Joint Hearing on

"Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows"

The Subcommittees on Commerce, Manufacturing, and Trade, and Communications and Technology

November 3, 2015

Washington, DC

Testimony of Victoria Espinel
President and CEO
BSA | The Software Alliance

Testimony of Victoria Espinel
President and CEO, BSA | The Software Alliance
Joint Hearing on "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows"
November 3, 2015
Washington, DC

Good morning Chairman Burgess, and Ranking Member Schakowsky, Chairman Walden and Ranking Member Eshoo, and members of both Subcommittees. My name is Victoria Espinel, and I am the President and CEO of BSA | The Software Alliance ("BSA"). BSA is the leading advocate for the global software industry in the United States and around the world.[1]

I appreciate the opportunity to testify today on behalf of BSA. BSA has long been a strong supporter of efforts to promote and preserve free flows of data across borders.

BSA members provide a wide range of market-leading software and online services to consumers and enterprises across the globe. Billions of customers from around the world—from the smallest business and most remote farm to the largest multinational corporations—rely on our solutions to store, process and derive insights from their data, and to do business with suppliers, partners, and their own customers. In a very real sense, data is the fuel that helps businesses today compete and succeed. Cross-border data flows are therefore key to the current and future success of the United States economy. When events occur that threaten the legal underpinnings that enable such data flows, they pose great disruptions which can forestall that promise of common benefit.

The recent decision in Europe striking down the U.S.-EU Safe Harbor is thus of significant concern to us. Uncertainty about international data flows deters innovation, and makes it much more difficult for our millions of customers to do business in Europe.

Congress, and the U.S. Government more broadly, need to engage immediately and actively with their European counterparts to restore trust and efficiency to trans-Atlantic data flows. Specifically, we need three things: rapid consensus on a new agreement to replace the Safe Harbor, sufficient time to come into compliance with the new rules, and a framework in which the European Union and United States can develop and agree on a sustainable, long-term solution that reflects and advances the interests of all stakeholders.

BSA's members are totally committed to protecting data in their care, regardless of where that data originates, and to providing solutions that give individuals robust control over their data. Our members work hard to build privacy and security into their products and services from day one. We are ready to work with our Government, and with the governments of Europe, to ensure that data continues to flow across our borders to the benefit of both Americans and Europeans.

The U.S.-EU Safe Harbor

As the Subcommittees are well aware, on October 6, 2015, the EU's highest court—the Court of Justice of the European Union—struck down the U.S.-EU Safe Harbor Framework.

Under EU law, personal information—which includes a very wide range of data—can generally only be moved to third countries under the cover of protections deemed "adequate" by the European Union. The U.S.-EU Safe Harbor Framework, which was adopted in 2000, was designed to allow companies to self-certify their commitment to seven specific privacy principles, and thereby demonstrate that they provide "adequate" privacy protection as required by EU law. For 15 years, thousands of U.S. and European companies relied on that mechanism to do business with each other and to serve individuals and enterprises in Europe.

[1] BSA's members include Adobe, Altium, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks and Trend Micro. *See* www.bsa.org.

In striking down the Safe Harbor, the Court of Justice explained that "adequacy" requires that the protections afforded to European information when it travels *outside* of Europe must be "essentially equivalent" to the protections afforded to that information *inside* of Europe. The Court made clear that in assessing essential equivalence, it is necessary to consider a country's rules governing the storage and access of data by law enforcement, and the ability of Europeans to seek judicial redress for breaches of their privacy rights. The Court was particularly troubled by the Snowden leaks and allegations of "indiscriminate surveillance and interception" and "mass and undifferentiated accessing" of Internet users' personal data by U.S. public authorities.

The Importance of the U.S.-EU Safe Harbor on Both Shores of the Atlantic

The striking down of the Safe Harbor has created substantial legal and business uncertainty. The disruption is not a one-way street, limited in its harm to U.S. companies that do business in Europe. Many European companies that do substantial business in the United States, including pharmaceutical, aviation, and automotive firms, routinely transfer data between the United States and Europe.

At the time of the Court's decision, more than 4,000 companies were using the Safe Harbor mechanism to transfer data to the United States. This included multinational software companies, such as BSA's own members, who often move data across the Atlantic for processing or to improve the quality and efficiency of their services. But it also included American companies in a diverse range of other sectors including media, retail, leisure, consumer goods, and even agribusiness, who relied on the Safe Harbor to serve European consumers, to do business with European partners, and to make use of our world-class datacenter capabilities and innovative data analytics services. As important, following the Court of Justice's decision, European companies that could transfer data to Safe Harbored companies simply and easily may now need to comply with more burdensome rules to transfer data outside of Europe. Furthermore, while still valid, those alternative transfer mechanisms have been called into question as potentially susceptible to the same concerns as the Safe Harbor.

The invalidation of the Safe Harbor disrupts each and every one of these companies.

A 2013 study by the European Centre for International Political Economy ("ECIPE"), for example, found that in the absence of the Safe Harbor, the value of U.S. services exported to the European Union could drop by -0.2 percent to -0.5 percent.

The harm would be bilateral: EU service exports to the United States would be expected to decrease anywhere between -0.6 percent and -1 percent.[2] With U.S. imports of private commercial services totaling more than $148 billion in 2013,[3] this is not an insignificant figure.

Alternative Routes to Transfer Data

Now that the Safe Harbor has been struck down, American companies can no longer rely on it to transfer data here from the 28 countries in the European Union. However, the Court did not address any of the other EU law mechanisms that are used today to transfer data from the European Union to the United States, such as model contract clauses, or binding corporate rules.

Both the European Commission and European data protection authorities have reaffirmed that these and other EU data transfer mechanisms remain available at least for another three months following the Court's decision. This has given both companies transferring data and their customers some confidence that their data can still flow to the United States consistent with EU law in the near term. In addition, companies transferring data, including BSA's members, continue to apply the same robust security measures to information in their care – providing further reassurance to customers.

---

[2] ECIPE, "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce" (March 2013); available online at https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf

[3] United States Trade Representative, European Union, Key Trade and Investment Data and Trends, *available online at* https://ustr.gov/countries-regions/europe-middle-east/europe/european-union.

Those alternative mechanisms are not a cure-all, however. While many companies used the Safe Harbor as part of an array of different transfer mechanisms, the Safe Harbor served a unique role as among the simplest of these mechanisms. For example, if a U.S. cloud provider does business with 100 European enterprises, prior to the Court's judgment, that cloud provider could do so through compliance with a single mechanism—the Safe Harbor. Today, that company might need to put in place a data transfer agreement with all 100 enterprises, possibly in 28 different EU markets, and potentially file or even seek regulatory approval from data protection authorities in many of these markets. That process places a heavy burden on the cloud provider, and one that can be particularly difficult for smaller companies to bear. It is also a long process as European regulatory approvals can take time, especially if many companies seek this approval simultaneously. With the invalidation of Safe Harbor, European data protection authorities face the prospect of having to process hundreds or thousands of such applications.

Also concerning, there are signs that the overall stability of the EU-U.S. framework for transferring data is threatened. Recently, for example, German data protection authorities announced that they will no longer authorize transfers to the United States on the basis of Safe Harbor, nor will they issue new authorizations for transfers to the United States under data transfer agreements or binding corporate rules. The ECIPE study that I mentioned above in fact contemplated this "worst case" scenario. It found that if the alternatives to the Safe Harbor were also unavailable, bringing data flows to a near halt, imports of services into the European Union from the United States could decrease by -16.6 percent to -24 percent.

There are also warning signs that this trend may be spreading to countries outside the European Union, many of which have adopted European-style data protection laws. Swiss authorities have now said that the U.S.-Swiss Safe Harbor, which mirrors the U.S.-EU Safe Harbor, no longer constitutes a sufficient legal basis for data transfers under Swiss law. Israel, also, has revoked authorizations for data transfers under the Safe Harbor.

Immediate Next Steps

When the Court of Justice issued its decision, the United States and European Union governments were already deep in negotiations on revising the Safe Harbor agreement. This new version of the Safe Harbor Framework will include up-to-date safeguards for "Safe Harbored" data in the United States.

Updating the Safe Harbor Framework makes good sense. Much has changed since the Safe Harbor was first agreed in 2000. Today, data is generated and transferred in quantities that were scarcely imaginable 15 years ago. The volume of business data worldwide, across all companies, is now doubling every 1.2 years,[4] and more than 90 percent of the world's data was created in the last two years.[5]

Updating the Safe Harbor to reflect these changes is timely. EU-U.S. negotiations must continue – on an expedited timetable and with the vocal support of Member State governments—and a new Safe Harbor must be agreed quickly, ideally well before January 31, 2016. European data protection authorities have already made clear that "[i]f by the end of January 2016, no appropriate solution is found with the U.S. authorities . . . EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions."[6]

Even if there is quick consensus on a new agreement to replace the Safe Harbor, American (and European) companies will need a longer standstill period in which to adapt their operations to the new legal realities. A longer standstill period is essential to preserving the expectation of software and technology providers, companies that rely on these services, and consumers on both sides of the Atlantic.

---

[4] Corry, Will. "BIG Data / The Volume Of Business Data Worldwide, Across All Companies, Doubles Every 1.2 Years, According To Estimates." The Marketing Blog 2012. *available at* http://www.themarketingblog.co.uk/2012/10/big-data-the-volume-of-business-data-worldwide-across-all-companies-doubles-every-1-2-years-according-to-estimates/

[5] IBM, "What Is Big Data"; *available at* http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

[6] *See* Statement of the Article 29 Working Party (October 16, 2015), available at http://www.cnil.fr/fileadmin/documents/Communications/20151016_wp29_statement_on_schrems_judgement.pdf

U.S. and EU negotiators have indicated that they have made significant progress toward a new agreement to replace the Safe Harbor. We encourage them to push forward aggressively with this dialogue, and to agree and announce a new agreement within the next 90 days if possible, with the encouragement of Congress wherever necessary at both the EU and Member State levels.

Looking Ahead

A new agreement to replace the Safe Harbor is a vital and essential step. But it is not the complete solution to the larger issue of privacy protections in the digital age. We urge Congress, and the United States Government more broadly, to look to the longer term.

The European Court of Justice's ruling set a standard of "essential equivalence" between the protections over data in Europe and the United States. What "essential equivalence" means is going to require careful consideration and analysis. One potential place to start is with a comparison of the European Union's and United States' rules and practices in relation to surveillance and law enforcement access to data.

Of course, the United States already has many laws in place that protect against the concerns over "mass and undifferentiated" surveillance raised by the European Court. And the United States has also recently made important reforms to its surveillance laws and processes, including through Executive Orders and the USA FREEDOM Act. These reforms are not well understood in Europe. We urge the United States Government to actively communicate these reforms.

At the same time, we also urge the U.S. Government to listen carefully to Europe's concerns about the extent and the limitations of U.S. law, including in relation to its limited applicability to non-U.S. persons.[7] It may well be that further reform of U.S. law is appropriate to address at least some EU concerns. This change can come through vehicles like the Judicial Redress Act, which BSA strongly supports and which speaks directly to one of the points raised by the European Court. This and similar reforms will help reassure Europeans that their rights will be respected when their data is transferred to the United States. Equally important, and independent of the Safe Harbor controversy, these changes will also reassure customers of American companies around the world.

It is also clear that there are concerns on the European Union side in relation to the transparency of what happens to data collected in the European Union when it is exported to the United States under the Safe Harbor. Significant changes in this space have been made in the past two years. U.S. companies fought for, and won, the ability to provide increased transparency around data requests to all consumers around the world. The U.S. government also has worked to increase transparency around data requests.[8] Creative, and multilateral, approaches will be needed to reach compromise here.

Ultimately, however, "essential equivalence" will be a dynamic concept that will change as European and U.S. laws and practices evolve. Companies cannot, and should not, be expected to update their compliance mechanisms every few years, each time the "essential equivalence" equation shifts. The Safe Harbor lasted nearly 15 years. To achieve that sort of stability, we will need to arrive at a meeting of the minds between the United States and Europe that will allow for a more enduring solution for data transfers, capable of standing the test of time.

Helpfully there are already several good ideas on the table. For example, a number of commentators have suggested and supported the idea of a new trans-Atlantic—or potentially even broader – agreement that ensures that public authorities in the United States and the European Union can ensure

[7] Some of the perceived limitations of the USA FREEDOM Act's reforms have been discussed in a recent study by the European Parliament Directorate General for Internal Policies, "A Comparison between US and EU Data Protection Legislation for Law Enforcement," September 2015; *available online at* http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf

[8] *See* ODNI Releases Transparency Implementation Plan (describing plans for new efforts as well as US intelligence community efforts to increase transparency in recent years) (Oct. 27, 2015), *available online at* http://www.dni.gov/index.php/newsroom/press-releases/210-press-releases-2015/1275-odni-releases-transparency-implementation-plan.

access to data when necessary (wherever that data is held), but in a way that ensures that those demands respect the domestic law of the individual's home country.

The United States and Europe are not as far apart in terms of privacy principles and practices as some might think. Just as privacy is a fundamental human right in Europe, the U.S. Constitution's 4th Amendment enshrines protection from government intrusion, and has done so since 1791. And many American companies already meet European-level data protection standards as a result of their global business operations. Congressional support in communicating this common ground to European leaders is essential to achieving a durable solution.

Where there are gaps that span the Atlantic, whether perceived or actual, we can close these, through a combination of dialogue, domestic legal reform, and international commitments. Congress will be a key part of enabling this to happen.

Thank you again Chairman Burgess, and Ranking Member Schakowsky, Chairman Walden and Ranking Member Eshoo, and members of both Subcommittees for providing this opportunity to share BSA's views on this important matter. I look forward to answering any questions you might have.