October 23, 2015

THE CHERTOFF GROUP

POINT OF VIEW

The European Court of Justice Decision on United States-European Union Safe Harbor Framework: Policy Highlights and Business Implications

Executive Summary

On October 6, 2015 the European Court of Justice (ECJ) ruled in the case of Schrems v. Data Protection Commissioner, calling into question the utility of the United States-European Union (U.S.-E.U.) Safe Harbor Framework. The agreement, explained in detail below, allowed U.S. companies to transfer data on European customers to the U.S. by agreeing to handle this data in accordance with a data privacy framework deemed to be consistent with European data privacy regulations. By abrogating the preemptive aspects of this agreement the ECJ has removed legal and regulatory certainty regarding the mechanisms used by U.S. companies to transfer data on their European customers to the United States.

Further, Data Protection Authorities (DPAs) in individual E.U. countries are now able to conduct their own investigations of the data transfer practices of U.S. companies and challenge those transfers in European Courts. Should the DPAs and European Courts determine that the data
transfer practices of a U.S. company violate European data protection regulations (and there is good reason to think they will), the company would be subject to penalties, including the possible suspension of their ability to transfer data between the U.S. and the E.U.

U.S. Information Technology (IT) companies may find it difficult to operate and expand in the European market as risks associated with heightened legal scrutiny and an increasing “buy local” atmosphere could propel European IT companies ahead of many U.S. brands. Though this change would likely not affect large U.S. IT companies with established European presence, including infrastructure, data centers, and a loyal consumer customer base, many U.S. firms would struggle to compete with European companies because of the potentially high regulatory costs, greater legal risks, and general public opposition to and distrust of U.S. firms. European enterprise customers may choose to do business with European companies over their U.S.-based competitors in order to minimize their risk, opting to purchase products and services from Europe-based IT companies that have less exposure to E.U. data protection regulation issues. This advantage will expand opportunities for E.U.-based providers and place further constraints on U.S. firms operating in the European market. The decision may also complicate E.U. companies’ efforts to comply with some of their U.S. legal obligations under the Health Insurance Portability and Accountability Act (HIPPA) or the Dodd-Frank Act.

In the short term, companies will be able to continue their business operations and accompanying data transfers from the E.U. to the U.S. However, they are likely to face disruptions over the next year as DPAs challenge their data transfer practices and E.U.-based enterprise customers shift to E.U.-based IT product and service providers. Companies will no longer be able to use the Safe Harbor program as a means to demonstrate compliance with E.U. data protection regulations, and will instead need to demonstrate compliance with these regulations through alternative means. Perhaps more importantly, companies will potentially need to demonstrate this compliance to the DPAs and courts of each of the 28 E.U. member states—inconvenient for any U.S. company operating in Europe. Such actions could force U.S.-based IT companies to alter their cloud computing and corporate structures to minimize or eliminate the transfer of data on E.U. citizens to the U.S.

These companies will also need to reevaluate their position in the European market place and determine if their company is able to compete with E.U.-based competitors who face fewer data protection regulatory risks. Ultimately, U.S. firms will need to have a strong understanding of their customers’ needs, the capabilities of their E.U.-competitors, and the legal and regulatory dimensions of E.U. data protection requirements and if they wish to continue doing business in Europe.
What is the European Directive on Data Protection and what does it have to do with Safe Harbor?

Safe Harbor and its requirements are rooted in Europe’s primary privacy protection regulation, the European Directive on Data Protection (95/46/EC).1 This directive, adopted by the European Parliament and European Council in 1995, regulates the processing of personal data in the European Union and is an important part of E.U. privacy law. The directive took effect on October 24, 1998 and was meant to standardize data protection and privacy regulations across Europe. By doing so, the regulation simplified and, in some cases, enhanced legal protections and requirements for citizens and companies across the continent.2

As a whole, the Directive reflects Europe’s general view that personal privacy protections are a human right. It requires transparency in how companies handle personal data, requires that data to be used for legitimate purposes for which the data subject has explicitly consented, and requires that data be processed in a manner that is “proportional” to the purpose of the processing. It also forbids “the transfer of personal data to non-European Union countries that do not meet the European Union ‘adequacy’ standard for privacy protection.”3 It is this prohibition that is the subject of the both the Safe Harbor agreement and the ECJ’s decision.

Article 29 of the Data Protection Directive also required the European Commission to establish a “working party” on data protection issues that would serve as an advisor to the Commission. The party, known as the Article 29 Data Protection Working Party, has developed and presented a number of data protection related proposals for the European Commission’s consideration, including Safe Harbor framework.4 The framework was created due to the difficulties that foreign companies, particularly U.S. companies, had determining whether or not they or their country had “adequate” protections in the eyes of European law. The European Commission and the Article 29 Working Party worked with the Department of Commerce to develop a mechanism that would allow them to meet the European standard without being subject to having to achieve some form of certification in all 28 E.U. member states. The result of this effort was the Safe Harbor framework.5

---

1 The full text of European Directive on Data Protection (95/46/EC) is available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. Revisions of the Directive are currently being considered by the EU and may further complicate matters if, and when, those revisions are implemented.
3 See the European Directive on Data Protection (95/46/EC).
What is Safe Harbor?

The Safe Harbor framework is an agreement between the European Commission and the U.S. Department of Commerce that allows companies to transfer data between the U.S. and the E.U. in a manner that was deemed complaint with both U.S. and E.U. law. The agreement provided companies with “safe harbor” for their cross-border data transfers, thus the name of the agreement. It allowed U.S. companies to comply with European data protection regulations through a self-certification process. The agreement, which took effect in 2000, permitted U.S. companies to self-certify that they met the framework’s requirements and thus had “adequate” privacy protections in place, as defined by the E.U. Data Protection Directive. Qualifying companies agreed to “comply with the framework’s requirements,” self-certifying on an annual basis through a filing with the Department of Commerce. In their filing, companies declare their intent to comply with the framework’s requirements and publicize this compliance through a “privacy policy statement.”

The framework’s requirements, while rooted in the data privacy protections contained in the directive, had fewer requirements than the directive itself as it reflects both E.U. and U.S. privacy protection standards. Instead of certifying compliance with the data protection directive, companies instead self-certify their compliance with seven core data protection principles — Notice, Choice, Onward Transfer, Access, Security, Data Integrity, and Enforcement — as well as 15 core data protection compliance questions. Companies must also certify their compliance with a number U.S. government directives and E.U. regulatory decisions specific to the Safe Harbor framework, all of which are available to companies at Export.gov.

As a result of the European Commission’s Decision 2000/520, companies that self-certified with the U.S. Department of Commerce were considered to have an “adequate” level of data protection and thus were compliant with E.U. data protection regulations. As a result, E.U. member states were to consider companies participating in the program as compliant with E.U. data privacy requirements. Companies no longer needed prior approval before transferring personal data from the E.U. to the U.S. This decision effectively pushed the majority of enforcement activity to the United States for U.S. companies (and, likewise, gave the E.U. enforcement over European companies). The decision also allowed companies to avoid seeking approval and certification for their data transfer activities for each E.U. state in which they operated.

---


8 Ibid.
Under the terms of Safe Harbor, U.S. companies were subject to Federal Trade Commission (FTC) review of their compliance with Safe Harbor requirements. While companies are generally expected to regulate themselves, violations of the requirements could result in FTC civil action, including fines, decertification, and public acknowledgement of the violation. Since its inception, the FTC has taken enforcement action against dozens of U.S. companies accused of violating the Safe Harbor agreement, including Facebook, Google, MySpace, L3 Communications, BitTorrent, and the Atlanta Falcons. Notably, while E.U. DPAs are able to file Safe Harbor complaints against U.S. companies with the FTC, they have only done so on four occasions since the inception of the agreement in 2000.

As of October 7, 2015, over 5,000 U.S. companies have participated in the Safe Harbor program with over 4,500 listed as having a certification status of "current." This list includes a wide variety of companies, including major IT players such as Facebook, Google, and Microsoft, security focused companies such as Rapiscan, Raytheon, and Lockheed Martin, and industrial firms including Caterpillar, General Electric, and Honeywell.

What prompted the case?

The case, Schrems vs. Data Protection Commissioner, was prompted by a complaint made by Max Schrems, an Austrian citizen who joined Facebook in 2008, to the Irish Data Protection Authority regarding Facebook’s data privacy practices. In his complaint, Shrems argues that the European Commission, through the Safe Harbor program, allows U.S. companies to effectively declare themselves in compliance with the European Data Protection Regulation without effective oversight, violating his human rights under European law. His complaint alleges violations of his rights to privacy, protection of personal data, and an effective remedy for such violations. He cited U.S. surveillance programs as evidence of the violation of his rights.

Shrems filed his complaint with the Ireland Data Protection Authority, which has jurisdiction over Facebook’s European operations as they are based in Ireland. While Shrems is technically a

---


11 The full list of companies that have participated in the Safe Harbor program is available at the Department of Commerce’s Export.gov site: https://safeharbor.export.gov/list.aspx.

Facebook Ireland subscriber, the nature of Facebook’s operations lead subscriber data to be transferred to the United States—transfers that are covered by the Safe Harbor Agreement. The complaint was filed in the immediate aftermath of the Snowden revelations regarding the National Security Agency’s (NSA’s) Section 702 surveillance program, more widely known as PRISM. This complaint was one of 22 filed by Schrems with the Irish Data Protection Authority regarding Facebook’s handling of personal data.\(^\text{13}\)

Schrems’ voice was part of a larger set questioning how U.S. companies handled the personal data of European citizens in the aftermath of the Snowden revelations. Parliamentarians, privacy advocates, government ministers, and DPA representatives from across Europe questioned U.S. practices and the suspected cooperation of U.S. technology firms with American authorities. Among the most vocal were German DPA authorities and European Justice Commissioner Viviane Reding, who announced that the European Commission would review the Safe Harbor program and its role as a “loophole” that allowed U.S. companies to circumvent E.U. data protection regulation.\(^\text{14}\) These comments helped spur negotiations with the U.S. on possible changes to the Safe Harbor agreement as well as renewed debate over proposed changes to the European Data Protection Directive.

After reviewing Schrems’ complaint, the Irish Data Protection Authority refused to investigate its claims. The Irish Data Protection Commissioner found no evidence that the NSA had accessed Mr. Schrems’ data and noted that the Safe Harbor framework precluded the authority from finding that Facebook and the U.S. offered inadequate protection of Schrems’ rights. Schrems appealed the case to the Irish High Court, who in turn referred it to the ECJ.\(^\text{15, 16}\)


\(^\text{14}\) Ibid.

\(^\text{15}\) See Loomis, “Is the Safe Harbor Framework in Trouble?,”

\(^\text{16}\) On September 23, Yves Bot, the European Advocate General responsible for the case, published a non-binding opinion which found in favor of Schrems and invalidated the Safe Harbor aspects of the framework. The opinion was considered significant as the ECJ often follows the recommendations of the Advocate General when writing its opinion. Notably, the Advocate General’s opinion frequently cited U.S. national intelligence programs as partial grounds for the decision. Media reports prior to the release of the Advocate General’s opinion suggested that the ECJ would invalidate the Safe Harbor framework and it was widely expected that the ECJ’s opinion would closely resemble that of the Advocate General. See Sam Schechner and Natalia Drozdiak, “U.S.-E.U. Data-Transfer Pact Should Be Invalidated, Says Advocate General,” The Wall Street Journal, September 23, 2015, available at http://www.wsj.com/articles/u-s-eu-data-transfer-pact-should-be-invalidated-says-advocate-general-1442998520; “Advocate General Advises E.U.’s Highest Court to Deem Safe Harbor Invalid and to Allow E.U. Data Protection Authorities to Suspend Data Transfers to the U.S.,” Wilson Sonsini Goodrich & Rosati, September 23, 2015, available at https://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-schrems.htm; Loomis, “Is the Safe Harbor Framework in Trouble?”
What did the ECJ decide?

The court, which is the highest court in the European Union in matters of European Union law, had two principal findings in its decision that mirror those from the Advocate General’s opinion in September.

In its first finding, the court found that that the European Commission’s decision that the U.S. has “adequate” data protection under E.U. Law and the Safe Harbor agreement (per Decision 2000/520) does not preempt an E.U. court’s finding to the contrary. That said, the court acknowledged that the courts of E.U. member states had very limited power in such cases, and that only the ECJ has the authority to invalidate a European Commission decision. Limiting this power to the ECJ ensures that E.U. law is applied uniformly across the 28 member states. As such, E.U. states must simply “provide for legal remedies” that allow E.U. citizens to challenge a Commission decision through the local DPA and courts, with the ultimate decision being left to the ECJ. E.U. member states are obliged to comply with Commission decision’s until the ECJ declares a Commission decision to be invalid.17

The second finding, and the one with the most impact, was that the Safe Harbor framework, in its current form, is invalid. While the court’s ultimate finding was the same as the European Advocate General’s, its grounds were much narrower and less reliant on the suspected impacts of U.S. national intelligence programs.

First, it found that U.S. “legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications” to be a direct violation to the right to privacy under the Charter of Fundamental Rights of the European Union. Second, it deemed any failure to provide citizens with a judicially enforceable right to access and delete their personal data as a violation of the right to judicial protection under the charter. It did not directly hold that the U.S. and companies covered by Safe Harbor lacked these protections, but it did note that there was evidence that the U.S. government had excessive access to data.18

Finally, it found several flaws in the European Commission’s decision on Safe Harbor, Decision 2000/250. The court found that the European Commission had not explicitly stated in Decision 2000/250 that the U.S. provides an adequate level of protection through its domestic law or international commitments. It also found that the E.U. Commission had exceeded its authority when it restricted E.U. member states from conducting investigations of companies participating in Safe Harbor suspected of violating E.U. data protection laws. Further, it found that the

---

Commission cannot prevent E.U. countries from suspending data transfers to countries that lack adequate data protection under E.U. law, even if that country was determined to have adequate protection by the Commission. As such, Decision 2000/250, and thus the core of the Safe Harbor agreement, is invalid.\(^\text{19}\)

Thereafter, the court returned the case to the Irish Data Protection Authority for it to decide whether Facebook’s transfer of personal data from Ireland to the U.S. should be suspended on the grounds that the U.S. does not provide an adequate level of personal data protection. It is worth noting that there is no transition period—any protections for data transfers provided by Safe Harbor certification are no longer valid.\(^\text{20}\)

**What is the impact of the decision on companies?**

The immediate impact on the business operations of U.S. companies will be somewhat limited, as the ECJ did not hold that Facebook or any other U.S. company had actually violated the European Data Protection Directive by transferring personal data from the E.U. to the U.S. Further, companies that participated in the Safe Harbor arrangement should, at least in theory, already be engaging in data handling practices that comply with European data protection requirements, though they may not meet the most conservative of interpretations of those requirements. Regardless, companies are likely to face a torrent of regulatory and legal actions. Many companies, if they haven’t already done so, will also consider altering their business operations to ensure they meet European Data protection regulations. These changes may include corporate restructuring to segment E.U data from U.S. data, the implementation of alternative legal provisions in their contracts, the use of model clauses, and/or a shift to European data centers.\(^\text{21}\) However, even with these changes, U.S.-based companies may find it more difficult to compete with their E.U.-based competitors who are likely to be perceived as “lower risk” by European enterprise customers.

U.S. firms are likely to face, as former Department of Commerce General Counsel Cameron Kerry put it, “a Tsunami of legal challenges” regarding their data handling practices, which will prompt investigations from European DPAs and legal action in all 28 E.U. member states.\(^\text{22}\) These complaints will be handled differently by every DPA and court. We may even see legal

---


challenges brought by DPAs that represent provinces or regions within one country, such as Germany, meaning that the possibility of inconsistent judgments exists both across European borders and even within a single country. Some DPAs, such as Ireland’s, are likely to be friendly to at least some technology companies while others will intensely scrutinize U.S. companies for violations of E.U. protections. Some companies have adopted alternative legal strategies for data transfer operations that may help them succeed in these legal actions, but, overall, the decision makes it unclear how most U.S. companies can achieve compliance with the E.U. Data Protection Directive. This lack of clarity has the potential to lead to a legal mess and one that would ultimately require further action by the ECJ, the European Commission, the European Parliament, and/or European Council to rectify conflicting DPA and court decisions across Europe.

Second, the decision has generated negative press for U.S. technology companies in Europe. Many, including Google, Facebook, and Microsoft, have long been the subject of European suspicions regarding their business practices, respect for privacy rights, and cooperation with U.S. intelligence services. This decision reinforces many of those perceptions and will encourage privacy advocates and other opponents of the U.S. technology industry to speak loudly about the decision and how it demonstrates the need for Europe to take further action to protect European rights and businesses. This press will likely affect public perception of other U.S. companies as well, potentially having a negative impact on their business in Europe.

Third, many companies will take steps to demonstrate compliance with European data protection regulations. Some of these strategies may be legal, such as adopting E.U. model data protection clauses for contracts or altering their corporate structure to make E.U. subsidiaries more independent. Others will focus on physical changes, such as relocating operations from the U.S. to Ireland or building new data centers in Europe that make data transfers back to the U.S. unnecessary. Other companies may pursue technology-based strategies to demonstrate their compliance, such as wide-spread encryption of customer data to prevent the U.S. government from obtaining access. All of these options come with associated costs, many of them prohibitive for smaller technology companies without the resources to build a new data center or completely restructure their company. As such, large companies are much better positioned to make changes that will meet European demands—smaller, U.S.-based companies may be forced to withdraw from the market if they are unable to implement new policies, procedures, or technologies which satisfy E.U. DPAs.

26 See Cunningham, “European Safe Harbor Non-Compliance Could Have U.S. Consequences.”
It is also worth noting that this decision will have little direct impact on European companies operating in Europe. These companies were and remain obligated to comply with European data protection regulations, including on how their companies handle data transfers to the U.S. Safe Harbor was set up to cover data transfers from Europe made by U.S. companies, not European companies. However, European companies may face greater scrutiny from E.U. regulators on their data transfer practices because of the current atmosphere. While the decision lacks direct impact on E.U. companies, it will create business opportunities with customers who have lost trust in U.S. companies or faced disruption in their business with U.S. companies as a result of the decision. A less likely parallel opportunity may, however, exist for U.S. companies who process American data under standards, such as HIPAA or the Dodd-Frank act that are arguably more stringent than European data protection rules. These opportunities for European IT companies translate as risk to U.S.-based IT firms impacted by the Safe Harbor decision. The decision is likely to create a difficult operating environment for U.S. IT firms, as they are likely to be perceived as “higher risk” than their E.U.-based competitors when it comes to E.U. data protection regulation compliance. E.U. based enterprise customers may also worry about the potential operational impacts of future DPA actions against their U.S.-based service providers, choosing to instead do business with E.U.-based competitors that will not be impacted by future DPA or court activities on this issue.

How have and should companies react to the decision?

Many larger U.S. companies, especially those with an information technology focus, have been closely tracking Europe’s reaction to the Snowden revelations and the accompanying questions that have been raised regarding the Safe Harbor framework. As such, the ECJ’s decision did not come as a surprise to most technology firms. Some U.S. technology companies have been preparing for the possibility of Safe Harbor’s suspension for years, finding alternative ways to ensure that their operations comply with European data protection regulations even in the absence of Safe Harbor. Proactive companies have already begun reaching out to their customers, explaining what impact, if any, the decision will have on their services, and outlining what the company does to ensure that it adequately protects its customers and their data. Companies looking for guidance on how to respond to the decision would be well served to follow the playbooks being used by some of the larger U.S. IT companies—understand E.U. data protection requirements, build and pursue a plan to ensure company compliance, and communicate with customers regarding plans and commitments to protecting their privacy and personal information.

Microsoft’s President and Chief Legal Officer Brad Smith, for example, issued a public statement via its corporate blog explaining the steps the company has taken to ensure adequate protection of its customers’ data. These steps include, most notably, the adoption of E.U. Model Clauses in its service agreements and contracts which ensure that the company provides adequate data protections to its customers. The Standard Contractual Clauses, created by the European Commission in 2004 and updated in 2010, establish more data privacy requirements than Safe Harbor and incorporate additional language regarding the relationship between
providers and their customers. Microsoft began work on implementation of E.U. Model Clauses in 2011 and received confirmation that it had correctly implemented the Model Clauses from the Article 29 Working Party in April 2014. Smith also noted the company's expanding network of data centers and its, at times public, fights with the U.S. government over providing access to customer data.27

Amazon and Salesforce have also publicly acknowledged their adoption of the E.U.'s Model Clauses and thus remain in compliance with E.U. data protection regulations regardless of the Safe Harbor decision. Others, including Facebook and Google, have expanded their European data centers to an extent that may allow them to alter their data transfer practices in a manner that satisfies E.U. DPAs and courts.28

Another option developed by the Article 29 Working Party, Binding Corporate Rules, legally obligate companies to comply with strict European data protection regulations across their international operations but can be expensive to implement, due to their potential impact on business operations and the need to secure the approval of multiple DPAs. The Binding Corporate Rules process requires companies to identify a primary DPA to handle the process, iterate on draft rules that meet E.U. requirements with the DPA, receive approval and input from the DPAs of other countries/provinces where they operate, and obtain final authorization from all of the above DPAs in order to begin transfers under the auspices of the approved rules. This process often takes over a year and can require the company to make significant changes to their operations in order to achieve compliance.29

Companies impacted by the decision that are still formulating their response should follow the lead of companies such as Microsoft, Google, and Amazon. They should also ensure that their company and counsel understand E.U. data protection requirements. If necessary, retain the services of experts who are able to review business operations and determine company obligations under European law.

The decision leaves most small businesses in a difficult position. Safe Harbor offered a relatively low cost method for small U.S. technologies companies to achieve compliance with E.U. data protection requirements. Without Safe Harbor, small businesses will need to make a difficult choice: find the resources to implement E.U. Model Clauses or Binding Corporate Resolutions, or withdraw from the European market. Some will see it as too resource intensive and difficult to go through these processes, especially if they seek the Article 29 Working Party's blessing for their implementation of either. As a result, a number of U.S. small businesses will

29 See Cunningham, “European Safe Harbor Non-Compliance Could Have U.S. Consequences.”
choose to avoid doing business in Europe rather than meet European data protection requirements.

Finally, whatever a company decides to do, it needs to communicate with its customers and understand its competitors. European customers are paying close attention to this ruling and may already be skeptical of the data protection practices of the U.S. companies they do business with. Some E.U. enterprise customers may consider moving to E.U.-based IT service providers in order to reduce their risk of encountering data protection regulation issues or service disruptions related to future court or DPA decisions. U.S. companies should provide their customers with an overview of the data protection policies they already have in place and outline any plans they have to ensure future compliance with E.U. data protection regulations in light of the ECJ decision, such as adoption of E.U. Model Clauses or limiting transfers of European data to the U.S. Companies may also want to highlight legal reforms in the U.S., such as the passage of the Freedom Act or Presidential Policy Directive 28, in order to highlight changes to U.S. law that enhance privacy protections for E.U. citizens.

U.S. companies will also want to ensure that they understand their E.U.-based competition and their capabilities. Many European companies may be inclined to move their business away from higher-risk U.S.-based firms to European-based ones, especially if European based firms are able to offer a nearly identical service at roughly the same cost. Competitive differentiation will become even more important for U.S.-based firms as the ability to provide a superior service or product may be the only reason a European firm has to choose a U.S.-based company over a European one in the aftermath of this decision.

What do U.S. national intelligence programs have to do with the decision and possible solutions?

U.S. intelligence programs, especially collection occurring under the auspices of Section 702 of the Foreign Intelligence Surveillance Act (such as PRISM), had a significant role in how the Schrems case came to pass and how the ECJ reached its decision. Perceived U.S. government overreach through its intelligence programs made many Europeans uneasy with the idea of their personal data finding its way to the U.S., whether it was through legitimate commercial means or via covert intelligence collection. Europeans remain particularly concerned over allegations of U.S. technology firm cooperation with U.S. intelligence programs.

These concerns were clear in the court’s opinion, which noted the plaintiff’s allegations of unrestricted access to mass data storage on servers in the U.S. The court also referenced the PRISM program in its decision and European suspicions of indiscriminate collection of bulk data.30 Unfortunately, the court did not fully capture the legal restrictions that are in place for access to European data held by American corporations under existing U.S. law. First, the PRISM program can only be used to target specific foreign individuals and only for approved

30 See “Judgement of the Court,” ¶22.
foreign intelligence purposes, such as the investigation of suspected criminal activity. Second, the U.S. government must obtain a court order in order to conduct its surveillance and only once the government receives a court order can it compel a service provider to cooperate. Ironically, data on European citizens actually receives greater legal protection when stored in the U.S., as the NSA does not need to obtain a court order to collect data on non-U.S. citizen intelligence targets stored outside of the U.S.\(^{31}\)

It is also worth noting that the U.S. has made a number of major changes to its intelligence collection programs in the aftermath of the Snowden revelation, many of which extend legal protections to European citizens that are not extended to U.S. citizens by the E.U. One of the largest reforms was the June 2015 Freedom Act (the successor to the Patriot Act). The act reformed the NSA’s bulk collection of metadata, now requiring Internet Service Providers (ISPs) to retain the data and the NSA to obtain a Federal Court order in order to obtain the data from the ISP. It also requires advance approval from the Foreign Intelligence Surveillance Court for each query, reduces the number of “hops” that can be made when reviewing cellphone correspondence, and created a panel of amicus curiae at the Foreign Intelligence Surveillance Act (FISA) court to provide guidance on privacy and civil liberties.\(^{32}\)

The U.S. has also adopted Presidential Policy Directive 28, which was issued by President Obama in January 2014. The directive ordered the Intelligence Community to write detailed rules assuring that privacy protections would apply regardless of nationality. The directive also limits NSA retention of Personally Identifiable Information (PII) on non-intelligence subjects to five years, limits dissemination of PII that is unnecessary to understand foreign intelligence, creates an oversight program for foreign PII, and limits bulk collection of signals intelligence to core national security threats. These threats are espionage and other foreign threats against the U.S., threats to the U.S. from terrorism, threats to the U.S. from WMD, cybersecurity threats, threats to U.S. or allied armed forces, and transnational criminal threats. These restrictions are the first public restrictions placed on an intelligence service on electronic surveillance on non-citizens outside of their home country.\(^{33}\)

In contrast, most European intelligence services face no restrictions on the collection of data on non-European intelligence targets (or for that matter on most European targets). Indeed, on a


per capita basis, European surveillance equals or exceeds American activity.\textsuperscript{34} Meanwhile although Italy requires judicial authorization for an intelligence service to conduct surveillance, neither France, Germany, nor the United Kingdom do. In fact, a new French national security law passed in July 2015 allows the French government to monitor the phone calls and emails of terrorism suspects without a court order, requires ISPs to install monitoring equipment on the behalf of the intelligence services, and allows intelligence agents to plant microphones, cameras, and key loggers in private homes.\textsuperscript{35} While Germany does not run its own bulk collection program, the country’s intelligence service cooperated with the NSA’s collection efforts and is a close partner of intelligence services in both the U.S. and United Kingdom.\textsuperscript{36}

This reality does not, however, change the fact that the perception of American overreach in the intelligence area is strong among European citizens and policy makers. It is likely, therefore, that part of the effort to ameliorate European concern will involve further modifications to, and limitations on, America’s intelligence programs.

**How will this impact the negotiations over Safe Harbor revisions and the European Data Protection Directive?**

When the Schrems decision was announced, the European Commission and U.S. Department of Commerce negotiators were close to a final agreement on the so-called “Umbrella Agreement,” which would effectively amend the Safe Harbor framework and enhanced privacy protections for European citizens.\textsuperscript{37} Negotiators had been working on this agreement for over one year, largely in response to criticisms levied by Safe Harbor’s critics regarding its role as a potential “loophole” in E.U. data protection regulations. While the final version of the agreement has not been released, earlier drafts of the agreement and reports made it clear that the agreement would be contingent on the U.S. extending Privacy Act protections, which are meant to prevent U.S. government misuse of U.S. citizen data, to most European citizens through the passage of the Judicial Redress Act.\textsuperscript{38} The Privacy Act includes exceptions for law enforcement


\textsuperscript{38} An earlier draft of the agreement is available at http://statewatch.org/news/2015/sep/eu-us-umbrella-agreement-full-text.pdf.
and national intelligence, making it unclear how this would effectively address European concerns over intelligence data collection.\(^{39}\)

The invalidation of the existing Safe Harbor framework is likely to throw a wrench in these negotiations. It is unclear if U.S. negotiators will be pressed to provide additional protections to E.U. citizens beyond those already negotiated or if the U.S. is prepared to offer additional concessions. It is also unclear if the U.S. is willing to put more energy into a framework that has been invalidated by the ECJ and has become a primary target of European privacy advocates – especially since the ECJ called into question the legal authority of the European Commission to enter into an agreement that binds the DPA's of the member states. Similarly, Europeans may be skeptical of any agreement involving the “Safe Harbor” label in the aftermath of the court’s decision.

The decision is also likely to have an impact on the E.U.'s continuing consideration of an updated European Data Protection Directive. In 2012 the European Commission released a draft of a new directive that would supersede the 1995 directive and include new language and additional provisions meant to address many of the technological changes that have occurred since the original directive was passed.\(^{40}\) Among the more contentious debates surrounding the new draft related to Article 42, an article included in early drafts but dropped by the Commission prior to public release. The article, sometimes known as the “anti-FISA” provision, would require companies to receive European DPA approval prior to transferring any data to a third-party government. While aimed at disrupting U.S. surveillance programs, it would have the practical effect of disrupting routine trans-Atlantic legal activity, including compliance with the Foreign Corrupt Practices Act, as it would technically prohibit the transfer of even basic compliance related information. Further, DPA's would find it difficult to enforce the provision, which U.S. diplomats in Brussels oppose.\(^{41}\)

It is likely that European Parliamentarians will revive the Article 42 debate in light of the ECJ decision, arguing that it demonstrates the need for the provision and is complimentary to the court’s decision. U.S. diplomats may also have a more difficult time fighting the provision in the current environment, especially if their attention is focused on rescuing the Safe Harbor


Framework. Regardless, any changes to the Data Protection Directive will be subject to re-evaluation in light of the court’s decision.

What does this have to do with Internet “balkanization”?

While perhaps unintended, the invalidation of Safe Harbor is likely to spur further debate over Internet “balkanization,” specifically as it relates to data residency requirements and data transfer restrictions. Some companies will react to the ECJ decision by moving their data on European citizens to European data centers, effectively “localizing” this data in order to ensure that they comply with European Data protection regulations. While this may provide additional protections to European citizens, it will come at a significant cost to the affected companies and may have a negative impact on their operations by reducing the efficiency of their cloud infrastructure and thereby their ability to deliver benefits to consumers.

Cloud computing is dependent on efficient operations that enable the company to offer their customer significant capabilities at a low cost. This efficiency comes from both the scaling of its computing operations and efficient placement of its data center, variables that lead companies to make decisions on data center placement based on operational considerations, not the data residency requirements of local governments. While companies such as Google, Microsoft, and Facebook may find it efficient to place a data center in Europe because of their size and customer base, a smaller startup may find any European data center requirement an impenetrable barrier to entry. The loss of smaller players can have a negative effect on the market, reducing competition and limiting innovation.

The ECJ decision creates clear barriers to cross-border data flows. By invalidating Safe Harbor, the ECJ has effectively placed new restrictions on U.S. companies who are no longer able to legally transfer data between the E.U. and U.S. This disruption in data flows can have a negative impact not just on companies, but on citizens looking to take advantage of the services provided by a U.S.-based information technology company. While well intentioned, the invalidation of the Safe Harbor framework results in further impediment to the free flow of information across the Internet.

If you have any questions about this information, please contact The Chertoff Group directly at strategy@chertoffgroup.com or (202) 552-5280.