Congressional Research Service
Informing the legislative debate since 1914

The EU-U.S. Safe Harbor Agreement on Personal Data Privacy: In Brief

Martin A. Weiss
Specialist in International Trade and Finance

Kristin Archick
Specialist in European Affairs

October 29, 2015

Congressional Research Service
7-5700
www.crs.gov
R44257

CRS REPORT
Prepared for Members and
Committees of Congress

Contents

Contacts

Overview

On October 6, 2015, the Court of Justice of the European Union (CJEU) delivered a judgment[1] that invalidates the Safe Harbor Agreement between the United States and the 28-member European Union (EU).[2] Safe Harbor is a 15-year-old accord, under which personal data could legally be transferred between EU member countries and the United States. 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 applies 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 case stems from a 2013 complaint brought by an Austrian citizen and Facebook user, Maximillian Schrems, who claimed that the United States, and ultimately the Safe Harbor Agreement, failed to meet EU data protection standards in light of the unauthorized disclosures of classified U.S. surveillance programs by former U.S. National Security Agency (NSA) contractor Edward Snowden. In its decision, the CJEU determined that U.S. data protection measures do not provide an "adequate level of protection" for personal data as required by the EU DPD, and thus Safe Harbor, as currently agreed, is invalid. The CJEU ruling also found that the agreement's national security exemptions essentially prevail over the Safe Harbor principles. Any companies that were using Safe Harbor as a legal basis for transatlantic data transfers must now individually implement alternative measures including so-called "model contractual clauses" or Binding Corporate Rules (BCRs) to legitimize the transfer of personal data between the United States and the EU.

Given that some 4,500 U.S. companies (including U.S. subsidiaries of European firms) participate in Safe Harbor and that digital trade flows make up an important and growing segment of the transatlantic economy, many trade and industry groups were deeply dismayed by the CJEU's decision. Experts suggest that the CJEU ruling could create legal uncertainties for many U.S. companies. Some contend that the CJEU judgment could raise operating costs, especially for small- and medium-size businesses, and negatively affect U.S.-EU trade and investment ties.

Some analysts also contend that the broad nature of the CJEU's decision could have implications for other U.S.-EU data-sharing arrangements, in both the commercial sector and the law enforcement field. Such U.S.-EU agreements, including Safe Harbor, have come under increased scrutiny since the revelation of the NSA programs and subsequent allegations that some U.S. Internet and telecommunication companies were involved in the reported NSA activities. The United States and the EU have engaged in a number of efforts to address European concerns about U.S.-EU data flows, including discussions started in late 2013 to improve the Safe Harbor Agreement. Although negotiations between the EU and U.S. authorities are reportedly close to completion, divisions still exist over the EU demand to ensure only limited access to "Safe Harbor data" for national security purposes. Some experts suggest, however, that U.S. legislation currently under consideration, *the Judicial Redress Act of 2015* (H.R. 1428 and S. 1600), could

[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.

help ease at least some concerns about U.S. data protection standards and facilitate a revised Safe Harbor accord. The proposed legislation would essentially provide citizens of EU countries with judicial redress for data protection breaches. H.R. 1428 passed the House on October 20, 2015.

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 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.

---

[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).

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 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. However, this reform package must still be finalized by the EU member states (acting in the Council of the European Union) and the directly-elected European Parliament (which represents the citizens of the EU).[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

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

[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 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 Gina Stevens.

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.

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]

[12] 18 U.S.C. § 2510 et seq.

[13] For example, see: CRS Report RL34693, *Online Data Collection and Disclosure to Private Entities: Selected Federal Laws and Self-Regulatory Regimes*, by Kathleen Ann Ruane; CRS Report R41756, *Privacy Protections for Personal Information Online*, by Gina Stevens; and CRS Report R42338, *Smart Meter Data: Privacy and Cybersecurity*, by Brandon J. Murrill, Edward C. Liu, and Richard M. Thompson II.

[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 Shayerah Ilias Akhtar, Vivian C. Jones, and Renée Johnson. See also, CRS In Focus IF10120, *Transatlantic Trade and Investment Partnership (T-TIP)*, by Shayerah Ilias Akhtar and Vivian C. Jones.

[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.

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.

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 may be limited to the extent necessary for national security, public interest, or law enforcement requirements.

Under Safe Harbor, a U.S. company can self-certify annually to the Department of Commerce that is has 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, are as follow.

- **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.

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

[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.

- **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.
- **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 is 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 are on the Safe Harbor list. To qualify, organizations must self-certify annually in a letter to the DOC that they adhere to the Safe Harbor principles. The FTC is 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 are required to enforce the Safe Harbor Agreement. Private sector enforcement has three components: verification; dispute resolution; and remedies. Persistent failure to comply will result in withdrawal of "Safe Harbor" status, a fact that will be listed 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 do not fall under the jurisdiction of the FTC and the DOT are not eligible for "Safe Harbor." Notably, this includes U.S. financial firms and telecommunications carriers. Following the Schrems decision, however, the FTC will no longer enforce Safe Harbor.[21]

[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.

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 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 adhering to Safe Harbor provided an "adequate level of protection" as required by the DPD. Upon request by the Irish High Court, the CJEU considered whether the Irish DPA was permitted to 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 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 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.

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

[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.

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.

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] European Commission officials announced three broad priorities for managing U.S.-EU data flows in the short term: (1) protecting personal data transferred across the Atlantic; (2) ensuring the continuation of transatlantic data flows; 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]

Moving Toward Safe Harbor 2.0

Since late 2013, the European Commission and U.S. authorities have engaged in discussions aimed at "making Safe Harbor safer" in response to concerns raised after the unauthorized disclosures of U.S. surveillance activities. These negotiations have taken on new urgency following the CJEU decision. However, a key sticking point (even before the CJEU judgment) has been the existing Safe Harbor Agreement's national security exemptions. Recent Congressional efforts to essentially extend the 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)[25]—could help facilitate a revised "Safe Harbor 2.0" accord.

[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] 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 (continued...)

In March 2015, Representative Jim Sensenbrenner and Representative John Conyers introduced H.R. 1428, which would essentially extend the core of the judicial redress provisions in the U.S. Privacy Act of 1974 to EU citizens; S. 1600 Senator Chris Murphy and Senator Orrin Hatch introduced a companion measure, S. 1600, in June 2015. The House passed H.R. 1428 on October 20, 2015. Given that the CJEU's ruling on Safe Harbor highlighted the lack of judicial remedies for EU citizens in the United States as a significant problem in the U.S. data protection approach, some experts believe that if enacted, such U.S. judicial redress legislation (and the DPPA) could help ameliorate at least some EU concerns about U.S. government access to data shared through Safe Harbor as well. Others note that the scope of the judicial redress in the proposed U.S. legislation (as in the U.S. Privacy Act) is relatively limited, and is unlikely to be considered an overall "fix" that will enable the United States to more broadly meet EU "adequacy" standards.[26]

Current Status of U.S.-EU Safe Harbor Negotiations

For many years, some European privacy advocates argued that the Safe Harbor Agreement contained loopholes and did not adequately protect European citizens' data privacy. They 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. Some critics also viewed with concern Safe Harbor's national security and law enforcement exemptions, even before the public revelations of the NSA programs.[27]

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" and to improve the functioning of the program as part of a number of efforts to help restore trust in U.S.-EU data flows. These 13 recommendations centered on four broad priorities: enhancing

(...continued)

United States has negotiated the DPPA as an executive agreement). Thus, experts believe it will likely be several years before the DPPA is finalized and enters into force.

[26] 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 Edward C. Liu. Additionally, several legal challenges to the same provisions are currently being considered by U.S. courts. See CRS Report R43459, *Overview of Constitutional Challenges to NSA Collection Activities*, by Edward C. Liu, Andrew Nolan, and Richard M. Thompson II.

[27] Nikolaj Nielsen, "Hundreds of U.S. Companies Make False Data Protection Claims," EUObserver.com, October 8, 2013; Nikolaj Nielsen, "Leading EU Party Wants to Ditch U.S.-EU Data Protection Agreement," EUObserver.com, October 29, 2013; "FTC's Response to Alleged Safe Harbor Violations Could Change Enforcement Standards, Lawyers Say," *Warren's Washington Internet Daily*, August 15, 2014.

transparency; ensuring redress; strengthening enforcement; and limiting the access of U.S. authorities to data transferred under the Safe Harbor framework.[28]

EU policymakers assert that substantial progress has been made on a majority of the 13 recommendations, but EU demands to ensure only limited access to Safe Harbor data for national security purposes reportedly remain a key hurdle. Following the CJEU decision, both U.S. and EU officials stated that they are committed to completing negotiations on an updated version of Safe Harbor as soon as possible. In testimony on October 26, 2015, before the European Parliament, European Commissioner for Justice, Consumers, and Gender Equality, Věra Jourová, noted that U.S. and EU authorities are engaged in "intensive technical discussions," and expressed confidence that there would be significant progress by mid-November 2015.[29]

Future Prospects

Many observers expect that the CJEU decision will spur the negotiations on a new Safe Harbor agreement forward. Officials and industry leaders on both sides of the Atlantic also hope that the recent movement on U.S. legislation aimed at essentially extending U.S. judicial redress to EU citizens will help ameliorate some EU concerns about Safe Harbor's national security exemptions. U.S. technology groups have welcomed the passage of H.R. 1428 and have urged the Senate to act quickly to help restore trust in U.S.-EU data flows and facilitate conclusion of Safe Harbor 2.0.[30]

Other experts suggest, however, that the CJEU ruling could further complicate U.S.-EU efforts to conclude a revised Safe Harbor accord. Even if the parties reach a new agreement, some analysts assert that the CJEU's decision essentially gives national data privacy authorities the ability to second-guess it and conduct their own investigations. As such, some argue that national regulators should be brought into the U.S.-EU negotiations on Safe Harbor, both to ensure that the agreement meets the "adequate" protection threshold and to minimize potential differences in its interpretation among national regulators.[31]

Some analysts also note that given the sweeping nature of the CJEU's decision, the United States and the EU may need to consider further revisions to U.S.-EU data-sharing arrangements and any potential new Safe Harbor framework in order to guarantee EU privacy rights and compliance with the CJEU's judgment. Following the CJEU ruling, a working party of EU DPAs (the Article 29 Working Party) expressed broad concern about the impact of the CJEU's findings on U.S.-EU data-sharing "transfer tools" and 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." The Article 29 Working Party noted, however, that the current negotiations on a revised Safe Harbor accord could be part of the larger solution (along with the

[28] 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.

[29] European Commission, Speech by Commissioner Jourová before the Commitee on Civil Liberties, Justice and Home Affairs, October 26, 2015.

[30] See, for example, Computer and Communications Industry Association, "Tech Industry Applauds House Passage of Judicial Redress Act," press release, October 20, 2015; and Peter Sayer, "Judicial Redress Act Heads for Senate, Making New Safe Harbor Agreement More Likely," *PCWorld.com*, October 21, 2015.

[31] Natalia Drozdiak and Sam Schechner, "EU Court Says Data-Transfer Pact with U.S. Violates Privacy," *Wall Street Journal*, October 6, 2015; Mark Scott, "Data Transfer Pact Between U.S. and Europe Is Ruled Invalid," *New York Times*, October 6, 2015.

proposed U.S.-EU Data Privacy and Protection Agreement). The Article 29 Working Party also asserted that national DPAs may bring legal action against companies that continue to transfer data (in the absence of alternative arrangements). 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.[32]

European Commission officials stress that transatlantic data flows between companies can continue using other mechanisms for international transfers of personal data available under the DPD. In addition, Commission officials point out that the EU's proposed data protection reform regulation—which, as discussed previously, would establish a single set of rules for data protection throughout the EU—is on track to be finalized by the end of 2015.[33] Supporters suggest that it should help ensure a coordinated response from national data protection authorities on data transfers across the Atlantic in the longer term.

Options for Affected Companies

The CJEU's invalidation of Safe Harbor is having an immediate effect on a wide range of U.S. and European companies. As noted above, Safe Harbor was one of several mechanisms used to legitimize transatlantic data transfers. Furthermore, Safe Harbor was limited to FTC-regulated sectors. Others, such as financial services, were never covered by Safe Harbor. However, these alternative mechanisms are unlikely to be an appropriate long-term alternative to Safe Harbor. U.S. concerns about the invalidation of Safe Harbor are shared across the Atlantic. As European Commissioner Jourová commented in response to the CJEU decision, "it is important that transatlantic data flows can continue, as they are the backbone of our economy."[34]

In an October 20 presentation, FTC Commissioner Julie Brill said that companies would need to implement other data transfer mechanisms, including model contract clauses, binding corporate rules, and/or consent agreements.[35] None of these options, however, are a complete alternative to a new comprehensive transatlantic Safe Harbor accord.[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

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

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

[34] Ibid.

[35] 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.

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

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 raises issues that Members of Congress may want to explore. These include:

- **Effect on 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.
- **Impact on T-TIP Negotiations.** Although negotiations on a revised Safe Harbor agreement have been progressing on a track separate from the T-TIP negotiations, and are reportedly nearing completion, 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.
- **Impact on a New Safe Harbor Agreement.** On October 9, Senate Committee on Commerce, Science, and Transportation Chairman John Thune, along with the Ranking Democrat, Senator Bill Nelson and Representative Fred Upton and Representative Frank Pallone, Chairman and Ranking Chairman of the House Committee on Energy and Commerce wrote a letter on behalf of 56 members of the House and Senate to Secretary of Commerce Penny Pritzker and FTC Chairwoman Edith Ramirez urging them to redouble efforts to conclude a successor agreement to Safe Harbor.[38] Prior to any new agreement, several issues likely need to be addressed, including the competency of the European Commission to negotiate such an agreement and the future roles of national DPAs and the CJEU in vetting and approving the potential agreement. Enforcement procedures will also likely need to be addressed in greater depth.

[37] Presentation of The Honorable Julie Brill, Op. cit.

[38] http://www.commerce.senate.gov/public/_cache/files/535d865e-7f3f-472a-9483-1a7ad444c90e/97B62EDD588FD2D56DF3B84FE0B6003C.us---eu-safe-harbor-agreement-letter-from-cst-and-ec.pdf.

- **Impact of U.S. Judicial Redress Legislation.** Members may also explore whether the current legislation (H.R. 1428/S. 1600) is sufficient to address European concerns and if not, what additional domestic legislation may be required. 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.

Author Contact Information

Martin A. Weiss
Specialist in International Trade and Finance
mweiss@crs.loc.gov, 7-5407

Kristin Archick
Specialist in European Affairs
karchick@crs.loc.gov, 7-2668