.S. approach, especially in the area of online data collection, and note that public demands for stronger protections appear to be growing amid data breaches and misuse at companies such as Facebook, Apple, Amazon, and others over the last several years.[12] Some states, including California and Virginia, have implemented state-level data privacy laws based, in part, on the EU's GDPR.[13] Congress is currently debating potential comprehensive national policy on data privacy and Members have proposed various bills on data protection and security.[14]

Transatlantic Data Flows and Trade

"Cross-border data flows" refers to the movement or transfer of information between computer servers across national borders. Such data flows underlie today's globally connected world and are essential to conducting international trade and commerce. Cross-border data flows enable

[10] Siona Listokin, "Industry Self-Regulation of Consumer Data Privacy and Security," George Mason University, 2015.

[11] Natasha Singer, "Data Protection Laws, An Ocean Apart," *New York Times*, February 2, 2013; Alan McQuinn and Daniel Castro, "Why Stronger Privacy Protections Do Not Spur Increased Internet Use," Information Technology and Innovation Foundation, July 11, 2018; Bret Swanson, "Securing the Digital Frontier: Policies to Encourage Data Privacy, Data Security, and Open-Ended Innovation," American Enterprise Institute, May 31, 2019.

[12] Nuala O'Connor, "Reforming the U.S. Approach to Data Protection and Privacy," Council on Foreign Relations, January 30, 2018; Daniel Castro, "It's Time for a New Approach to Solving America's Data Privacy Dilemma," Information Technology and Innovation Foundation, March 17, 2021.

[13] California Privacy Rights Act is codified as Cal. Civ. Code §§ 1798.100-1798.199.100 and Virginia Consumer Data Protection Act, 2021 ch. 35 (to be codified at Va. Code Ann. §§ 59.1-571-59.1-581). For more information, see "GDPR v. CCPA: What You Need to Know," *American Marketing Association*, https://www.ama.org/pages/california-consumer-privacy-protection-act-what-you-need-to-know/ and Arent Fox, "Virginia Consumer Data Protection Act: Here Comes the Next State Privacy Law of the Land," *JDSUPRA*, March 8, 2021, athttps://www.jdsupra.com/legalnews/virginia-consumer-data-protection-act-2724869/.

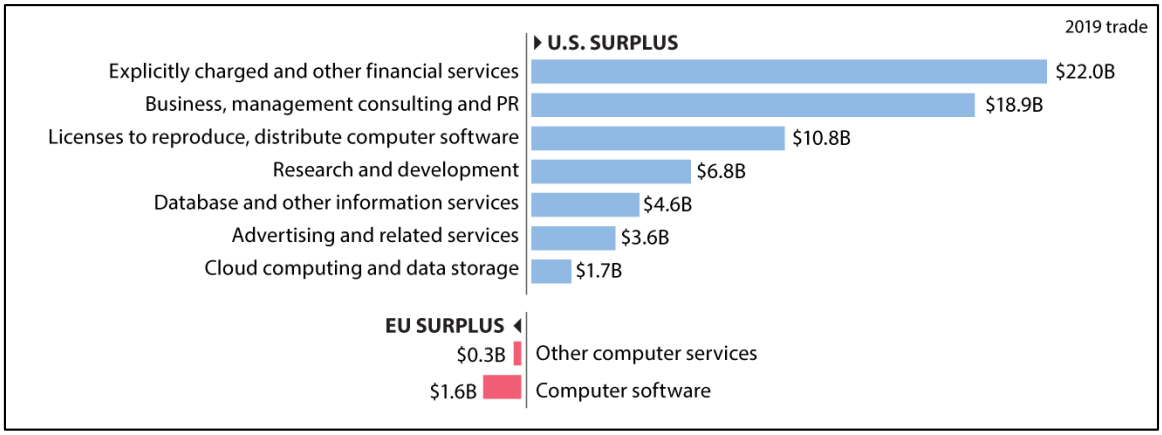
[14] See, for example, from the 117th Congress, S. 224, H.R. 1816, H.R. 4801, S. 2499. For more information, see CRS Legal Sidebar LSB10441, *Watching the Watchers: A Comparison of Privacy Bills in the 116th Congress*, by Jonathan M. Gaffney.

people and companies to transmit information for online communication, track global supply chains, share research, provide cross-border services, and support technological innovation.

The United States and the EU share an extensive, highly integrated trade and investment relationship. Cross-border data flows between the United States and EU are the highest in the world and are integral to much of the U.S.-EU economic relationship. Total U.S.-EU trade in goods and services (exports plus imports) is typically valued at around $1 trillion per year.[15] U.S.-EU trade of information and communications technology (ICT) services and potentially ICT-enabled services was valued at over $264 billion in 2020.[16] The United States maintains a relatively large digital trade surplus over the EU (see **Figure 2**). According to one study, two of the top five e-commerce retailers in Europe in 2020 were U.S. firms Amazon and Apple.[17]

Figure 2. U.S.-EU Digitally Enabled Services Trade Flows

2019



Source: Mark Scott, "Digital Bridge," *Politico*, April 1, 2021, based on U.S. Bureau of Economic Analysis data.

Transatlantic data flows include both personal and non-personal data. Organizations rely on the transmission of information to use cloud services, and to send non-personal corporate data, as well as personal data to partners, subsidiaries, and customers. Organizations value consumers' personal online data for a variety of reasons. For example, companies may seek to facilitate business transactions, analyze marketing information, detect disease patterns from medical histories, discover fraudulent payments, improve proprietary algorithms, or develop competitive innovations. Some analysts compare data to oil or gold, but many also note that, unlike those valuable substances, data can be reused, analyzed, shared, and combined with other information; it is not a scarce resource.[18]

Personal data is viewed as personal private property. Individuals often want to control who accesses their data and how it is used. The United States has traditionally supported open data flows, and U.S. trade policy has sought to balance the goals of maintaining consumer privacy,

[15] Also see, CRS In Focus IF10930, *U.S.-EU Trade and Investment Ties: Magnitude and Scope*, by Shayerah Ilias Akhtar.

[16] U.S. Bureau of Economic Analysis, Table 3.3. U.S. Trade in ICT and Potentially ICT-Enabled Services, by Country or Affiliation.

[17] Retail-Index, *Top 100 E-Commerce Retailers in Europe*, https://www.retail-index.com/E-commerceretail.aspx.

[18] For example, see Antonio Garcia Martinez, "No, Data Is Not the New Oil," *Wired*, February 26, 2019, or Kiran Bhageshpur, "Data Is The New Oil – And That's A Good Thing," *Forbes*, November 25, 2019.

security, and open commerce, including eliminating trade barriers and opening markets. In passing Trade Promotion Authority (TPA), Congress specified digital trade policy objectives for U.S. trade negotiations including to "ensure that governments refrain from implementing trade-related measures that impede digital trade in goods and services, restrict cross-border data flows, or require local storage or processing of data," while allowing exceptions for legitimate policy objectives that are nondiscriminatory and promote an open market environment.[19] Despite common underlying democratic principles and norms, differences in how the United States and the EU approach data protection have ramifications for digital flows and international trade and have, at times, disrupted U.S.-EU data flows.

Various studies have attempted to quantify the economic importance of cross-border data flows. Studies and estimates vary widely given the difficulty in quantifying intangible data flows that often are not measured or associated with monetary transactions (e.g., internal corporate transactions or free online services). Many of these studies focus on estimating the impact of potential EU restrictions on cross-border data flows.

- One study measured the statistical impact of restrictions on data flows on a country's economy, calculating that a one-point increase in a nation's data restrictiveness reduces gross trade output 7%, slows productivity 2.9%, and increases downstream prices 1.5% over five years.[20] While the report cited China, Indonesia, Russia, and South Africa as the most restrictive, it named Europe a "leading offender" of protectionist data localization policy justified by EU leaders' calls for digital and data sovereignty.
- One report stated that a loss of cross-border data flows on exports from the EU's data-reliant sectors would lead to an annual reduction in the EU's gross domestic product (GDP) worth at least €330 billion (roughly $388 billion), or around 2.5% of total EU GDP.[21]
- Another study attempted to quantify the impact of curtailed cross-border data flows for specific EU sectors including telecommunications, digital payments, global services outsourcing, and pharmaceutical research and development.[22] For example, the research estimated that restrictions on transfer of personal data outside of the EU would result in lost transactions of digital payments of €128 million per day ($150 million) immediately, and up to €4.2 billion to €9.3 billion ($5.0-$11.0 billion) per year. Such restrictions could impede drug development, for example, by hindering scientists and medical researchers from aggregating sufficient genomic and medical data, thereby increasing costs and reducing patient outcomes. The study estimated that this would have added €70 billion ($82.6 billion) in damage to the EU economy for each month of delay in the approval of the COVID-19 vaccine.
- Specific to the transatlantic economy, an analysis of cross-border data flows from the EU to the United States calculated that a total ban on such data transfers

[19] Bipartisan Congressional Trade Priorities and Accountability Act of 2015, Title I, (b)(6) (P.L. 114-26).

[20] The authors used an econometric model to calculate a composite index of a country's data restrictiveness. Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology and Innovation Foundation, July 19, 2021.

[21] Frontier Economics, "The Value of Cross-Border Data Flows to Europe: Risks and Opportunities," June 2021.

[22] Rozi Kepes, et al., "The Importance of Cross-border Data Flows – An Economic Assessment of Restrictions on Extra-EU Data Transfers," Analysis Group, June 2021.

could result in a loss of up to €420 billion ($493 billion) of EU GDP. Such a ban could lead to a 31% decline in digital service imports from the United States. The study also calculated that the invalidation of the Privacy Shield alone could reduce bilateral digital services trade by 6% and cost the EU up to €31 billion ($36 billion) in economic output while U.S. GDP could decline by 0.01%.[23]

U.S.-EU Data Transfer Accords: From Safe Harbor to Privacy Shield

The Safe Harbor Framework

Following the EU's adoption of its Data Protection Directive in 1995, the United States and the EU began negotiations on devising a mechanism that would allow U.S. businesses and organizations to meet the "adequate" level of data protection required by the DPD and thus prevent the disruption of the transfer of personal data from the EU. In 2000, U.S.-EU negotiations resulted in the Safe Harbor Privacy Principles, issued by the U.S. Department of Commerce.[24] The European Commission recognized that U.S. companies that complied with these principles met EU requirements to allow the transfer of personal data from the EU; in granting this so-called "adequacy decision," the European Commission also noted that application of the effective principles could be limited to the extent necessary for national security, public interest, or law enforcement requirements.[25] The Safe Harbor mechanism was developed by the executive branch and did not require specific congressional approval.

Under Safe Harbor, a U.S. company or organization could self-certify annually to the Department of Commerce that it was in compliance with seven basic privacy principles (notice, choice, onward data transfer, security, data integrity, access, and enforcement) and related requirements deemed necessary to meet the EU's data protection adequacy standards. Participation in Safe Harbor was open to any U.S. organization subject to regulation by the FTC, which included most entities other than certain exempted entities such as nonprofits, banks, and common carriers,[26] and to U.S. air carriers and ticket agents subject to regulation by the Department of Transportation (DOT). The FTC committed to reviewing all referrals from EU member state authorities of potential Safe Harbor violations. Entities that did not fall under FTC or DOT jurisdiction were not eligible for Safe Harbor.

CJEU *Schrems I* Decision

In October 2015, the CJEU delivered a judgement that invalidated the Safe Harbor accord.[27] The CJEU decision stemmed from a complaint initially brought to Ireland's data protection authority

[23] European Centre for International Political Economy and Kearney Global Business Policy Council, "The Economic Costs of Restricting the Cross-border Flow of Data," July 2021.

[24] U.S. Department of Commerce, *Safe Harbor Privacy Principles and Related Frequently Asked Questions*, July 21, 2000.

[25] Commission Decision 2000/520/EC of July 26, 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 U.S. Department of Commerce, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520.

[26] 15 U.S.C. §§ 44–45.

[27] Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, October 6, 2015, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362.

(DPA) by an Austrian national, Maximillian Schrems, concerning Facebook's transfer of some or all of his data from Facebook's EU-based servers in Ireland to its servers located in the United States. Schrems lodged his complaint with Ireland's DPA in light of the 2013 leaks of U.S. NSA surveillance activities. Although Ireland's DPA dismissed Schrems' complaint, Schrems appealed to the Irish High Court, which referred the matter to the CJEU.

In the CJEU's ruling—which has become known as *Schrems I*—the court found that the European Commission failed to examine U.S. domestic laws or international commitments (as required by the DPD) prior to issuing its determination that the Safe Harbor principles provided an adequate level of protection for EU citizens' personal data. In addition, the CJEU ruling held that U.S. national security, public interest, and law enforcement requirements had "primacy" over the Safe Harbor principles, and that U.S. undertakings were bound to disregard, without limitation, the protective rules laid down by Safe Harbor where they conflicted with such requirements. Consequently, the CJEU concluded that the Safe Harbor scheme "enables interference" by U.S. authorities "with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States." Furthermore, the CJEU noted that the European Commission did not consider either the existence of U.S. rules or effective U.S. legal protections intended to limit such interference, such as the possibility of judicial redress, when finding that the Safe Harbor principles provided adequate data protection.[28]

At the time of the CJEU's *Schrems I* decision, approximately 4,500 companies and organizations were participating in Safe Harbor. U.S. officials and business leaders were disappointed by the CJEU's ruling and concerned that it could disrupt data flows from the EU, with significant negative implications for U.S.-EU trade and economic relations. EU data protection authorities, however, announced a four-month grace period during which they agreed to not enforce the *Schrems I* decision while U.S. and EU officials continued negotiations on a new agreement.[29]

Negotiating Privacy Shield

Although the Safe Harbor framework applied to a wide range of businesses and organizations that collect and hold personal data, the internet was still in its infancy at the time it was concluded in 2000. The range of public and private actors engaged in the mass processing of personal data, including across borders, was much more limited than it is today. The CJEU's ruling gave added impetus to U.S.-EU negotiations underway since late 2013 aimed at "making Safe Harbor safer."[30] These discussions were part of several initiatives seeking to restore transatlantic trust in the security of U.S.-EU data flows following the unauthorized disclosures of NSA surveillance programs and activities. U.S.-EU negotiations on a successor agreement to Safe Harbor also took into consideration the changes and reforms anticipated in the EU's GDPR.

In February 2016, U.S. and EU officials announced an agreement, "in principle," on a replacement for Safe Harbor—the U.S.-EU Privacy Shield. As discussed in greater detail below and similar to the former Safe Harbor accord, the Privacy Shield Framework requires compliance with seven basic privacy principles. In contrast to Safe Harbor, however, Privacy Shield sought to address the concerns raised by the CJEU in *Schrems I*. In particular, the Privacy Shield agreement contained written assurances in letters from U.S. officials that U.S. government access to EU citizens' personal data would be subject to limitations, and outlined redress mechanisms,

[28] Also see, Court of Justice of the European Union, "The Court of Justice Declares that the Commission's US Safe Harbour Decision Is Invalid," press release, October 6, 2015.

[29] Article 29 Working Party, "Statement of the Article 29 Working Party," press release, October 16, 2015.

[30] European Commission, "European Commission Calls on the U.S. To Restore Trust in EU-U.S. Data Flows," press release, November 27, 2013.

including the creation of a Privacy Shield Ombudsman at the U.S. Department of State to handle complaints from EU citizens' about possible access to their personal data by U.S. national security authorities (see "Privacy Shield Framework," below).

Many U.S. business and industry leaders expressed a hope that concurrent congressional efforts to provide a limited right of judicial redress to EU citizens would also help to restore EU trust in U.S. data protection standards and bolster confidence in Privacy Shield.[31] In 2015, before the *Schrems I* ruling, legislation was introduced in Congress to address EU judicial redress demands and help conclude a separate U.S.-EU data protection accord for law enforcement purposes (known as the U.S.-EU Data Protection Umbrella Agreement).[32] In February 2016, Congress passed the resulting U.S. Judicial Redress Act (P.L. 114-126), extending certain judicial redress provisions in the U.S. Privacy Act of 1974 to EU citizens. The scope of the Judicial Redress Act is limited, however, and relates specifically to personal information of EU citizens transferred in a law enforcement context.[33] The Judicial Redress Act also includes provisions mandating that the Act is applicable only to citizens of countries or regional organizations that also permit the transfer of personal data for commercial purposes to the United States and whose data transfer policies "do not materially impede the national security interests of the United States."[34]

In July 2016, the European Commission adopted an adequacy decision for Privacy Shield, formally designating the new program as a valid mechanism for transferring personal data for commercial purposes to the United States. The European Commission noted in particular its confidence that "any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred…will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective [U.S.] legal protection against such interference."[35] Privacy Shield became operational on August 1, 2016. Like the former Safe Harbor agreement, Privacy Shield was negotiated as an executive branch accord and, thus, did not require congressional approval.

---

[31] Cat Zakrzewski, "Tech Firms Support Bill Expanding Privacy Rights to Non-EU Citizens," TechCrunch.com, September 16, 2015; Information Technology Industry Council, "ITI Statement on the Senate's Passage of the Judicial Redress Act," press release, February 9, 2016; Heather Greenfield, "President Obama Signs Judicial Redress Act – Key to Improving Transatlantic Trust," Computer and Communications Industry Association, February 25, 2016; Adam Schlosser, "Progress Made in Fixing Transatlantic Data Fiasco; Obama Signs Data Judicial Redress Act," U.S. Chamber of Commerce, February 25, 2016.

[32] In 2011, the United States and the EU began negotiations on this "umbrella" accord to bridge differences in the application of privacy rights, better protect personal information exchanged in a law enforcement context, and help make the negotiation of future U.S.-EU data-sharing accords for law enforcement purposes easier. Throughout the negotiations, EU demands for judicial redress for EU citizens posed a hurdle. In September 2015, negotiators finalized and initialed the text of the umbrella agreement, but the EU asserted that it would not sign it until the United States adopted judicial redress legislation. Following passage of the U.S. Judicial Redress Act, the EU signed the umbrella agreement in May 2016 and it was formally adopted in December 2016. See, Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, December 10, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN.

[33] Mary Ellen Callahan, Nancy Libin, Lindsay Bowen, "Will the Judicial Redress Act Address Europeans' Privacy Concerns?," *Privacy Tracker*, March 2, 2016; Mark L. Krotoski, et al., "The Judicial Redress Act of 2015 Becomes Law," *National Law Review*, March 3, 2016.

[34] U.S. Department of Justice, *Judicial Redress Act of 2015 and U.S.-EU Data Protection and Privacy Agreement*, https://www.justice.gov/opcl/judicial-redress-act-2015.

[35] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN.

U.S. and EU officials claimed that, compared with Safe Harbor, Privacy Shield contained significantly stronger privacy protections and oversight mechanisms, multiple redress possibilities, and new safeguards related to U.S. government access to personal data. Nevertheless, questions existed at the time of its approval about whether Privacy Shield would go far enough in addressing broader EU concerns about U.S. data protection standards, and whether it would be able to stand up to future legal challenges to it at the CJEU.[36]

Privacy Shield Framework[37]

Key Principles and Implementation

The Privacy Shield Framework is substantially longer and more detailed than the previous Safe Harbor accord. The Privacy Shield Framework requires adherence to seven distinct privacy principles (see **text box "EU-U.S. Privacy Shield Principles"**). The Framework also sets out 16 mandatory supplemental principles that include provisions on sensitive data, secondary liability, the role of DPAs, human resources data, pharmaceutical and medical products, and publicly available data. The Framework clarifies an organization's responsibilities for compliance, and provides a model for binding arbitration to address "residual" complaints.

EU-U.S. Privacy Shield Principles

(1) Notice to provide transparency to individuals
(2) Choice allowing individuals to opt out
(3) Accountability for onward data transfer for when data is sent to a third party
(4) Security to protect data collected
(5) Data integrity and purpose limitation for personal data collection
(6) Access of individuals to personal data collected
(7) Recourse, enforcement and liability for compliance

To voluntarily join the Privacy Shield program, a U.S.-based organization self-certifies annually to the Department of Commerce, publicly committing to comply with the Framework's principles and requirements that are enforceable under U.S. law. While decisions by organizations to participate in the Privacy Shield program are voluntary, once an organization opts in, effective compliance is compulsory (see "Enforcement," below).

As noted above, in contrast to the former Safe Harbor accord, the Privacy Shield Framework contains written assurances from U.S. authorities, including letters from the U.S. Department of Justice and the Office of the Director of National Intelligence, guaranteeing that U.S. access to EU citizens' personal data will be subject to limitations, safeguards, and oversight mechanisms. The European Commission and the Department of Commerce conduct annual joint reviews of the program and invite U.S. national intelligence experts and European DPAs to participate.

Any EU citizen who considers that his or her personal data has been compromised under Privacy Shield also has multiple redress possibilities. Individuals may complain directly to companies or to EU DPAs, which are able to refer unresolved complaints to the FTC. Furthermore, Privacy Shield provides claimants with a free alternative dispute resolution mechanism in the event that the FTC does not pursue an individual's case. As noted above, a Privacy Shield Ombudsman at the U.S. Department of State handles complaints on possible access and misuse of EU citizens'

[36] See, for example, Natasha Lomas, "Europe and U.S. Seal Privacy Shield Data Transfer Deal to Replace Safe Harbor," Techcrunch.com, February 2, 2016; Julia Fioretti, "U.S. Reluctant to Change Data Pact after EU Watchdogs' Concerns," Reuters, April 20, 2016.

[37] For the entire text of the EU-U.S. Privacy Shield Framework (including the Privacy Shield principles issued by the U.S. Department of Commerce and U.S. Government letters on the framework's oversight and enforcement), see https://www.privacyshield.gov/EU-US-Framework.

personal data by U.S. national security agencies. The Ombudsman is independent of the intelligence agencies, but has clearance to review issues referred by EU DPAs.

Enforcement

The Privacy Shield Framework is administered by the Department of Commerce and the European Commission. Commerce monitors firms' effective compliance and investigates complaints. Despite the CJEU's 2020 decision invalidating Privacy Shield (see below), Commerce has stated it will continue to administer the Framework and that the ruling "does not relieve participating organizations of their Privacy Shield obligations," noting that "continued participation in the EU-U.S. Privacy Shield demonstrates a serious [U.S.] commitment to protect personal information in accordance with a set of privacy principles that offer meaningful privacy protections and recourse for EU individuals."[38]

The FTC and DOT enforce compliance.[39] In June 2020, the FTC reported enforcement actions against dozens of companies that made false or deceptive representations about their Privacy Shield participation.[40] The FTC's $5 billion penalty against Facebook included holding executives accountable for privacy-related decisions and prohibiting misrepresentations related to Privacy Shield.[41]

The U.S. Department of State Under Secretary of State for Economic Growth, Energy, and the Environment currently serves as the independent Privacy Shield Ombudsperson to handle complaints regarding U.S. government access to personal data.[42] The Under Secretary works with other U.S. officials, including independent oversight bodies such as inspectors general, to resolve requests submitted by individuals through the ombudsperson mechanism.

The U.S. Privacy and Civil Liberties Oversight Board (PCLOB), while not formally part of the Privacy Shield arrangement, is responsible for oversight of the implementation of executive branch counterterrorism efforts, including surveillance practices and policies, to ensure that privacy and civil liberties are protected.[43] In the first annual review of Privacy Shield, the European Commission recommended that the United States fill the then-vacancies on the PCLOB and release its latest oversight reports.[44] The Senate confirmed President Trump's two nominees in 2018, before the second annual review, to fill the five-person board. The PCLOB published its latest oversight reports on Executive Order (E.O.) 12333 in April 2021 and on Presidential Policy

[38] U.S. Department of Commerce, "U.S. Secretary of Commerce Wilbur Ross Statement on *Schrems II* Ruling and the Importance of EU-U.S. Data Flows," press release, July 16, 2020, and Privacy Shield Framework, "FAQs – EU-U.S. Privacy Shield Program Update," March 31, 2021, https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update.

[39] See https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield.

[40] Lesley Fair, "FTC Settlement Focuses on those Other Privacy Shield Framework Requirements," Federal Trade Commission, June 30, 2020.

[41] "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," Federal Trade Commission July 24, 2019.

[42] See https://www.state.gov/privacy-shield-ombudsperson/.

[43] See https://www.pclob.gov/.

[44] European Commission, "First Annual Review of the EU-U.S. Privacy Shield," October 18, 2017.

Directive 28 (PPD-28) in October 2018.[45] There are currently two members of the PCLOB, as three members' terms expired in 2021.[46]

In September 2019, EU and U.S. officials held their third annual review of the administration and enforcement of Privacy Shield. The EU cited progress in U.S. oversight and enforcement actions, but noted concern about a "lack of oversight in substance" and the need for more checks for onward transfers, issues similar to those cited by the CJEU.[47] No review was conducted in 2020 and none has been announced for 2021 due to the CJEU invalidation.

Invalidation of Privacy Shield

CJEU *Schrems II* Decision

Following the CJEU's *Schrems I* ruling in 2015 invalidating Safe Harbor, Facebook Ireland said it was transferring most data to its U.S. servers using standard contractual clauses (SCCs), another approved EU mechanism for transferring personal data between EU and non-EU countries. SCCs are model contract terms "pre-approved" by the EU to ensure that data transferred is protected according to EU-equivalent standards (for more information on SCCs, see "Implications for Business"). Privacy activist Maximillian Schrems lodged another complaint with Ireland's DPA, challenging the ability of SCCs to provide an adequate level of data protection given that U.S. surveillance laws could allow U.S. authorities access to personal data transferred to Facebook servers in the United States. Ireland's DPA brought the case before Ireland's High Court, which subsequently referred questions about the validity of SCCs to the CJEU.

Schrems was not the only one to challenge the cross-border transfer of personal data from the EU to the United States. In 2016, a French digital privacy advocacy group (*La Quadrature du Net*) brought a separate complaint against Privacy Shield directly before the CJEU. The French privacy group contended that Privacy Shield, similar to the former Safe Harbor accord, failed to protect EU citizen's personal data in light of U.S. surveillance laws and activities.[48]

In a judgement issued in July 2020—known as *Schrems II*—the CJEU decided to address the validity of both SCCs and Privacy Shield given the similar issues raised in both cases.[49] The CJEU determined that:

- **Privacy Shield is not a valid mechanism for transferring personal data from the EU to the United States.** The CJEU rejected the European Commission's determination that the United States ensures an adequate level of protection for data transferred under the Privacy Shield Framework, given the breadth of U.S. data collection powers authorized in U.S. electronic surveillance laws and the

[45] Privacy and Civil Liberties Oversight Board, "Executive Order 12333," April 2, 2021, and "Presidential Policy Directive 28 (PPD-28) Report," October 16, 2018, redacted versions available at https://www.pclob.gov/Oversight.

[46] https://www.pclob.gov/Board/Index.

[47] European Data Protection Board, *EU-U.S. Privacy Shield - Third Annual Joint Review,* November 12, 2019.

[48] See, for example, Electronic Privacy Information Center, *Data Protection Commissioner v. Facebook Ireland and Max Schrems (Irish High Court),* https://epic.org/privacy/intl/dpc-v-facebook/ireland/; Natasha Lomas, "EU-US Privacy Shield Complaint to be Heard by Europe's Top Court in July," TechCrunch.com, May 28, 2019; Kenneth Propp, "Return of the Transatlantic Privacy War," Atlantic Council, July 20, 2020.

[49] Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems,* July 16, 2020, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0311.

lack of redress options for EU citizens. The CJEU found that Section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA) and E.O. 12333—which authorize surveillance of non-U.S. persons located outside of the United States—allow U.S. intelligence agencies to collect more information than is strictly necessary. Furthermore, although Presidential Policy Directive 28 (PPD-28) issued by President Obama prohibits certain bulk data collection and limits retention periods for information on non-U.S. persons, the CJEU judgment asserted "PPD-28 does not provide data subjects with actionable rights before the courts against U.S. authorities."[50] The CJEU also questioned the independence of the Privacy Shield Ombudsperson and held that the ombudsperson could not provide sufficient redress because it was not evident that the ombudsperson has the power to adopt binding decisions on U.S. intelligence services.

- **SCCs remain valid but data exporters must take into account the legal systems of "third countries" (i.e., non-EU countries) to ensure an adequate level of data protection.** The CJEU reasoned that SCCs are inherently of a "contractual nature" and thus "cannot bind the public authorities of third countries." The CJEU ruling, however, essentially increases due diligence requirements for companies and organizations using SCCs to transfer personal data outside of the EU. The CJEU ruled that when relying on SCCs, data exporters must "verify, on a case-by-case basis" whether the laws of third countries afford EU citizens a level of data protection equivalent to that guaranteed under EU law, and adopt "supplementary measures" if necessary to compensate for any shortfalls. If additional measures cannot guarantee adequate data protection, data exporters must suspend the data transfers.[51]

Guidance for Privacy Shield Organizations

Unlike after the invalidation of the Safe Harbor program, the EU did not grant a grace period after *Schrems II,* during which an organization could continue to use Privacy Shield as a legal basis for data transfers. In July 2020, the European Data Protection Board (EDPB) issued a Frequently Asked Questions document to help Privacy Shield organizations understand the implications of the CJEU ruling and options for entities conducting cross-border data flows.[52] The document clarified that the burden falls on the individual organization to take extra steps in order to ensure compliance with the court judgment. The EDPB later issued guidance and recommendations for organizations using SCCs, providing supplementary information and outlining specific measures (such as encryption or pseudonymization) that companies could take to make sure they meet EU data protection requirements.[53] In June 2021, the EU also updated the SCCs to better reflect

[50] For more information on Section 702 of FISA, E.O. 12333, and PPD 28, see CRS Report R46724, *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield*, by Chris D. Linebaugh and Edward C. Liu.

[51] Also see, Law Library of Congress, "European Union: Court of Justice Invalidates U.S.-EU Privacy Shield," *Global Legal Monitor*, August 4, 2020; Hendrik Mildebrath, "The CJEU Judgment in the Schrems II Case," European Parliamentary Research Service, September 2020.

[52] The EDPB is an independent body composed of representatives of all EU member state data protection authorities and the European Data Protection Supervisor (EDPS). The EDPB contributes to the consistent application of data protection rules throughout the EU and promotes cooperation among the national DPAs in the EU. European Data Protection Board, "Frequently Asked Questions on the Judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems," July 23, 2020.

[53] European Data Protection Board, *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure*

GDPR requirements and, in light of the *Schrems II* decision, to ensure that personal data transferred using SCCs receives a level of protection equivalent to that under EU law.[54]

In September 2020, shortly after the CJEU ruling, the Department of Commerce released a white paper to assist organizations that continue to participate in Privacy Shield to assess whether their transfers offer appropriate data protection in accordance with the CJEU's ruling.[55] The paper provides a wide range of information about privacy protections in current U.S. law and practice relating to government access to data for national security purposes. The paper is publicly available so organizations can strengthen their argument for data transfers and evaluate their risk of noncompliance with the CJEU judgment. It specifies that "most U.S. companies do not deal in data that is of any interest to U.S. intelligence agencies, and have no grounds to believe they do. They are not engaged in data transfers that present the type of risks to privacy that appear to have concerned the ECJ in *Schrems II*."[56]

Industry groups have also provided guidance to their members. For example, the Business Software Alliance published "Seven Principles for Additional Safeguards to Supplement SCCs" to provide legal, technical, and organizational measures for companies to safeguard data in the event of government requests.[57] The CJEU ruling does not affect specific derogations identified in the GDPR that allow for the transfer of personal data outside of the EU (such as when needed to perform a contract or if there is explicit consent).[58]

Implications for Business

According to one study, the invalidation of the Privacy Shield framework may result in a five to six percent reduction in imports and exports of digital services and lead to €19-31 billion ($22-36 billion) in lost EU economic output annually.[59] The researchers noted that the U.S. losses would not be as great if resources shifted to other non-digital sectors. At the time of the CJEU's July 2020 *Schrems II* decision invalidating Privacy Shield, the program had 5,380 participants, 75% of which were SMEs. Privacy Shield participants include U.S. businesses and other organizations, U.S. subsidiaries in Europe, and 250 entities headquartered in Europe. By June 2021, about a year after the *Schrems II* decision, the number of organizations participating in Privacy Shield fell to 4,166, as many sought alternatives (see below) or opted to exit the EU market.[60]

The CJEU decision has created uncertainty for companies enrolled in Privacy Shield and also for those who rely on SCCs. Given the CJEU finding that U.S. surveillance authorities render U.S. data protections inadequate, some experts suggest that SCCs may not be usable in practice for social media and ICT companies subject to U.S. electronic surveillance laws. The EDPB

Compliance with the EU Level of Protection of Personal Data, November 10, 2020, and updated version 2.0 dated June 18, 2021.

[54] European Commission, *Standard Contractual Clauses for International Transfers*, June 4, 2021, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

[55] U.S. Department of Commerce, *Letter from Deputy Assistant Secretary James Sullivan on the Schrems II Decision*, September 28, 2020.

[56] Ibid.

[57] Business Software Alliance, "Principles: Additional Safeguards for SCC Transfers," October 22, 2020.

[58] EU GDPR, Article 49, Derogations for specific situations.

[59] European Centre for International Political Economy and Kearney Global Business Policy Council, "The Economic Costs of Restricting the Cross-border Flow of Data," July 2021.

[60] Privacy Shield list, data pulled on June 10, 2021, https://www.privacyshield.gov/list.

recommendations, noted above, acknowledge that there are some scenarios in which even "supplementary measures" are not sufficient to eliminate the risks of foreign intelligence surveillance and permit SCC-based data transfers. Facebook Vice-President for Global Affairs and Communications, Nick Clegg, noted this dilemma, stating that "many companies, in keeping and in common with Facebook, would find it difficult to provide our services as they are presently constituted, if data no longer has a legal basis upon which it can be transferred from one side of the world to the other."[61]

Apart from Privacy Shield, U.S. firms have limited options for cross-border data flows with the EU. They include:

- Create Binding Corporate Rules (BCRs) that EU officials must approve on a firm-by-firm basis.
- Implement updated EU-approved SCCs and reassess for adequate safeguards according to the CJEU ruling.
- Use commercial cloud services provided by large technology firms that use approved BCRs or updated SCCs (e.g., Microsoft, IBM).
- Store EU citizens' personal data only in the EU or other approved country (known as *data localization*), an idea advocated by some European DPAs and other stakeholders.
- Obtain consent from individuals for every single transfer of personal data, likely a logistically challenging and costly option for many entities.
- Exit or limit participation in the EU market.

BCRs and SCCs are approved mechanisms in the GDPR,[62] but they have some drawbacks for businesses, including potentially higher operating costs (see **text box "Standard Contractual Clauses and Binding Corporate Rules"** for more information). Although data localization is increasingly raised as a practical option, the United States has generally viewed the imposition of data localization policies as a trade barrier and has sought and negotiated commitments in its recent trade agreements to prohibit it, and companies and organizations would have to consider possible downsides. These could include data disruption, the financial costs of setting up data centers, complexities in segregating EU data, increasing an entity's cybersecurity risk, and losing the efficiency gains of aggregated data.[63] The U.S. Trade Representative cited GDPR and EU data localization requirements as trade barriers for U.S. businesses in the agency's annual report.[64]

Business groups and a number of analysts contend that in the absence of a successor to Privacy Shield, European DPAs could increasingly take action to interrupt data transfers to the United States. The U.S. Chamber of Commerce notes several examples in which European DPAs have ordered European entities to stop data transfers to small U.S. companies, and some DPAs have raised concerns about European government officials using certain U.S. digital services, such as Microsoft's cloud hosting services.[65] Also, in May 2021, Ireland's High Court backed the Irish

[61] Mark Scott, "Facebook's Clegg: Stopping Data Transfers Would Have 'Profound Consequences'," *Politico Pro*, June 21, 2021.

[62] GDPR Articles 46 and 47.

[63] Nigel Cory, "Cross-Border Data Flows," Information Technology & Innovation Foundation, May 3, 2018.

[64] U.S. Trade Representative, *2021 National Trade Estimate Report on Foreign Trade Barriers*, March 1, 2021, p. 215-216.

[65] Evangelos Razis, "U.S. Businesses Face the Specter of Data Localization in Europe," U.S. Chamber of Commerce, June 1, 2021; Kenneth Propp, "Progress on Transatlantic Data Transfers? The Picture After the US-EU Summit,"

DPA's preliminary view in a case against Facebook that the company cannot use SCCs to transfer personal data from Facebook Ireland to the United States without additional safeguard measures in light of the CJEU's *Schrems II* ruling.[66] Some analysts have cautioned that the ruling could lead to more legal challenges of U.S. companies who rely on SCCs for data transfers.

Standard Contractual Clauses and Binding Corporate Rules

Standard Contractual Clauses (SCCs) are template contract terms set by the EU that require the organization receiving the data to commit to EU equivalent standards of data protection, even where none exists in domestic legislation. In addition, SCCs set out who is liable, determine in which jurisdiction disputes will be settled, and give data subjects legal standing to pursue complaints.

According to a 2020 study by European trade associations, SCCs are the most widely used mechanism for data transfers, and 90% of the SCCs are used for business-to-business data transfers. The study found that 70% of SMEs used SCCs.

In general, the costs associated with using SCCs are higher than those associated with participating in Privacy Shield. The costs vary depending on how many SCCs an entity may need (depending on the number of third parties to which it transfers data) and how much information it already has regarding its data collection, management practices, and data flows. One investigation found that most firms will need to hire specialist data compliance and consulting firms to assist with data mapping, data management and auditing. Specifically, data mapping is the biggest challenge cited, as most SMEs lack the knowledge and tools to do so themselves. However, there may be situations where transfers are not possible using SCCs because there are not sufficient supplemental measures in place to eliminate the risks of foreign intelligence surveillance, such as when the recipient needs to have access to the unencrypted data.

Binding Corporate Rules (BCRs) are a mechanism for cross-border data flows for intra-company transfers (e.g., from a European subsidiary to a U.S. headquarters). They must be legally binding and enforced by every concerned member of the corporate or enterprise group. Many companies criticized BCRs as exceedingly complex, costly, and risky because the EU data protection authority in every EU member state where the entity is located needs to approve them. Companies that have such concerns are more likely to use other mechanisms to facilitate cross-border data flows.

Sources: DIGITALEUROPE, et al., *Schrems II Impact Survey Report*, 2020; Nigel Cory, "Comments to the UK Parliament's Subcommittee on International Agreement Regarding U.S.-UK Digital Trade," Information Technology & Innovation Foundation, September 25, 2020.

Notes: For more information on SCCs, see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. For more information on BCRs, see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.

Future Prospects for U.S.-EU Data Flows

U.S.-EU Negotiations on an Enhanced Privacy Shield

Following the *Schrems II* decision in July 2020, the Trump Administration began negotiations with the European Commission on next steps to update or replace Privacy Shield.[67] Building on those efforts, the Biden Administration is continuing negotiations to conclude an enhanced successor agreement to Privacy Shield. The Biden Administration portrays such an accord as important in renewing and strengthening the broad U.S.-EU partnership and as crucial to ensuring

Lawfare, June 25, 2021; Mark Scott, "Digital Bridge," *Politico*, August 26, 2021.

[66] Vincent Manancourt and Mark Scott, "Facebook's US Data Transfers Suffered a Setback in Ireland. Here's What You Need to Know," *Politico Pro*, May 14, 2021.

[67] U.S. Department of Commerce, "Joint Press Statement from U.S. Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders," August 10, 2020.

continued transatlantic data flows for U.S. businesses and industries. The Department of Commerce is leading the negotiations for the United States. Similar to the approach pursued by the Trump Administration, the Biden Administration is reportedly seeking to address EU concerns by providing greater assurances through executive orders and administrative action on how the United States safeguards non-U.S. citizens' personal data and how Europeans can pursue redress in U.S. courts for any alleged misuse of their data.[68]

Some in both the United States and the EU question whether U.S. executive and/or administrative measures would satisfy the European Data Protection Board or, ultimately, the CJEU, and contend that legislative action may be necessary to limit U.S. national security agency access to EU citizens' personal data and/or make it easier for EU citizens to challenge alleged infringements in U.S. courts. In discussing the state of negotiations on a successor to Privacy Shield in late May 2021, European Commission Vice President Věra Jourová asserted that, "On the commercial side, we don't see such a big issue … but of course, there is the issue of access to data from the national security agencies … a legally-binding rule would be very useful, I would even say necessary."[69] Many experts, however, regard U.S. statutory changes to surveillance authorities or providing greater access to U.S. courts for EU citizens via legislation as unlikely in the short term given the political challenges and complexities involved.[70]

Some U.S. officials and outside experts contend that intelligence regimes and surveillance practices in the United States and in EU member states are comparable; they also argue that U.S. surveillance safeguards and oversight mechanisms are robust and possibly stronger than in many EU countries. Because of this, some in the United States bristle at EU demands for changes to U.S. national security legislation and limits on U.S. data collection programs "when European countries themselves are not averse to similar [surveillance] practices," which could potentially target U.S. citizens.[71] Those with this view note that national security is not an EU competence (i.e., member states retain sovereignty over national security policy) and the CJEU therefore does not have authority over member states' surveillance practices. According to one analyst, each EU member state essentially has "the discretion to balance national security needs with data privacy rights. Yet, the EU is not according a similar discretion to third countries. In fact, GDPR uses the threat of withdrawing access to EU personal data as a tool to seek reform of other country's security agencies to reflect the CJEU notion of proportionality, while exempting member state governments from similar expectations or threats."[72]

---

[68] Steven Overly and Mark Scott, "Step One in Repairing U.S.-EU Relations: A Data Privacy Deal," *Politico*, December 4, 2020; Mark Scott, "Biden Seeks High-level Data Deal to Repair EU-US Digital Ties," *Politico*, June 2, 2021. Also see, Alex Greenstein, Director Privacy Shield Negotiations, U.S. Department of Commerce, speaking at Information Technology & Innovation Foundation event, "How Can Countries Support Data Flows, Digital Trade, and Good Data Governance?," July 20, 2021, https://itif.org/events/2021/07/20/how-can-countries-support-data-flows-digital-trade-and-good-data-governance.

[69] As quoted in, Mark Scott and Vincent Manancourt, "Europe to US: Pass New Laws If You Want a Data-transfer Deal," *Politico*, June 1, 2021. Also see, Cameron F. Kerry, "The Oracle at Luxembourg: The EU Court of Justice Judges the World on Surveillance and Privacy," Brookings Institution, January 11, 2021.

[70] See, for example, Kenneth Propp, "Progress on Transatlantic Data Transfers? The Picture After the US-EU Summit," *Lawfare*, June 25, 2021.

[71] Mark Scott, "Privacy Shield Is Stuck," *Politico Digital Bridge*, July 15, 2021. Also see, Joseph Duball, "Senate Hearing Ponders US Remedies for Privacy Shield Invalidation," International Association of Privacy Professionals, December 10, 2020.

[72] Joshua Meltzer, "The Court of Justice of the European Union in *Schrems II*: The Impact of GDPR on Data flows and National Security," Brookings Institution, August 5, 2020. Other experts point out that the CJEU has heard cases on whether certain national data retention and collection laws for national security pupose s are compatible with EU fundamental rights and EU-wide data protection and privacy laws. In an October 2020 ruling, the CJEU found that

U.S.-EU negotiations on an enhanced Privacy Shield are continuing. At the June 2021 U.S.-EU summit, President Biden and EU leaders committed to "work together to ensure safe, secure, and trusted cross-border data flows that protect consumers and enhance privacy protections, while enabling transatlantic commerce…we plan to continue to work together to strengthen legal certainty in transatlantic flows of personal data."[73] On the sidelines of the U.S.-EU summit, U.S. Department of Commerce Secretary Gina Raimondo and European Commissioner for Justice Didier Reynders (the European Commission's lead negotiator on Privacy Shield) also issued a statement asserting their "shared commitment to find a comprehensive successor to Privacy Shield that is fully in line with the *Schrems II* requirements and with US law."[74]

European Commissioner Reynders has reportedly suggested that a successor agreement to Privacy Shield could be reached by the end of 2021. However, other EU officials caution that "speed should not trump quality."[75] U.S. officials express the hope for a "quick resolution" in the negotiations on an enhanced Privacy Shield, but assert that the United States also wants to ensure that a successor accord is "legally defensible because we certainly don't wish this to fall to another legal challenge" at the CJEU.[76]

Alternatives to Privacy Shield

The GDPR specifies various legal means for cross-border data flows and Privacy Shield is not the only option for U.S. organizations that process or store personal data of EU citizens.[77] The absence of a full EU adequacy determination for the United States, however, limits the options for conducting transatlantic data flows. BCRs and SCCs, as explained above, are approved mechanisms under the GDPR and provide ways for companies to comply with EU data protection rules, but may come with additional compliance burdens as compared to Privacy Shield. Derogations in the GDPR allow for cross-border data flows but only in specific circumstances (e.g., when necessary to perform a contract). Some experts suggest that the longer it takes for the United States and the EU to reach an enhanced Privacy Shield accord, the stronger the appeal of storing personal data locally within the EU (data localization) as a possibly faster and more durable solution for U.S. firms that can afford the investment.

Other alternatives would be for the EU to establish codes of conduct or certifications that meet GDPR requirements which organizations could apply to their cross-border data transfers and business practices.[78] These programs could be U.S.-EU specific or at a broader, global level.

Belgian, French, and UK data retention schemes needed to be proportionate, limited, and have strong privacy safeguards—similar to concerns raised by the CJEU in its ruling invalidating Privacy Shield. See Theodore Christakis and Kenneth Propp, "How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—And What It Means for the United States," *Lawfare*, March 8, 2021.

[73] The White House, *U.S.-EU Summit Statement*, June 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/.

[74] U.S. Commerce Secretary Gina Raimondo, Tweet, June 15, 2015, https://twitter.com/SecRaimondo/status/1404848799265267723.

[75] As reported in, Kenneth Propp, "Progress on Transatlantic Data Transfers? The Picture After the US-EU Summit," *Lawfare*, June 25, 2021.

[76] As quoted in, Doug Palmer, "U.S. Wants 'Legally Defensible' Privacy Shield Pact, Commerce Negotiator Says," *Politico Pro*, July 20, 2021. Also see, Vincent Manacourt and Mark Scott, "Washington Says a Transatlantic Data Deal Is Close. Brussels Disagrees," *Politico*, September 17, 2021.

[77] Regulation (EU) 2016/679 (General Data Protection Regulation) Chapter 5: Transfers of Personal Data to Third Countries or International Organisations, https://gdpr-info.eu/chapter-5/.

[78] GDPR Article 46.

Industry stakeholders have sought such programs in the hopes that they would be less cumbersome than SCCs. According to a top official on international data flows and protection at the European Commission, these programs are currently being developed by the European Commission and the EDPB but they will be subject to the same requirements as SCCs.[79] Until finalized codes of conduct or certification programs are implemented, it is not clear if such options would be more or less practical for SMEs conducting cross-border trade.

Potential U.S.-EU Digital Agreement

During the June 2021 U.S.-EU Summit, the two sides announced the formation of a U.S.-EU Trade and Technology Council (TTC) to bolster U.S.-EU cooperation on such issues. Ten separate working groups are to address issues such as emerging technology standards, ICT security, export controls, investment screening, semiconductor supply chains, and joint innovation. The summit also launched a separate U.S.-EU Joint Technology Competition Policy Dialogue, established specifically to address online competition policy and enforcement, as well as collaborative research. The TTC and competition dialogue present opportunities for the United States and the EU, as entities with shared democratic values, to more closely align their technology agendas and work together to confront concerns such as those raised by China's model of what many experts call digital authoritarianism. Although the U.S.-EU Privacy Shield negotiations remain on a separate track, these new forums present opportunities for broader U.S.-EU discussions on cross-border data flows and data protection. The first meeting of the TTC is scheduled for the end of September 2021.

Another option would be for the United States and the EU to launch negotiations of a broader digital trade agreement, covering cross-border data flows and other issues, such as barring customs duties on electronic transmissions, ensuring online consumer protection, prohibiting forced technology transfer, promoting open government data, and cybersecurity cooperation. As a possible template, negotiators could look to the U.S.-Japan Digital Trade Agreement, concluded in October 2019. The USTR has called it the "most comprehensive and high-standard trade agreement" negotiated on digital trade barriers and said it could set precedents for other talks.[80]

Unlike the United States, however, the EU does not include obligations to ensure cross-border data flows or prohibit localization in its trade agreements. Rather, the EU seeks to maintain regulatory flexibility on data flows and localization requirements. The EU has long maintained that data protection is a fundamental right and not negotiable in trade agreements. In its free trade agreement with Japan, for example, the EU included a carve-out for measures to ensure compliance with laws or regulations for "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."[81] The provision on free flow of data in the agreement states "the Parties shall reassess within three years of the date of entry into force of this Agreement the need

[79] Bruno Gencarelli, Head of Unit International Data Flows and Protection, European Commission DG Justice, speaking at Information Technology Industry Council event, "*Schrems II*: One Year Later," July 14, 2021, https://www.itic.org/news-events/events/schrems-ii-one-year-later.

[80] For more information see, CRS In Focus IF11120, *U.S.-Japan Trade Agreement Negotiations*, by Cathleen D. Cimino-Isaacs and Brock R. Williams.

[81] European Union, *Agreement Between the European Union and Japan for an Economic Partnership*, Chapter 8, Trade in Services, Investment Liberalization, and Electronic Commerce, Article 8.3, entered into force February 1, 2019, https://ec.europa.eu/trade/policy/in-focus/eu-japan-economic-partnership-agreement/.

for inclusion of provisions on the free flow of data."[82] Alongside the trade negotiations, the EU granted Japan an adequacy decision to allow for the free flow of data between the parties.[83]

The EU's reluctance to include data flows in a trade agreement and its preference for using adequacy decisions could pose a challenge for any U.S.-EU negotiations to address the topic. Data flows were among the stumbling blocks when the United States and EU attempted to conclude a comprehensive trade agreement under the Obama Administration.[84]

Potential Multilateral Agreement

Global rules on data protection and cross-border data flows present an opportunity to bridge the U.S.-EU divide and find consensus. At the moment, there are no comprehensive binding multilateral rules specifically addressing cross-border data flows and privacy, and there is no globally accepted standard or definition of online data privacy. Several international organizations, including the Organisation for Economic Co-operation and Development (OECD), G-20, and Asia-Pacific Economic Cooperation (APEC) forum, have sought to develop best practice guidelines or principles related to privacy and cross-border data flows, although none are legally binding. Recent U.S. and other trade agreements, including the U.S.-Mexico-Canada Agreement (USMCA) and U.S-Japan Digital Trade Agreement, are establishing new and, in some cases, enforceable trade rules and disciplines among subsets of trading partners.[85] The United States could also consider negotiating a digital trade or data flows agreement with the United Kingdom, now that it is no longer a member of the EU (see **text box "U.S.-UK Cross-Border Data Flows"**).

Ongoing negotiations between over 80 parties on the sidelines of the World Trade Organization (WTO) that include the United States and EU aim to establish a global framework and obligations to enable digital trade in a nondiscriminatory and less trade restrictive manner. Many stakeholders express hope that the negotiations will result in obligations, standards, and best practices regarding personal data protection and cross-border data flows. The initial U.S. and EU proposals, however, illustrate their differing approaches to data protection, including a large EU carve-out for personal data and privacy.[86] Although the co-convenors have announced agreement on many provisions and areas of digital trade, negotiations on cross-border data flows are ongoing.[87] If the *Schrems II* decision leads the EU to review and potentially invalidate any or all of its existing adequacy decisions with other countries, the EU could be open to supporting a multilateral solution.[88]

---

[82] Ibid, Article 8.81.

[83] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan under the Act on the Protection of Personal Information, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC.

[84] For more information, CRS In Focus IF10120, *Transatlantic Trade and Investment Partnership (T-TIP)*, by Shayerah I. Akhtar and Vivian C. Jones.

[85] For more information on U.S.-Mexico-Canada and U.S-Japan Digital Trade Agreements, see CRS Report R44981, *The United States-Mexico-Canada Agreement (USMCA)*, by M. Angeles Villarreal and Ian F. Fergusson and CRS Report R46140, *"Stage One" U.S.-Japan Trade Agreements*, coordinated by Brock R. Williams.

[86] For more information, see CRS Report R45584, *Data Flows, Online Privacy, and Trade Policy*, by Rachel F. Fefer.

[87] WTO, "E-commerce Negotiations Advance, Delve Deeper Into Data Issues," Joint Statement on E-commerce, May 20, 2021.

[88] Joshua Meltzer, "The Court of Justice of the European Union in *Schrems II*: The Impact of GDPR on Data Flows and National Security," Brookings Institution, August 5, 2020.

U.S.-UK Cross-Border Data Flows

The United Kingdom (UK) withdrew as a member of the EU on January 31, 2020 (commonly termed *Brexit*) and ceased applying EU laws and regulations on December 31, 2020. Post-Brexit, the UK essentially incorporated the EU's GDPR into UK law, but the UK is no longer a participant in Privacy Shield.

In June 2021, the EU adopted two adequacy decisions to allow cross-border data flows between the UK and EU (for both commercial and law enforcement purposes). The decisions are valid for four years and then will need to be renewed or renegotiated, creating a level of uncertainty for U.S. firms that rely on such data flows to communicate with UK and EU customers, partners, and subsidiaries. The United States may consider whether to negotiate a separate UK-specific Privacy Shield agreement, and to what extent it might align with any enhanced EU-U.S. Privacy Shield that is negotiated with the EU. In August 2021, the UK government announced that it would prioritize reaching a new "data adequacy partnership" with the United States (and also five other non-EU countries). In a press release, the government asserted that it intended to "make it easier for UK organizations to exchange data with important markets and fast-growing economies." The UK believes that concluding data flow deals with the United States and other countries with "high data protection standards" will reduce compliance costs for UK firms and minimize trade barriers while supporting growth and innovation.

Going forward, the UK may consider trade-offs between maintaining rules that align with the EU to preserve EU equivalence or market access for UK firms, versus diverging to create a distinct UK regulatory environment. The UK government plans to launch a consultation on reforming its data protection laws in an effort to make its data regime "even more ambitious, pro-growth and innovation-friendly, while still being underpinned by secure and trustworthy privacy standards." EU officials reportedly intend to monitor developments in the UK closely. Some experts warn that diverging from EU data protection standards poses significant risks to UK digital trade with the EU and could hurt UK businesses and citizens.

The UK also could seek to create its own codes of conduct or certification schemes for cross-border data flows, or join already existing international arrangements or agreements. For example, the UK has begun formal negotiations to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), a free trade agreement that contains obligations on open cross-border data flows. The CPTPP digital trade provisions are based on those that the United States negotiated in the original TPP, from which the U.S. later withdrew; the USMCA digital trade chapter and U.S.-Japan Digital Trade Agreement build on the CPTPP provisions. UK membership in CPTPP could potentially make it easier to reach a data flow agreement with the United States, but it could also jeopardize the EU's adequacy decision for the UK.

Sources: UK Department for Digital, Culture, Media & Sport, "EU Adopts 'Adequacy' Decisions Allowing Data to Continue Flowing Freely to the UK," press release, June 28, 2021, and European Commission, *Adequacy Decisions*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Also see, UK Department for Digital, Culture, Media & Sport, "UK Unveils Post-Brexit Global Data Plans to Boost Growth, Increase Trade and Improve Healthcare," press release, August 26, 2021; Vincent Manancourt, "UK to Seek U.S. Data Deal, Reforms to Privacy Laws," *Politico Pro*, August 26, 2021; Madhumita Murgia and Javier Espinoza, "EU Takes Aim at UK Plan to Rewrite Data Law," *Financial Times*, August 26, 2021; and UK Department for International Trade, *UK Approach to Joining the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)*, June 22, 2021.

U.S. Interests and Options for Congress

Many Members of Congress have supported the Privacy Shield framework as being vital to U.S.-EU trade and investment ties. In August 2020, for example, bipartisan leaders of House and Senate committees of jurisdiction voiced concern to the Trump Administration about the impact of the CJEU's invalidation of Privacy Shield and potential business disruptions for SMEs.[89] In October 2020, a group of Members expressed support for U.S. efforts to conclude a successor arrangement in a letter to the Commerce Department and FTC. In this letter, they sought to "emphasize the importance of ensuring stable and reliable mechanisms to transfer data" between the United States and the EU, and asserted that, "Without a successor to the Privacy Shield, disruption of transatlantic data transfers will have significant adverse effects on US consumers, businesses, and economic growth."[90]

Some Members may be concerned by the impact of the CJEU decision on U.S. trade and U.S.-EU relations, more broadly. Congress has also expressed interest in the U.S. role in international standard-setting for digital trade and technologies. In December 2020, a Senate Committee on Commerce, Science, and Transportation hearing focused on these and other issues related to the implications of the CJEU's Schrems II ruling on transatlantic data flows.[91] Some Members are reportedly concerned by the delays in reaching a successor to Privacy Shield and have urged the Biden Administration to reach an enhanced agreement with the EU quickly.[92]

Possible options for Congress to facilitate U.S.-EU data flows and a potential enhanced Privacy Shield accord include:

- Exploring changes when authorizing and overseeing surveillance programs to better protect data privacy or otherwise address EU concerns;
- Strengthening the Privacy and Civil Liberties Oversight Board (PCLOB) by urging the Administration to fill the open positions and considering whether to amend the Board's responsibilities to specifically include oversight of intelligence community activities with regards to Privacy Shield to ensure protection of individual rights;
- Considering comprehensive national privacy legislation to protect U.S. personal data with data protection provisions that may align to some extent with GDPR requirements and provide some level of certainty to EU businesses and individuals while recognizing the limits that privacy legislation would have to address national security surveillance concerns;

[89] Letter from Frank Pallone, Chairman Committee on Energy and Commerce, Greg Walden, Ranking Member Committee on Energy and Commerce, and Roger F. Wicker, Chairman Committee on Commerce, Science, and Transportation, to Maria Cantwell, Ranking Member Committee on Commerce, Science, and Transportation, to Department of Commerce Secretary Ross and FTC Chairman Simons, August 5, 2020, https://republicans-energycommerce.house.gov/news/press-release/committee-leaders-urge-commerce-department-ftc-to-work-with-european-regulators-following-privacy-shield-decision/.

[90] Letter from Peter Welch, et al., October 2, 2020, https://www.bsa.org/files/policy-filings/10022020congresslettersupportprivacyshield.pdf.

[91] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows*, 116th Cong., December 9, 2020.

[92] Alexandra S. Levine, "Languishing EU-US Data Pact Becomes a China Issue for Biden," *Politico Pro*, July 16, 2021.

- Considering if a federal privacy law, combined with specific steps to address U.S. surveillance concerns, would provide sufficient safeguards and guarantees so that the EU could grant a full U.S. "adequacy" decision, eliminating the need to rely on special arrangements like Privacy Shield; or
- Providing greater authority to FTC to bring privacy enforcement actions and enforce Privacy Shield by removing limitations on the FTC's jurisdiction with respect to common carriers and nonprofits.

Although many experts consider legislative changes to U.S. surveillance programs and/or introducing a federal privacy law as options that may go farthest in meeting EU concerns about Privacy Shield, these both could be contentious and complex pieces of U.S. legislation.[93] Views differ across the political spectrum on these issues and would likely take considerable time to reach agreement and enact. As noted previously, debate is ongoing in Congress on possible comprehensive data privacy legislation and a number of bills seek to address data protection and security issues.[94] Changes to intelligence practices also could raise complex constitutional issues, such as separation of powers and Article III standing concerns.[95] The Biden Administration has expressed its intention to assuage EU concerns about U.S. government access to personal data and the availability of judicial redress through executive orders and administrative action, which could enable a successor accord to be reached more quickly.

Apart from legislation, Congress may also conduct oversight related to Privacy Shield and cross-border data flows, for example, by holding hearings on ongoing U.S.-EU negotiations on an enhanced Privacy Shield and implementation of any final arrangement. Congress may examine the implications and possible impact on U.S. companies if negotiators fail to reach an updated agreement on commercial data flows or if the EU, or member states, impose data localization requirements. Congress may consider how the new U.S.-EU Trade and Technology Council can prioritize creating common approaches to these issues. Congress may be interested in evaluating how best to achieve broader consensus on data flows and privacy at the global level, or on a sectoral or market basis, and in assessing U.S. engagement in ongoing bilateral and multilateral digital trade negotiations, including in the OECD and WTO. In addition, some Members of Congress may seek to explore how an enhanced Privacy Shield could contribute to creating transatlantic rules and standards that promote U.S. and European norms and values and provide an effective alternative to counter China's growing influence in the digital space.

[93] See, for example, Steven Overly and Mark Scott, "Step One in Repairing U.S.-EU Relations: A Data Privacy Deal," *Politico*, December 4, 2020; Kenneth Propp, "Progress on Transatlantic Data Transfers? The Picture after the US-EU Summit," *Lawfare*, June 25, 2021; Alexandra S. Levine, "A U.S. Privacy Law Seemed Possible this Congress. Now Prospects Are Fading Fast," *Politico*, June 1, 2021; European Parliament Directorate-General for Internal Policies, *Exchanges of Personal Data after the Schrems II Judgment*, July 2021.

[94] See, for example, from the 117th Congress, S. 224, H.R. 1816, H.R. 4801, S. 2499. For more information, see CRS Legal Sidebar LSB10441, *Watching the Watchers: A Comparison of Privacy Bills in the 116th Congress*, by Jonathan M. Gaffney.

[95] See CRS Report R46724, *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield*, by Chris D. Linebaugh and Edward C. Liu, p. 13. Also see, CRS Report R44334, *Separation of Powers: An Overview*, by Matthew E. Glassman.

Author Information

Kristin Archick
Specialist in European Affairs

Rachel F. Fefer
Analyst in International Trade and Finance

Disclaimer