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

(name redacted)
Specialist in International Trade and Finance

(name redacted)
Specialist in European Affairs

February 12, 2016

Congressional Research Service
7-....
www.crs.gov
R44257

CRS REPORT
Prepared for Members and
Committees of Congress

Contents

Contacts

Summary

Both the United States and the European Union (EU) maintain that they are committed to upholding individual privacy rights and ensuring the protection of personal data. Nevertheless, data privacy and protection issues have long been sticking points in U.S.-EU economic and security relations, in part because of differences in U.S. and EU data privacy approaches and legal regimes. In the late 1990s, the United States and the EU negotiated the Safe Harbor Agreement of 2000 to allow U.S. companies and organizations to meet EU data protection requirements and permit the legal transfer of personal data between EU member countries and the United States.

The unauthorized disclosures in June 2013 of U.S. National Security Agency (NSA) surveillance programs and subsequent allegations of other U.S. intelligence activities in Europe renewed and exacerbated European concerns about U.S. data privacy and protection standards. The alleged involvement of some U.S. Internet and telecommunications companies in the NSA programs also elevated European worries about how U.S. technology firms use personal data and the extent of U.S. government access to such data. As a result, a number of U.S.-EU data-sharing accords in both the commercial and law enforcement sectors have come under intense scrutiny in Europe.

In October 2015, the Court of Justice of the European Union (CJEU, which is also known as the European Court of Justice, or ECJ) invalidated the Safe Harbor Agreement. The CJEU essentially found that Safe Harbor failed to meet EU data protection standards, in large part because of the U.S. surveillance programs. Given that some 4,500 U.S. companies were using Safe Harbor to legitimize transatlantic data transfers, U.S. officials and business leaders were deeply dismayed by the CJEU's ruling. Companies that had been using Safe Harbor as the legal basis for U.S.-EU data transfers were required to immediately implement alternative measures. Experts claimed that the CJEU decision created legal uncertainty for many U.S. companies and feared that it could negatively impact U.S.-EU trade and investment ties.

On February 2, 2016, U.S. and EU officials announced an agreement, "in principle," on a revised Safe Harbor accord, to be known as Privacy Shield. Although the text of the new agreement is still being finalized and has not yet been released, U.S. and EU officials assert that it will address the CJEU's concerns. In particular, they stress that it will contain significantly stronger privacy protections as well as safeguards related to U.S. government access to personal data.

Some analysts question, however, whether Privacy Shield will sufficiently address the broader issues about the U.S. data protection framework raised by the CJEU decision, and thus be able to withstand future legal challenges. Many U.S. policymakers and trade groups hope that the recently concluded U.S.-EU "umbrella" Data Privacy and Protection Agreement (DPPA)—which seeks to better protect personal information exchanged in a law enforcement context—and the proposed U.S. Judicial Redress Act (H.R. 1428 and S. 1600)—which would extend the core of the judicial redress provisions in the U.S. Privacy Act of 1974 to EU citizens—could help ease at least some concerns about U.S. data protection standards and boost confidence in Privacy Shield. H.R. 1428 passed the House on October 20, 2015, and was passed by the Senate on February 9, 2016. Since the bill was amended by the Senate Judiciary Committee, essentially making special reference to the need for continued sharing of U.S.-EU commercial data, it went back to the House which approved the amended bill on February 10. H.R. 1428 now goes to the President.

This report provides background on U.S. and EU data protection policies and the Safe Harbor Agreement, discusses the CJEU ruling, and reviews the key elements of the newly-proposed Privacy Shield. It also explores various issues for Congress, including implications for U.S. firms of Safe Harbor's invalidation and the role of the proposed Judicial Redress Act in helping to ameliorate U.S.-EU tensions on data privacy and protection issues.

Introduction

On October 6, 2015, the Court of Justice of the European Union (CJEU) delivered a judgment[1] that invalidated the Safe Harbor Agreement between the United States and the 28-member European Union (EU).[2] Safe Harbor was a 15-year-old accord, under which personal data could legally be transferred between EU member countries and the United States for commercial purposes. The negotiation of Safe Harbor was largely driven by the EU's 1995 Data Protection Directive (DPD) and European concerns that the U.S. approach to data privacy did not guarantee a sufficient level of protection for European citizens' personal data. The Safe Harbor Agreement applied to a wide range of businesses and organizations that collect and hold personal data. When the parties concluded the Safe Harbor Agreement in 2000, however, the Internet was still in its infancy, and the range of public and private actors engaged in the mass processing of personal data, including across borders, was much more limited than today.

The CJEU's decision gave added impetus to U.S.-EU negotiations underway since late 2013 aimed at "making Safe Harbor safer." These discussions were part of several initiatives seeking to restore transatlantic trust in the security of U.S.-EU data flows following the so-called "Snowden leaks." On February 2, 2016, U.S. and EU officials announced an agreement, "in principle," on a replacement to Safe Harbor—the U.S.-EU Privacy Shield, which if approved by the European Commission, would allow companies to continue to transfer EU citizen's personal data to the United States while complying with the requirements outlined by the CJEU when it declared Safe Harbor invalid in October 2015. The text of the new agreement is being finalized and has not yet been released.

U.S. and EU officials claim that Privacy Shield will contain significantly stronger privacy protections and oversight mechanisms, multiple redress possibilities, and new safeguards related to U.S. government access to personal data. Nevertheless, questions exist about whether Privacy Shield will go far enough in addressing broader EU data privacy and protection concerns, and whether it will be able to stand up to future legal challenges against it that will likely be brought before the CJEU. Many U.S. officials and business leaders hope that the recently concluded (but not yet finalized) U.S.-EU Data Privacy and Protection Agreement (DPPA)—an "umbrella" accord aimed at better protecting personal information exchanged in a law enforcement context—and the proposed U.S. Judicial Redress Act (H.R. 1428 and S. 1600)—which would extend the core of the judicial redress provisions in the U.S. Privacy Act of 1974 to EU citizens—could help ameliorate European concerns about U.S. data protection standards and bolster confidence in the newly proposed Privacy Shield Agreement.

Data Privacy and Protection in the EU and the United States

Both the United States and EU assert that they are committed to upholding individual privacy rights and ensuring the protection of personal data, including electronic data. Nevertheless, data privacy and data protection issues have long been sticking points in U.S.-EU economic and

[1] Case C-362/14, Maximillian Schrems v. Digital Rights Ireland Ltd. (2015).

[2] The EU 28 member states 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; Sweden; and the United Kingdom.

security relations, in large part due to fundamental differences between the United States and EU in their approaches to data protection and data privacy laws. For instance, in the United States, what the European Commission (the EU's executive) refers to as the "collecting and processing of personal data" is allowed unless it causes harm or is expressly limited by U.S. law.[3] In Europe, by contrast, processing of personal data is prohibited unless there is an explicit legal basis that allows it.[4]

The EU Approach and the 1995 Data Protection Directive (DPD)

The EU considers the privacy of communications and the protection of personal data to be fundamental human rights, as incorporated into Articles 7 and 8 of the 2000 Charter of Fundamental Rights of the European Union[5] and made binding on all EU members through the 2007 Treaty of Lisbon (which took effect in 2009).[6] Europe's past history with fascist and totalitarian regimes clearly informs its views on data protection and contributes to the demands from European politicians and publics for strict data privacy controls.

In October 1995, the EU agreed on a Data Protection Directive (DPD) to harmonize differing national legislation on data privacy protection and establish a comprehensive EU-wide framework.[7] The DPD sets out common rules for public and private entities in all EU member states that hold or transmit personal data. The DPD governs how information about European citizens may be collected and used across all industries, with each EU member state responsible for implementing the Directive through its own national laws. The EU hoped that the DPD would facilitate information flows within the EU, strengthen the EU's internal market, and foster the development of an information-based economy. EU member states were given three years to implement the DPD.

The DPD provides that the transfer of personal data to a country outside of the EU may occur only if the European Commission determines that the country provides an adequate level of protection of personal data. The adequacy of the level of protection is assessed in the 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 countries of origin, and final destination of the data, and that country's laws, rules, and security measures.[8]

The DPD applies to all organizations, public and private, operating in the EU, including affiliates of U.S. corporations. It covers the processing of all personal data, whether done automatically or manually. There is no exception for public records, such as telephone directory listings. Only information compiled for private, personal household use is excluded. Under the DPD, data may

[3] European Commission, *Collecting & processing personal data: what is legal?*, http://ec.europa.eu/justice/data-protection/data-collection/legal/index_en.htm.

[4] Ioanna Tourkochoriti, "The Snowden Revelations, "The Transatlantic Trade and Investment Partnership and the Divide between U.S.-EU Data Privacy Protection," *University of Arkansas at Little Rock Law Review*, vol. 36 (2014). See also, Paul M. Schwartz and Daniel J. Solove, "Reconciling Personal Information in the United States and the European Union," *California Law Review*, vol. 102, no. 4 (2014).

[5] Charter of Fundamental Rights of the European Union, art. 7, 2000 O.J. (C 364) 18.

[6] Treaty of Lisbon Amending the Treaty of the European Union and the Treaty Establishing the European Communities, December 13, 2007, O.J. (C306).

[7] 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).

[8] Data Protection Directive, at Art. 25 and 26.

be collected and used only for specified, explicit, and legitimate purposes. Security and accuracy must be guaranteed. Individuals not only have the right to access their personal information and the right to correct errors, but also the right to seek remedial measures and compensation, if necessary. The transfer of data to third parties may occur only under similarly strict requirements. More stringent rules apply to the processing of sensitive data, including data relating to race; ethnic origin; political, religious, or philosophical beliefs; and health status or sex life. The DPD requires the creation of "Data Protection Agencies" (DPAs) in each EU member state, registration of databases with these authorities, and, sometimes, prior DPA approval before organizations or firms may begin data processing.

Although the 1995 Data Protection Directive has since been complemented by other EU legal instruments (such as the 2002 "e-Privacy" Directive for the communications sector), the DPD currently remains the EU's main data protection instrument. In 2012, the European Commission proposed a new legislative package aimed at modernizing the DPD and introducing other data protection reforms in order to take into account the changes in data processing brought about by the widespread use of the Internet. In December 2015, EU member states (acting in the Council of the European Union) and the directly-elected European Parliament (which represents the citizens of the EU) reached political agreement on new data protection rules, which are expected to receive final approval in early 2016.[9]

The U.S. Approach

In the United States, respect for privacy is broadly enshrined in our Constitution. Unlike the EU, however, the United States does not have a single, overarching data privacy and protection framework. Many describe U.S. data privacy laws as a "patchwork" of federal and state statutes.[10] For example, concerns about how the federal government manages personal information in its possession led to the enactment of the *U.S. Privacy Act of 1974,*[11] while the *Electronic Communications Privacy Act of 1986,*[12] extended government restrictions on telephone wire taps to include computer transmissions of electronic data. Meanwhile, federal consumer privacy laws in the United States are largely industry specific and vary by sector, with different laws governing the collection and disclosure of financial data, health-related data, student information, and motor vehicle records.[13] U.S. states have also enacted a variety of digital privacy and data protection laws over the years.

[9] The EU data protection reform package proposed by the Commission in January 2012 included two legislative measures. First, a data protection regulation would update the 1995 DPD and cover the bulk of personal data processing in both the public and private sectors; in contrast to the 1995 DPD, this regulation would be directly applicable in all EU member states, thus establishing a single set of rules (rather than harmonized ones) for data protection throughout the EU. Second, a new directive would set standards for cross-border and domestic data processing for law enforcement purposes (not covered by the 1995 DPD). For more information, see European Parliament, "Q&A on EU Data Protection Reforms," June 24, 2015.

[10] For a brief description of the development of U.S. privacy law, see Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, Washington, DC, May 2014, pp. 15-19, and Rosemary P. Jay (ed), *Data Protection & Privacy*, at 208 (2015).

[11] 5 U.S.C. §552a. The Privacy Act covers personal records maintained by federal agencies. See CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by (name redacted)

[12] 18 U.S.C. §2510 et seq.

[13] For example, see CRS Report R41756, *Privacy Protections for Personal Information Online*, by (name redacted), and CRS Report R42338, *Smart Meter Data: Privacy and Cybersecurity*, by (name redacted), (name redacted), and (name redacted) .

Many U.S. officials and industry representatives maintain that the U.S. approach to data privacy is more nimble than what they view as the EU's "one-size-fits-all" approach. They also contend that the U.S. approach helps to promote and sustain U.S. technological innovation.[14] Nevertheless, some U.S. privacy advocates argue that there are significant gaps in this "patchwork" approach, especially in terms of data collection online, and have long urged Congress to enact comprehensive data protection legislation.

Transatlantic Data Flows

The transatlantic flow of data is a form of international trade and is of critical importance for the U.S. and European economies. The United States and the EU remain each other's largest trade and investment partners. In 2013, total U.S.-EU trade in goods and services amounted to $1 trillion and U.S. FDI in EU totaled $2.4 trillion (or about 56%) of total U.S. direct investment abroad. Conversely, EU companies accounted for $1.7 trillion (or about 62%) of direct investment in the United States.[15] According to a 2014 study, cross-border data flows between the United States and Europe are the highest in the world—almost double the data flows between the United States and Latin America and 50% higher than data flows between the United States and Asia.[16]

Reports indicate that data protection standards are not part of the ongoing negotiations for the Transatlantic Trade and Investment Partnership (T-TIP), because the EU views its data privacy laws and protection standards as fundamental rights that are nonnegotiable. However, both U.S. and European officials recognize that a successful T-TIP agreement requires the ability to transfer data between the United States and EU member countries in a legally sound and cost-effective manner. As noted by U.S. Under Secretary for Economic Growth, Energy, and the Environment Catherine A. Novelli:

> The U.S. and the EU are the two largest net exporters of digital goods and services to the rest of the world. In 2012, the United States' $151 billion trade surplus in digital services was surpassed only by the EU's $168 billion surplus.[17]

Many observers expect the negotiations to address digital trade issues. U.S. business interests have reportedly been advocating for measures in T-TIP that would prevent restrictions on cross-border data flows, and for new mechanisms that would provide alternative ways for U.S. companies to comply with EU data privacy rules beyond those that already exist.[18] This issue could become even more important in T-TIP negotiations in light of the CJEU's judgment on Safe Harbor.

[14] Natasha Singer, "Data Protection Laws, An Ocean Apart," *New York Times*, February 2, 2013.

[15] CRS Report R43387, *Transatlantic Trade and Investment Partnership (T-TIP) Negotiations*, by (name redacted) , (name redacted), and (name redacted) . See also, CRS In Focus IF10120, *Transatlantic Trade and Investment Partnership (T-TIP)*, by (name redacted) and (name redacted) .

[16] Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, Brookings, Washington, DC, October 1, 2015.

[17] Catherine A. Novelli, *Growing the Digital Economy: Remarks before the Lisbon Council*, U.S. Department of State, June 2, 2015.

[18] "Chamber Wants TTIP to Ease Data Flows without Altering EU Regime," *Inside U.S. Trade*, March 7, 2014.

The Safe Harbor Agreement

As discussed above, the European Union and the United States have fundamentally different attitudes towards the protection of personal data. EU and U.S. officials recognized that, following the passage of the DPD in 1995, the substantial differences between the U.S. and EU data protection regimes threatened to disrupt or prevent the transfer of personal data between the EU and the United States. They worried that these differences in approach could negatively affect many businesses and industries on both sides of the Atlantic, and potentially impact the U.S.-EU trade and investment relationship.

Following negotiations between the United States and the EU, the parties agreed on a mechanism that would allow U.S. companies to meet the "adequate level of protection" required by the DPD. In 2000, the U.S. Department of Commerce issued the Safe Harbor Privacy Principles,[19] which were subsequently recognized by the European Commission.[20] However, according to the Commission's Decision, the Safe Harbor principles could be limited to the extent necessary for national security, public interest, or law enforcement requirements.

Under Safe Harbor, a U.S. company could self-certify annually to the Department of Commerce that it had complied with the seven basic principles and related requirements that have been deemed to meet the data privacy adequacy standard of the EU. The seven basic principles, in edited and abridged form, were as follows.

- **Notice.** An organization must inform individuals about the purposes for which it collects and uses information, how to contact the organization with inquiries or complaints, and the types of third parties to which it discloses the information.
- **Choice.** An organization must offer individuals the opportunity to choose (**opt-out**) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual.

  For **sensitive information**, individuals must explicitly **opt-in** when personal data is to be transferred to a third party or used for a purpose other than the one for which it was originally collected or subsequently authorized. Sensitive information includes information about medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information regarding the individual's sex life.
- **Onward Transfer**. In transferring information to a third party, organizations must apply the Notice and Choice Principles. Third parties acting as agents must provide the same level of privacy protection either by subscribing to Safe Harbor, adhering to the Directive or another adequacy finding, or entering into a contract that specifies equivalent privacy protections.
- **Security.** Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

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

[20] 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 Protect Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000.

- **Data Integrity**. Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
- **Access**. Individuals must have access to the information about them that an organization holds and must be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense would be disproportionate to the risks to the individual's privacy or where the rights of others would be violated. Furthermore, the Safe Harbor principles may be limited to the extent necessary for national security, public interest, or law enforcement requirements.
- **Enforcement**. Effective privacy protection must include mechanisms for verifying compliance, provide readily available and affordable independent recourse mechanisms in cases of noncompliance, and include remedial measures for the organization when the Principles are not followed. Sanctions must be rigorous enough to ensure compliance.

Participation in Safe Harbor was open to any U.S. organization subject to regulation by the Federal Trade Commission (FTC), which enforces a variety of consumer protection laws, including those related to unfair and deceptive practices, and to United States air carriers and ticket agents that are subject to regulation by the Department of Transportation (DOT). Some 4,500 companies were on the Safe Harbor list. To qualify, organizations were required to self-certify annually in a letter to the DOC that they adhered to the Safe Harbor principles. The FTC asserted that it was committed to reviewing all referrals of potential violations from EU member state authorities.

Both private sector entities and federal and state authorities that enforce unfair and deceptive practices laws were required to enforce the Safe Harbor Agreement. Private sector enforcement consisted of three components: verification; dispute resolution; and remedies. Persistent failure to comply would result in withdrawal of "Safe Harbor" status, a fact that would be indicated on the "Safe Harbor" website, and also, potentially, by regulatory action. To date, the FTC has charged 40 companies with violations of the Safe Harbor framework. Organizations that did not fall under the jurisdiction of the FTC and the DOT were not eligible for "Safe Harbor." Notably, this included U.S. financial firms and telecommunications carriers. Following the CJEU decision, however, the FTC announced that it would no longer enforce Safe Harbor.[21]

The CJEU Decision

On October 6, 2015, the CJEU (see text box) issued a decision that invalidated Safe Harbor (effective immediately), as currently implemented. The CJEU decision stemmed from a complaint brought to the Irish 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 in light of the unauthorized disclosures in June 2013 of U.S. surveillance activities. The Irish DPA dismissed the complaint, finding that it had no basis to evaluate the complaint since Facebook adhered to the Safe Harbor Agreement and the Irish DPA was thus bound by the 2000 decision by the European Commission recognizing that Safe Harbor provided an "adequate level of protection" as required by the DPD. Upon request by the Irish

[21] Presentation of The Honorable Julie Brill, Commissioner, U.S. Federal Trade Commission, The Amsterdam Privacy Conference, *Transatlantic Privacy after Schrems: Time for an Honest Conversation*, October 23, 2015.

High Court, the CJEU considered whether the Irish DPA could conduct an investigation into Facebook's data protection practices to assess their adequacy or whether the Irish DPA had to defer to the European Commission's earlier approval of the Safe Harbor framework.

The October 6, 2015, decision issued several findings.[22] Foremost, perhaps, the CJEU found that the existence of the Commission Decision on the Safe Harbor Agreement does not eliminate or reduce the powers available to the national DPAs. The CJEU found that national DPAs "must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him" and assess their compliance with the DPD and the EU's Charter of Fundamental Rights. Turning to the Safe Harbor Agreement specifically, the CJEU found Safe Harbor to be invalid. The CJEU found that according to Article 25 of the DPD, the European Commission is required to examine the domestic laws or international commitments of a third country prior to making a determination on the adequacy of their data privacy protection. Since the 2000 Commission Decision recognizing the Safe Harbor Agreement did not make any such finding, that Decision is now invalid. Safe Harbor no longer provides a legal basis for U.S.-EU data transfers, although other methods such as Standard Contractual Clauses or Binding Corporate Rules (see below) can be used.

In addition, the CJEU ruling found that U.S. national security, public interest, and law enforcement requirements have "primacy" over the Safe Harbor principles, and that U.S. undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict 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 2000 Commission's Decision on Safe Harbor does not refer to 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.

The Court of Justice of the European Union (CJEU)

The Court of Justice of the European Union (also commonly referred to as the European Court of Justice, or the ECJ) is the highest court in the EU in matters of EU law. Established in 1952 and based in Luxembourg, the CJEU reviews the legality of the acts of the EU institutions, ensures that EU member states comply with their obligations under the EU treaties, and interprets EU law at the request of national courts and tribunals. In doing so, the CJEU seeks to ensure that EU legislation is interpreted and applied uniformly in all EU countries. The CJEU has the power to settle legal disputes between EU national governments and EU institutions. In some instances, the CJEU can also be used by individuals, companies, and organizations to take action against an EU institution if, in their view, their rights have been violated. The CJEU's rulings are binding on the EU's member states and the EU institutions. The CJEU is divided into three bodies:

- The *Court of Justice* deals with requests for preliminary rulings from national courts, certain actions for annulling EU legal acts, and appeals. It is composed of one judge from each of the EU's 28 member states. The Court of Justice is assisted by nine advocates-general who present reasoned opinions on the cases brought before the court. The advocates-general are expected to be impartial and their opinions are public.
- The *General Court* was created in 1988 to help manage the CJEU's growing caseload. It is responsible for certain types of cases, particularly actions brought by private individuals, companies, and some organizations, and thus mainly deals with competition law, state aid, trade, and agricultural issues.
- The *Civil Service Tribunal* was established in 2004 and rules on disputes between the EU and its staff; it is composed of seven judges.

Approximately 28,000 judgments have been issued in total by the three bodies that compose the CJEU. Each judge

[22] 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.

and advocate-general in the CJEU is appointed by agreement among the EU's 28 member states for a renewable six-year term. In each of the three bodies, the judges select a President who serves a renewable term of three years. Approximately 2,100 civil servants support the work of the CJEU.

Sources: Court of Justice of the European Union, http://curia.europa.eu/jcms/jcms/j_6; European Union, *About the EU*, http://europa.eu/about-eu/institutions-bodies/court-justice/index_en.htm.

U.S. and European Responses

In an October 6, 2015, press release, Secretary of Commerce Penny Pritzker said the Obama Administration was "deeply disappointed" in the CJEU decision and that it "necessitates release of the updated Safe Harbor Framework as soon as possible."[23] Since late 2013, the European Commission and U.S. officials had been working on revising the Safe Harbor Agreement to take into account European concerns about U.S. data privacy and protection standards, especially in the wake of the so-called "Snowden leaks." Following the CJEU ruling, European Commission officials echoed U.S. calls to conclude a new and improved Safe Harbor Agreement and announced three broad priorities for managing U.S.-EU data flows in the meantime: (1) protecting personal data transferred across the Atlantic; (2) ensuring the continuation of transatlantic data flows (using other mechanisms available under the DPD); and (3) working with the national data protection authorities to deliver a coordinated response on alternative ways to transfer data to the United States (deemed by many as crucial to avoid potentially contradictory decisions by national authorities and provide predictability for citizens and businesses alike).[24]

Following the CJEU decision, a working party of EU DPAs (the Article 29 Working Party) reaffirmed that data transfers taking place under Safe Harbor were now unlawful and expressed broad concern about the impact of the CJEU's findings on other data-sharing "transfer tools" such as Standard Contractual Clauses or Binding Corporate Rules. The Article 29 Working Party called on the EU to "open discussions with U.S. authorities in order to find political, legal, and technical solutions" to enable data transfers to the United States "that respect fundamental rights," and noted that a re-negotiated and revised Safe Harbor Agreement "could be a part of the solution." According to their press release:

> If by the end of January 2016, no appropriate solution is found with the US authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions.[25]

Thus, the Article 29 Working Party effectively set a deadline of January 31, 2016 for U.S. and EU negotiators to reach agreement on a revised Safe Harbor Agreement.

The New EU-U.S. Privacy Shield Agreement

U.S.-EU discussions on revising and updating the Safe Harbor Agreement began in late 2013 in response to growing European concerns about the NSA surveillance programs and subsequent allegations of other U.S. intelligence collection operations in Europe. Even preceding the so-

[23] Department of Commerce, "Statement from U.S. Secretary of Commerce Penny Pritzker on European Court of Justice Safe Harbor Framework Decision," press release, October 6, 2015.

[24] European Commission, "First Vice-President Timmermans and Commissioner Jourova's Press Conference on Safe Harbor Following the Court Ruling in Case C-362/14 (Schrems)," press release, October 6, 2015.

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

called "Snowden leaks," some European privacy advocates had long contended that the Safe Harbor Agreement contained significant data protection loopholes. Those of this view asserted, for example, that some companies did not fully implement the Safe Harbor requirements because annual compliance checks were not mandatory, and that hundreds of companies over the years had made false claims about belonging to the accord. Others characterized U.S. enforcement of Safe Harbor as meager, pointing out that the FTC brought action against only ten companies during the first 13 years of the agreement's existence.[26] In addition, critics argued that Safe Harbor, negotiated in the late 1990s when the Internet was in its infancy, was long over-due for re-evaluation.

In light of such existing criticisms and amid allegations that some U.S. companies such as Google and Microsoft (among others that participated in Safe Harbor) may have been involved in U.S. surveillance activities, some European data protection officials and Members of the European Parliament (MEPs) called on the European Commission to suspend Safe Harbor. The European Commission rejected doing so because of concerns that suspending Safe Harbor would adversely affect EU business interests and the transatlantic economy. The European Commission agreed, however, that there were a number of weaknesses in the Safe Harbor scheme. In November 2013, the European Commission issued 13 recommendations to "make Safe Harbor safer," centered on four broad priorities: enhancing transparency; ensuring redress; strengthening enforcement; and limiting the access of U.S. authorities to data transferred under Safe Harbor.[27] Throughout the negotiations (both before and after the CJEU judgment), the Safe Harbor Agreement's national security exemptions and EU demands to ensure only limited access to Safe Harbor data for national security purposes were reportedly key sticking points.

On February 2, 2016, two days after the January 31 deadline established by the Article 29 Working Group, U.S. and EU officials announced their agreement, "in principle," on a replacement to Safe Harbor—the EU-U.S. Privacy Shield, which if approved by the European Commission, would allow companies to continue to transfer EU citizen's personal data to the United States while complying with the requirements outlined by the CJEU when it declared Safe Harbor invalid in October 2015.[28]

The text of the agreement is being finalized and has not yet been released. Like the now-invalidated Safe Harbor Agreement, the Privacy Shield Agreement would, if finalized and approved, take the form of an exchange of letters between U.S. and EU officials. EU officials have stated that they expect that the text of the Privacy Shield will be finalized and released by the end of February.

Following the new agreement, the Article 29 Working Group will issue an opinion, after which the agreement will be considered for formal approval by the European Commission. The Article 29 Working Group has announced that it will assess the new EU-U.S. Privacy Shield data-sharing

[26] Nikolaj Nielsen, "Hundreds of U.S. Companies Make False Data Protection Claims," EUObserver.com, October 8, 2013; "FTC's Response to Alleged Safe Harbor Violations Could Change Enforcement Standards, Lawyers Say," *Warren's Washington Internet Daily*, August 15, 2014.

[27] See European Commission, "European Commission Calls on the U.S. to Restore Trust in EU-U.S. Data Flows," press prelease, November 27, 2013, http://europa.eu/rapid/press-release_IP-13-1166_en.htm; also see Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, November 27, 2013.

[28] Department of Commerce, "EU-U.S. Privacy Shield," press release, February 2, 2016; European Commission, "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield," press release, February 2, 2016.

agreement against four criteria for the processing of data flows for intelligence activities.[29] These are:

1. Data processing should be based on clear, precise and accessible rules;
2. Data protections should be in place to ensure that processing of personal data is necessary and proportionate;
3. An independent and impartial oversight mechanism should exist; and
4. Effective remedies should be available to any individual.

Key Elements

Although the text of the agreement is not yet available, EU and U.S. press materials state that the Privacy Shield would address the concerns raised by the CJEU through:

- **Enhanced commitments and enforcement.** U.S. companies wishing to import personal data from Europe will need to commit to robust obligations on how personal data is processed and European data subject rights are guaranteed. The Department of Commerce will monitor compliance pursuant to FTC enforcement. Stronger sanctions may also be introduced. At the present time, it is uncertain what these "robust obligations" will be, or what precise data subject rights will have to be complied with by U.S. firms.
- **Clear safeguards and transparency obligations.** The United States has reportedly given written assurances that the access of U.S. authorities to EU personal data will be subject to clear limitations, safeguards and oversight mechanisms. U.S. authorities have also, reportedly, ruled out indiscriminate mass surveillance on the personal data transferred to the United States under the new arrangement. There will be an annual joint review, which will also include the issue of national security access, to regularly monitor the functioning of the arrangement. The European Commission and the Department of Commerce will conduct the review and invite national intelligence experts from the United States and European DPAs to participate.
- **Effective protection of EU citizens' rights with several redress possibilities.** Any citizen who considers that their data has been compromised under the new arrangement will have multiple redress possibilities, beginning with deadlines for companies to respond to individual complaints. European DPAs will also be able to refer unresolved complaints to the FTC. Furthermore, claimants would be provided with a free alternative dispute resolution mechanism in the event that the FTC does not pursue an individual's case. For complaints on possible access by national intelligence agencies, a new special ombudsman will be created in the U.S. State Department. This office will be independent of the intelligence agencies, but will have clearance to review issues on the referral of EU DPAs.

Next Steps

The Article 29 Working Group has asked the European Commission to present the formal text of the Privacy Shield Agreement by the end of February 2016. After receiving the text, they will

[29] European Commission Article 29 Working Party, "Statement of the Article 29 Working Party on the Consequences of the Schrems Decision," press release, February 3, 2016.

need to issue guidance in relation to the Privacy Shield Agreement and the acceptability of other transfer mechanisms, such as model contract clauses or binding corporate rules (discussed below). The Article 29 Working Group has indicated that the model contract clauses and binding corporate rules can still be used for personal data transfers while they are assessing the Privacy Shield Agreement.

European Commission officials must draft an adequacy decision, which would approve the U.S.-EU Privacy Shield as a valid data transfer mechanism under the existing European Data Protection Directive. The adequacy decision will need to be adopted by the full European Commission (the so-called College of Commissioners) following consultations with representatives of the EU member states and with the advice of the Article 29 Working Party.

In the United States, officials are expected to make the necessary arrangements to appoint the new Ombudsman at the State Department and put in place the new framework and monitoring mechanisms. The Privacy Shield Agreement, like the original Safe Harbor Agreement, is not a treaty and thus requires no special congressional consideration. Instead, the agreement would be reached by letters of commitment between U.S. and EU officials.

It is expected that the Privacy Shield would operate in a similar way to the Safe Harbor Agreement, with companies registering their commitment to the agreement with the Department of Commerce.

Future Prospects

U.S. and EU officials claim that Privacy Shield will contain significantly stronger privacy protections and oversight mechanisms, multiple redress possibilities, and new safeguards related to U.S. government access to personal data. Secretary of Commerce Pritzker asserted that "this historic agreement is a major achievement for privacy and for businesses...it provides certainty that will help grow the digital economy" and "underscores the strength of the U.S.-EU relationship."[30] Business groups, technology firms, and industry leaders on both sides of the Atlantic have welcomed the substantial progress made by the United States and the EU toward finalizing and concluding the Privacy Shield Agreement.[31]

Nevertheless, concerns exist about whether Privacy Shield goes far enough in addressing EU data privacy and protection concerns, and specifically whether it will be able to stand up to future legal challenges that will likely be brought before the CJEU. Following the announcement of Privacy Shield, the Article 29 Working Party asserted that it still has concerns about the current U.S. legal framework on privacy protections and intelligence activities, especially regarding scope and remedies.[32] Some critics of the proposed Privacy Shield Agreement claim that the privacy guarantees are largely based on U.S. promises rather than legal enforcement mechanisms; Jan Philipp Albrecht, a leading Member of the European Parliament on data privacy issues, reportedly asserted that "The proposal foresees no legally binding improvements. Instead, it

[30] Statement from U.S. Secretary of Commerce Penny Pritzker on EU-U.S. Privacy Shield, press release, February 2, 2016.

[31] For example, The Information Technology Industry Council, "Learn More about the EU-U.S. Privacy Shield," press release, February 4, 2016.

[32] European Commission Article 29 Working Party, "Statement of the Article 29 Working Party on the Consequences of the Schrems Decision," press release, February 3, 2016.

merely relies on a declaration by the U.S. authorities on their interpretation of the legal situation regarding surveillance by U.S. secret services."[33]

Many U.S. officials and industry leaders hope that recent Congressional efforts to provide a limited right of judicial redress to EU citizens—undertaken initially to help conclude a separate U.S.-EU umbrella accord for law enforcement, known as the Data Privacy and Protection Agreement (DPPA)[34]—could help ease at least some European concerns about U.S. data protection standards and the new Privacy Shield agreement as well. In March 2015, Representative Jim Sensenbrenner and Representative John Conyers introduced H.R. 1428, known as the "Judicial Redress Act" in order to help meet EU demands for U.S. judicial redress in the DPPA negotiations. An identical measure, S. 1600 was introduced by Senator Chris Murphy and Senator Orrin Hatch in June 2015.

As introduced, both H.R. 1428 and S. 1600 essentially sought to extend the core of the judicial redress provisions in the U.S. Privacy Act of 1974 to citizens of covered countries or regional organizations (such as the EU) with whom the United States has entered into an agreement "that provides for appropriate privacy protections for information shared for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses" (such as the DPPA). H.R. 1428 passed the House on October 20, 2015, and was approved by the Senate Judiciary Committee on January 28, 2016, with an amendment introduced by Senator John Cornyn. The Cornyn amendment included additional provisions mandating that the Judicial Redress Act would be 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." The amended H.R. 1428 passed the Senate on February 9, 2015, and the House on February 10, 2016.

Many U.S. officials and industry leaders hope that if enacted, the Judicial Redress Act would be a concrete indication of the U.S. commitment to addressing EU data protection concerns, restore trust in U.S.-EU data flows, and as a result, boost confidence in the new Privacy Shield accord. Others note that it remains unclear to what extent the Judicial Redress Act might help the United States meet EU data protection "adequacy" standards more broadly or ease concerns about U.S. government access to personal data in the commercial sector. They point out that the scope of the judicial redress in the proposed U.S. legislation is not exactly equivalent to what U.S. persons and residents enjoy under the Privacy Act, is relatively limited, and relates specifically to information transferred in a law enforcement context. As such, many experts doubt that the Judicial Redress Act will be considered an overall "fix" to the concerns about U.S. data protection standards raised by EU authorities and the CJEU.[35]

---

[33] As quoted in Natasha Lomas, "Europe and U.S. Seal Privacy Shield Data Transfer Deal to Replace Safe Harbor," Techcrunch.com, February 2, 2016.

[34] Negotiations on the DPPA began in 2011 to bridge U.S.-EU differences in the application of privacy rights and better protect personal information exchanged in a law enforcement context. The proposed DPPA is intended to serve as an "umbrella" agreement, thereby helping to 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 major hurdle. In early September 2015, negotiators finalized and initialed the text of the DPPA. The EU asserts that the DPPA will not be signed until U.S. judicial redress legislation is adopted. The European Parliament and the Council must then approve the DPPA for it to take effect (Congressional approval of the DPPA itself is not required because the United States has negotiated the DPPA as an executive agreement).

[35] Independently of the CJEU decision, Congress has been considering reform and reauthorization of the legal authorities used by the NSA which were found objectionable by the CJEU. Those authorities are currently scheduled to sunset at the end of 2017. See CRS Report R42725, *Reauthorization of the FISA Amendments Act*, by (name redacted) Additionally, several legal challenges to the same provisions are currently being considered by U.S. courts. See CRS (continued...)

Options for Affected Companies in the Interim

Until the new U.S.-EU Privacy Shield Agreement is formally concluded and implemented, companies engaged in transatlantic data transfers must employ other means to legitimize such transfers. As noted above, Safe Harbor was one of several mechanisms used as a legal basis for U.S.-EU data transfers. Furthermore, Safe Harbor was limited to FTC-regulated sectors. Others, such as financial services, were never covered by Safe Harbor. None of the alternative available mechanisms, however, are viewed as a complete alternative to a comprehensive transatlantic accord like Safe Harbor or the envisioned Privacy Shield.[36] For example:

- **Model Contract Clauses.** The European Commission has decided that certain standard contractual clauses offer sufficient data protection. These require organizations to have a data processing agreement based on the model clauses in place with any entity with which data is exchanged. This can be time consuming and expensive for many companies. While many large corporations such has Salesforce, Microsoft, and Google are employing model contract clauses, they may be challenging for small- and medium-sized enterprises (SMEs), which make up around 60% of Safe Harbor companies.
- **Binding Corporate Rules (BCRs).** These are a set of rules, based on European data standards, which a company can implement and have approved by national DPAs. A constraint with BCRs is that they only cover intra-company data transfers. Furthermore, implementing BCRs is a complex and time-consuming process that can take up to two years.
- **Consent.** Explicit consent agreements are another option, which may be useful in some business-to-consumer situations. Under the DPD, for a business to rely on consent as a valid ground for processing personal data, the consent must have been unambiguously given, 'freely' given and not given under compulsion or as a result of an act of deceit, and constitute a 'specific and informed indication' of a person's wishes for data to be processed. This may be a high threshold for many companies to meet for each data transaction, especially human resources-related companies, which comprise 50% of the Safe Harbor companies.[37]

Issues for Congress

The CJEU's invalidation of Safe Harbor and the newly proposed EU-U.S. Privacy Shield Agreement raise issues for Members of Congress. These include implications for the following:

- **U.S. and EU Economies.** As noted earlier, the United States and the EU remain each other's largest trade and investment partners and the transatlantic flow of data is of critical importance for the U.S. and European economies. Members may further explore the economic costs of a prolonged disruption of transatlantic data flows.

(...continued)

Report R43459, *Overview of Constitutional Challenges to NSA Collection Activities*, by (name redacted), (name redacted), and (name redacted) .

[36] Another option, which some companies are employing, is establishing data centers within EU member countries.

[37] Presentation of The Honorable Julie Brill, Commissioner, U.S. Federal Trade Commission, The European Institute, *Safe Harbor: The Schrems Case & What Comes Next*, Washington, DC, October 20, 2015.

- **T-TIP Negotiations.** Although negotiations on a revised Safe Harbor agreement have been progressing on a track separate from the T-TIP negotiations, the CJEU decision may influence the ongoing T-TIP negotiations. U.S. companies have been advocating for measures in T-TIP that would prevent restrictions on cross-border data flows and for new mechanisms that would provide alternative ways for U.S. companies to comply with EU data privacy rules beyond those that already exist. There may also be resistance in Europe to any T-TIP outcome perceived to adversely affect EU data protection and consumer privacy rules.
- **U.S. Judicial Redress Legislation.** Members may also wish to explore the European response to the passage of U.S. legislation (H.R. 1428). There remains debate whether the U.S. redress legislation will be sufficient to satisfy European critics. For example, the current legislation does not provide citizens of EU countries with redress that is exactly on par with that which U.S. persons enjoy under the Privacy Act. One area of particular concern is that the legislation currently being discussed does not extend privacy protections to records pertaining to non-U.S. persons collected by all U.S. agencies. Personal information collected by non-law enforcement agencies (such as the Department of Health and Human Services, for example) would not be covered.
- **Other U.S.-EU Information-sharing Agreements.** Some analysts contend that the sweeping nature of the CJEU's decision could have implications for other U.S.-EU data-sharing arrangements, especially in the law enforcement field. These include the U.S.-EU Passenger Name Record (PNR) agreement on sharing airline data, the U.S.-EU accord on tracking financial data (often referred to as the SWIFT agreement) as part of the U.S. Treasury Department's Terrorist Finance Tracking Program (TFTP), and the proposed "umbrella" Data Privacy and Protection Agreement. Congress has strongly supported the PNR and SWIFT agreements as key U.S. counterterrorism tools. Like Safe Harbor, however, both the PNR and SWIFT agreements have received increased scrutiny in the EU since the "Snowden leaks," and some Members of the European Parliament have raised questions about the security of PNR data and called for the suspension of the SWIFT agreement. Many U.S. officials hope that the intelligence safeguards proposed in the new Privacy Shield Agreement (along with the DPPA and the Judicial Redress Act, if enacted) will help to assuage some of the broader EU concerns about U.S. data protection standards and data sharing for law enforcement purposes.[38]

Author Contact Information

(name redacted)
Specialist in International Trade and Finance
[redacted]@crs.loc.gov, 7-....

(name redacted)
Specialist in European Affairs
[redacted]@crs.loc.gov, 7-....

[38] For more information, see CRS Report RS22030, *U.S.-EU Cooperation Against Terrorism*, by (name redacted)