Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated June 28, 2021

# U.S.-EU Privacy Shield

## Data Transfers and Surveillance Issues

For decades, data privacy and protection issues have been sticking points in U.S.-European Union (EU) relations. The EU considers the privacy of communications and the protection of personal data to be fundamental rights, codified in EU law, while U.S. policy protects certain data on a sectoral basis. To address EU concerns that the United States does not sufficiently protect personal data, the United States and the EU have concluded data transfer agreements in both the commercial and law enforcement sectors. However, unauthorized disclosures in the media in 2013 of U.S. surveillance programs and the alleged involvement of some U.S. telecommunications and internet companies heightened EU concerns about U.S. government access to EU citizens' personal data. Resulting tensions have impacted confidence in U.S.-EU data transfer accords, threatening bilateral trade for U.S. and EU businesses, and elevated congressional concerns that the EU approach to data protection creates unfair trade barriers and limits U.S. firms' access to the EU market.

### EU Court Invalidates Privacy Shield

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, most recently the Privacy Shield Framework in July 2020. In force since 2016, Privacy Shield provided a mechanism to transfer EU citizens' personal data to the United States while complying with EU data protection rules. Privacy Shield sought to address concerns raised in a 2015 CJEU decision that struck down a similar U.S.-EU data transfer accord, the Safe Harbor Agreement of 2000. Privacy Shield also was crafted in anticipation of the EU's General Data Protection Regulation (GDPR), which came into effect in May 2018, and created new individual rights and requirements for data protection throughout the EU. However, the CJEU found that Privacy Shield 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 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.

### U.S. and Congressional Interests

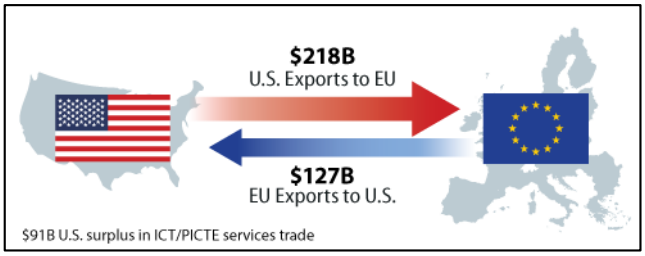
The CJEU Privacy Shield ruling raises several issues for the United States, including how to ensure continued data flows for U.S. companies and organizations that depend on Privacy Shield. Data flows underlie much of the $6.2 trillion U.S.-European economic relationship. The CJEU ruling creates legal 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 large multinational companies.

Congress has a role in U.S. surveillance legislation and oversight, and some Members are debating the need for a U.S. federal data privacy policy. In addition, ongoing international trade negotiations may address digital trade and data flows. Congressional action in these areas could help shape the future landscape for U.S.-EU data transfers.

## Transatlantic Data Flows

According to the U.S. Bureau of Economic Analysis, the United States and Europe are each other's most important commercial partners for digitally enabled services. U.S.-EU trade of information and communications technology (ICT) services and potentially ICT-enabled services was over $345 billion in 2018 (see **Figure 1**). Transatlantic data flows account for more than half of Europe's data flows and about half of U.S. data flows globally. Such data flows enable people to transmit information for online communication, track global supply chains, share research, provide cross-border services, and support technological innovation, among other activities. Organizations may use customer or employee personal data to facilitate business transactions, analyze marketing information, discover fraudulent payments, improve proprietary algorithms, or develop competitive innovations.

**Figure 1. U.S.-EU Trade of ICT and Potentially ICT-Enabled (PICTE) Services, 2018**




**Source:** CRS with data from the Bureau of Economic Analysis.
**Note:** Includes United Kingdom (UK).

As of July 2020, Privacy Shield had 5,380 participants, including U.S. businesses and other organizations, U.S. subsidiaries in Europe, and 250 entities headquartered in Europe. The CJEU judgment could raise operating costs, especially for SMEs, given the limited alternatives for data transfers (see below). The number of Privacy Shield participants began to fall after the CJEU ruling.

Following the CJEU ruling, the European Data Protection Board (EDPB) issued guidance providing examples of supplementary measures that data exporters using SCCs might take, and the EU updated the SCCs to ensure that personal data transferred receives a level of protection equivalent to that under EU law. Given the CJEU finding that U.S. surveillance authorities render U.S. data protections inadequate, experts suggest that SCCs may not be usable in practice for social media and ICT companies subject to U.S. electronic surveillance laws. Industry groups

and the U.S. Department of Commerce (Commerce) also released recommendations and information for entities implementing Privacy Shield and SCCs. In addition, specific derogations identified under EU law 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) and are not affected by the CJEU ruling.

## Privacy Shield Framework

The Privacy Shield Framework requires adherence to seven distinct privacy principles: notice, choice, accountability for onward data transfer, security, data integrity and purpose limitation, access, and recourse, enforcement, and liability. The Framework also sets out 16 mandatory supplemental principles that include provisions on sensitive data, secondary liability, the role of data protection authorities (DPAs), human resources data, pharmaceutical and medical products, and publicly available data. To address EU concerns about U.S. surveillance practices, the Privacy Shield agreement contains written assurances from U.S. officials, including in the intelligence community, asserting that U.S. access to EU citizens' personal data will be subject to clear limitations, safeguards, and oversight mechanisms. Nevertheless, the CJEU found these guarantees insufficient.

### Joining Privacy Shield and Program Enforcement

To voluntarily join the Privacy Shield program, a U.S.-based organization must self-certify annually to Commerce, publicly committing to comply with the Framework's principles and requirements that are enforceable under U.S. law. The program is administered by Commerce and the European Commission (the EU's executive). Commerce monitors firms' effective compliance and investigates complaints. Despite the CJEU decision, Commerce stated it will continue to administer the Privacy Shield Framework and that the ruling "does not relieve participating organizations of their Privacy Shield obligations."

The U.S. Federal Trade Commission (FTC) and the U.S. Department of Transportation enforce compliance. In June 2020, FTC reported enforcement actions against dozens of companies that made false or deceptive representations about Privacy Shield participation. The FTC's $5 billion penalty against Facebook included holding executives accountable for privacy-related decisions and prohibiting misrepresentations related to Privacy Shield. A separate Privacy Shield Ombudsperson at the U.S. Department of State handles complaints regarding U.S. national security access to personal data. The CJEU's ruling, however, questioned the ombudsperson's independence and ability to provide "effective judicial protection" for EU citizens.

### Future Prospects

The Trump Administration began negotiations with the EU on next steps to update or replace Privacy Shield. The Biden Administration has stated it intends to conclude an enhanced successor accord, both to help bolster U.S.-EU relations and address U.S. business demands for durable, protected transatlantic data flows. U.S. negotiators are reportedly seeking to provide greater assurances to the EU through executive orders and administrative action that would protect EU citizens' personal data and clarify how Europeans can pursue redress in U.S. courts for any alleged misuse of their data. Some in the EU question whether such measures would satisfy the EDPB or, ultimately, the CJEU, and contend that legally-binding mechanisms may be necessary to address EU concerns. In the June 2021 U.S.-EU summit statement, President Biden and EU leaders committed to "work together to strengthen legal certainty in transatlantic flows of personal data." U.S.-EU negotiations on an enhanced Privacy Shield are continuing.

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, an idea advocated by some European DPAs and other stakeholders;
- Obtain consent from individuals for every single transfer of personal data, a likely logistically challenging and costly option for many entities;
- Exit or limit participation in the EU market.

Other alternatives would be for the EU to establish codes of conduct or certifications that meet GDPR requirements which organizations could apply. These programs could be U.S.-EU specific or at a broader, global level.

## Options for Congress

Many Members of Congress have supported the Privacy Shield framework as vital to U.S.-EU trade and investment ties. Some policymakers may be concerned by the impact of the CJEU decision on SMEs, in particular, and on U.S. trade more broadly. Possible options for Congress include

- Exploring changes when authorizing and overseeing surveillance programs to better protect data privacy or otherwise address EU concerns;
- Considering comprehensive national privacy legislation that includes data protection provisions that may align to some extent with GDPR requirements, to provide some level of certainty to EU businesses and individuals;
- Examining how best to achieve broader consensus on data flows and privacy at the global level and hold hearings on U.S. engagement in ongoing bilateral and multilateral digital trade negotiations.

Also see CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick; 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, and CRS Report R45584, *Data Flows, Online Privacy, and Trade Policy*, by Rachel F. Fefer.

**Rachel F. Fefer**, Analyst in International Trade and Finance
**Kristin Archick**, Specialist in European Affairs

IF11613

## Disclaimer