Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

August 6, 2020

U.S.-EU Privacy Shield

Data Transfers and Surveillance Issues

For decades, data privacy and protection issues have been sticking points in U.S. relations with the European Union (EU), in part because of different data privacy approaches and legal regimes. To bridge differences and enable data transfers, the United States and the EU have concluded data-sharing accords in both the commercial and law enforcement sectors. However, unauthorized disclosures 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, with ramifications for U.S.-EU data transfer arrangements. Resulting trade tensions have impacted U.S. and EU businesses, elevating 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 on July 16, 2020. In force since 2016, Privacy Shield provided over 5,000 companies 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. 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's concerns about U.S. surveillance laws also may pose challenges for some firms using another EU mechanism—standard contractual clauses (SCCs)—to transfer personal data to the United States.

U.S. and Congressional Interests

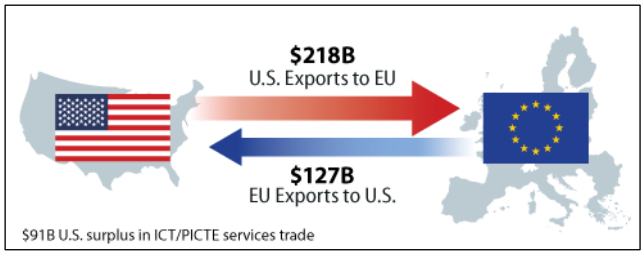
The CJEU Privacy Shield ruling raises several issues for the United States and Congress, including how to ensure continued data flows for U.S. companies and organizations that depend on Privacy Shield. Transatlantic data flows are of critical importance for the $5.5 trillion U.S.-European economic relationship. The CJEU ruling creates legal uncertainty for many firms engaged in transatlantic trade, both those that relied on Privacy Shield (over 65% of which are small and mid-sized firms, SMEs) and those using SCCs, including many large multinational companies.

Congress also has a role in U.S. surveillance legislation and oversight, and some Members are debating the need for a U.S. federal data privacy and protection policy. In addition, ongoing U.S.-EU and other 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 recent studies, 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, detect disease patterns from medical histories, 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). Although SCCs remain valid, the CJEU ruling increases due diligence requirements for data exporters using 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. Separate from Privacy Shield and SCCs, 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. In contrast to the former Safe Harbor accord, the Privacy Shield agreement contains written assurances from U.S. officials, including in the intelligence community, that U.S. access to EU citizens' personal data will be subject to clear limitations, safeguards, and oversight mechanisms. Privacy Shield 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.

Joining Privacy Shield and Program Enforcement

To voluntarily join the Privacy Shield program, a U.S.-based organization must self-certify annually to the U.S. Department of Commerce (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.

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.

Future Prospects

Following the invalidation of the Safe Harbor accord in 2015, U.S. and EU officials agreed to an enforcement moratorium while they negotiated Privacy Shield. No similar moratorium has been announced to protect Privacy Shield participants, although U.S. and EU officials have begun discussions on next steps to update or replace Privacy Shield in light of the CJEU decision. U.S. and EU industry groups have jointly called for a swift negotiation to ensure durable, protected transatlantic data flows. 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 EU-approved SCCs updated to align with the GDPR and reassessed for adequate safeguards in accordance with the CJEU ruling;
- Use commercial cloud services provided by large technology firms that use approved BCRs or SCCs (e.g., Microsoft, IBM);
- Store EU citizens' personal data only in the EU, 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 for firms include establishing codes of conduct or certifications that meet GDPR requirements for which individual organizations could apply. These programs could be U.S.-EU specific or at a broader, international level.

Options for Congress

Many Members of Congress have supported the Privacy Shield framework as vital to U.S.-EU trade and investment ties. Congress 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:

- Holding hearings with the U.S. agencies charged with administering and enforcing Privacy Shield to identify issues and provide direction for negotiating any new agreement or other alternative data transfer mechanisms.
- 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, potentially eliminating the need for a U.S.-EU-specific data flow agreement in the longer-term.
- Evaluating the trade-related aspects of data flows in trade agreements, including through oversight of ongoing U.S. trade negotiations with the EU and, separately, with the United Kingdom (UK) as the UK seeks to align its data protection laws with the GDPR.
- Examining how best to achieve broader consensus on data flows and privacy at the global level and U.S. engagement in ongoing international data initiatives.

Also see, CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick; 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

Disclaimer