Statement of the U.S. Chamber of Commerce

ON: The EU Safe Harbor Decision and Impacts for Transatlantic Data Flows

TO: United States House of Representatives Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade

BY: John Murphy
Senior Vice President for International Policy
U.S. Chamber of Commerce

DATE: November 3, 2015

1615 H Street NW | Washington, DC | 20062

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

More than 96% of Chamber member companies have fewer than 100 employees, and many of the nation's largest companies are also active members. We are therefore cognizant not only of the challenges facing smaller businesses, but also those facing the business community at large.

Besides representing a cross-section of the American business community with respect to the number of employees, major classifications of American business—e.g., manufacturing, retailing, services, construction, wholesalers, and finance—are represented. The Chamber has membership in all 50 states.

The Chamber's international reach is substantial as well. We believe that global interdependence provides opportunities, not threats. In addition to the American Chambers of Commerce abroad, an increasing number of our members engage in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Chairman Burgess, Chairman Walden, Ranking Member Schakowsky, Ranking Member Eshoo and distinguished members of the committees, my name is John Murphy, and I am Senior Vice President for International Policy at the U.S. Chamber of Commerce (Chamber). I am pleased to testify today on the European Court of Justice (ECJ) Safe Harbor decision and its impact on transatlantic data flows. The Chamber is the world's largest business federation, representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and it is dedicated to promoting, protecting, and defending America's free enterprise system.

Together, the United States and the European Union account for nearly half of global economic output, with each producing approximately $17 trillion in GDP. Total U.S.-EU commerce—including trade in goods and services and sales by foreign affiliates—tops $6 trillion annually and employs 15 million Americans and Europeans.

The U.S.-EU investment relationship is without peer. Companies headquartered in EU Member States had invested more than $1.7 trillion in the United States by the end of 2014 and directly employ more than 3.5 million Americans. Similarly, U.S. firms have invested $2.5 trillion in the EU—a sum representing more than half of all U.S. investment abroad. It's also nearly 40 times as much as U.S. companies have invested in China.

Almost all of this trade and investment is dependent on some form of digital services, whether through direct interactions with customers over the Internet, intra-company human resources management, or a European visitor using a credit card while vacationing in Washington, D.C.

The United States and the EU are global leaders in digital trade, which contributes more than $8 trillion annually to the global economy. The "Internet economy" represented $2.3 trillion or 4.1% of global GDP in 2010 and is expected to reach $4.2 trillion and 5.3% by 2016. One recent study has shown the benefits of a secure, stable, and interoperable Internet reaching as high as $190 trillion by 2030.[1]

These numbers may even underestimate the economic importance of these digital connections to the world economy. Consider, for example, the fact that three-quarters of the value created by digital trade accrues to firms not usually viewed as "Internet companies," such as manufacturers, retailers, and banks. In short, today, there are no Internet companies: There are only companies. And there is no Internet economy: There is only the economy.

Importance of Cross-Border Data Flows

The strength of the U.S.-EU economic relationship relies on the seamless flow of data across borders. While many immediately think of services such as email, in fact cross-border data flows are integral to Chamber members of every size and sector—from small businesses to multinationals, from banking to manufacturing to healthcare. Data is also transferred for

[1] See a recent report by the Atlantic Council and Zurich Insurance finding an optimal "Cyber Shangri-la" would result in substantial global economic gain http://www.atlanticcouncil.org/news/press-releases/atlantic-council-zurich-insurance-report-finds-the-global-benefits-of-cyber-connectivity-expected-to-outweigh-costs-by-160-trillion-through-2030.

purposes well beyond just the personal and commercial, including public health and safety concerns.

For example, medical device manufacturers routinely transfer data across the Atlantic for maintenance and repair purposes. In many cases sophisticated medical equipment cannot be transported to repair facilities, but skilled technicians can provide real-time service on large medical equipment across the Atlantic to facilitate effective patient care. In this case, cross-border data transfer restrictions literally could have life or death consequences for patients.

Data transfers are also used to prevent fraudulent activity, identifying criminals who, after racking up huge debts in one country, are able to start fresh with a clean slate by moving to another jurisdiction. Credit histories that follow individuals across borders also affect law-abiding expatriates who are unable to open accounts or obtain loans because they have no way to prove they have a strong credit history in their country of origin.

Safe Harbor and the European Court of Justice Decision

However, the overwhelming benefits of transatlantic data flows are now endangered due to the reverberations of the recent ECJ decision on Safe Harbor. The U.S.-EU Safe Harbor agreement was developed to help companies comply with a 1995 EU law that prohibits the transfer of personal data to any country that does not provide "adequate" protections for the use of that data. Only five countries outside Europe[2] are deemed "adequate," with the United States being "adequate" only to the extent that a company is committed to the Safe Harbor obligations—a commitment overseen by the Federal Trade Commission (FTC). It should be noted that the EU's "adequacy" determinations do not follow a set process.

Safe Harbor has served as a valuable tool for companies of all sizes and sectors to assure Europeans that companies are meeting EU data protection standards for a variety of business-to-consumer and business-to-business functions. For example, a U.S.-based education institution may use Safe Harbor to provide online services to remote students across the European Union. Or a Texas-based startup may provide data analytics for a German-headquartered energy company. Or very simply, many multinational companies use Safe Harbor to ensure employees around the world are paid; manage global supply chains; and ensure compliance with certain legal requirements, including SEC reporting.

On October 6, the ECJ ruled that the Safe Harbor agreement is invalid because it does not preclude U.S. authorities from accessing the personal data of Europeans and using it in a way that is "beyond what is strictly necessary and proportionate to the protection of national security." The ECJ also noted the inability of European citizens to seek redress for inaccurate personal information held by the authorities. That said, the decision itself was based largely on process concerns—namely, the EU Commission did not conduct a thorough analysis of U.S. national security standards at the time of the original Safe Harbor agreement and that the agreement attempted to unduly restrict Member State enforcement duties. The decision did not address the actual substantive commercial data protection rules, which are the focus of Safe Harbor.

[2] Argentina, Canada, Israel, New Zealand and the United States (for Safe Harbor); see "Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries," available at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

Impact of the Safe Harbor Decision

The decision had a very real and very immediate impact across the Chamber's entire membership. First, more than 4,400 companies, each of which apply Safe Harbor rules on a routine basis, were faced with immediate uncertainty about whether they could continue transferring personal data from Europe, as absent Safe Harbor the Court indicated such transfers are prohibited. They are now faced with the tough choice of deciding whether to continue their transatlantic business or face the potential for expensive enforcement actions, all while providing the same high level of data protection.

As an initial response to the uncertainty, the EU Commission suggested companies switch to other mechanisms to ensure the protection of personal data, such as binding corporate rules (BCR) or model contract clauses. Both mechanisms have limitations, and in any event the idea fails to take into account the realities of the complex technical systems needed to ensure strong privacy protections.

While companies in the Safe Harbor program continue to ensure a high level of data protection for the users of their products and services, developing compliance mechanisms other than Safe Harbor cannot happen overnight. Data privacy systems are legally and technically intricate and are often developed in connection with security protocols to keep data safe and bad actors away.

One supposedly simple solution that many in the EU Commission and the European Parliament have pointed to—BCRs—can cost more than $1 million and take 18 months to fully implement, from development to approval, and they are limited to governing how personal data is used within a corporation. The process is so complex that only about 70 companies are currently certified.[3] Even if Data Protection Authorities across Europe increased their approval process rate tenfold, such a Herculean effort could not swiftly address the challenge confronting the 4,400 companies left in limbo. Worse, German Data Protection Authorities have announced a temporary halt to approving new BCRs pending clarification of the ECJ's decision.

Another alternative, model contract clauses, might require a reexamination of tens of thousands of transfers. Model contract clauses are neither comprehensive nor flexible: They are largely impractical for when data is received directly from hundreds of customers.

More fundamentally, because the ECJ judgement is based on the right to privacy in the European Charter of Fundamental Rights, it is unclear that *any* of these mechanisms can work so long as the Court's rational for rejecting Safe Harbor stems from its finding that U.S. authorities have excessive and indiscriminate access to personal data held by companies. Further, the implications of such a finding reach far beyond the United States as many—indeed most—countries lack the political and judicial oversight our law enforcement and intelligence services face, and as such transfers of personal data to those countries should be prohibited. In this context, it is critical to note that the ECJ did not conduct any formal investigation in current U.S. surveillance oversight rules.

[3] See "List of companies for which the EU BCR cooperation procedure is closed," available at http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.

Importantly, the decision is felt not just in the United States or with Safe Harbor companies, but in the European Union as well because some services may no longer be offered to European users. Indeed, there may be instances in which U.S.-based companies choose to discontinue using EU-based third-party service vendors, particularly in smaller EU markets. The impact will undoubtedly be felt hardest by small and medium-sized enterprises (SMEs) that cannot afford large legal teams to conduct the thousands of reviews necessary.

Even in cases where a large multinational company seemingly has ample resources, there are often relationships with hundreds of sub-processors, typically SMEs. For example, consider the example of a large U.S.-headquartered hospitality company operating hotels in every EU Member State, often managing multiple properties in each. Each of those hotels in turn works with numerous small companies processing data, covering everything from operating customer rewards programs to in-house restaurant service and food supply. That means there are hundreds of arrangements across hundreds of properties that need to be reviewed and potentially changed. In situations like this, the multinational company may decide it is much easier to perform those services in-house, rather than be exposed to potential risk by continuing to work with those EU-based small businesses.

Another example we have heard from member companies is a large agricultural company that uses a personal expense vouchering system managed by a third-party platform on a global basis. After an initial analysis, company executives realized they might need now to negotiate data protection contracts with that processor for each of the firm's 60 legal entities in Europe. However, in the absence of guidance as to whether even these contracts might meet EU requirements, they have been unable to act.

The auto industry uses Safe Harbor to identify vehicle safety issues and for quality and development purposes. However, the industry now faces issues meeting both U.S. and EU regulatory requirements. Under U.S. law, auto manufacturers must share vehicle identification numbers of cars sold globally in the event of a vehicle service campaign, including recalls. This U.S. obligation, given the invalidation of the self-certification provisions of the Safe Harbor framework, may now conflict with EU privacy rules, creating a conundrum for automakers. This is just one example of the significant impacts that the recent ECJ Ruling will have on automakers' fundamental operations.

U.S. and European Government Responses

The Chamber greatly appreciates the efforts of the Department of Commerce to provide clarity and reach an agreement on a revised Safe Harbor. We recognize that Secretary Pritzker and her colleagues in the FTC have been working very hard to address concerns raised by the ECJ decision. The groundwork to a revised Safe Harbor has already been laid by conversations over the past few years.

Surprisingly, the ECJ decision did not examine recent changes to U.S. oversight of electronic surveillance, which certainly are relevant to the criteria the ECJ believes must be met to be considered "essentially equivalent" to the safeguards that exist in the EU. The Chamber is confident that the recently announced Umbrella Agreement and the swift passage of the Judicial

Redress Act, combined with other safeguards instituted since 2013,[4] provide a level of protection equivalent to or even greater than that found in the European Union and among its Member States.

We are encouraged by recent statements by Secretary Pritzker and EU Commissioner for Justice, Consumers and Gender Equality Věra Jourová indicating that an agreement on a revised Safe Harbor has been reached in principle. The Chamber remains hopeful that these efforts will result in needed guidance within the January 2016 timeline laid down by the European Union. However, the desire to provide clarity has not been universal.

Long-Term Impact

While it is critical that our governments continue to work expeditiously to announce a revised Safe Harbor agreement, we also want to sound a note of caution that even a renewed agreement will not serve as a panacea to all uncertainty for transatlantic business, or indeed all businesses in the European Union.

The ECJ decision affirmed the need for individual Member State Data Protection Authorities to conduct independent investigations into all complaints. Moreover the decision indicated the Commission cannot limit this through findings of "adequacy" in programs such as Safe Harbor. This means that companies may be faced with 28 different enforcement and compliance regimes, and potentially 40 if we include the German state-level data protection authorities.

In fact, Hamburg's Data Protection Officer indicated that the only way to avoid future investigations is to localize data, stating "[a]nyone who wants to remain untouched by the legal and political implications of the judgment, should in the future consider storing personal data only on servers within the European Union." [5]

This uncertainty, coupled with a tendency by some in Europe to use legitimate concerns about data protection as an excuse for protectionist policy, underscores the need to carefully monitor long-term developments in the EU beyond Safe Harbor. For example, a recent resolution by the European Parliament on Safe Harbor specifically called for "greater IT independence.[6]" There is a significant disconnect between the EU's stated goals of spurring innovation and fostering a startup culture and officials' statements about the need for IT independence and calls for localization.

This approach has been frequently rebuked by many in the EU, notably by Andrus Ansip, the EU Commission Vice President in charge of the Digital Single Market, who has pushed back

[4] See, e.g., an analysis of recent changes to U.S. national security practices oversight, including, the Privacy and Civil Liberties Oversight Board issued a nearly 200-page report in July 2014 on possible improvements to surveillance safeguards in the United States. Subsequently, the PCLOB found that "the administration has accepted virtually all recommendations in the… report" https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law/. See also more on why the U.S. currently is equivalent or greater to the EU, see http://datamatters.sidley.com/wp-content/uploads/2015/10/Memo-re-Section-702-10-25-15-Final.pdf.

[5] http://thehill.com/policy/cybersecurity/258341-germany-to-investigate-google-facebook-data-transfers-to-us.

[6] http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2015-1092&language=EN.

against notions that the EU is acting with underlying protectionist intent, explaining that "our doors are open, not closed."

While we are committed to working with our European colleagues in an effort to ensure a balanced and proportionate system of rules, we urge Congress and the United States government to remain vigilant to ensure that the European Union does not hold the United States to a different standard on national security and law enforcement issues, and that it otherwise ensures a level playing field for all actors. And by level playing field, we mean one that serves to boost innovation, rather than tear down or constrain those most widely used products and services.

Conclusion

The United States, the EU and its Member States share common values as strong democracies with an enduring commitment to civil liberties and the rule of law. For this reason, we are befuddled that some in the EU would put such an important economic relationship in jeopardy even as we remain hopeful that pragmatic decision-making and leadership will win the day.

The importance of data flows is too great to allow precipitous changes in policy to undermine them: Recent studies estimate that cutting off data flows between the United States and the EU would cut EU GDP by as much as 1.3%.[7] Given continued slow economic growth in the EU, our closest trading partner, that kind of hit to the EU economy would have significant negative repercussions on this side of the Atlantic as well.

We applaud the House for taking an important first step towards resolving these concerns with the passage of the Judicial Redress Act. We are encouraging the Senate to act swiftly to give this bill final passage.

This week, a group of European Parliamentarians are in town as part of the Transatlantic Leadership Dialogue, presenting our Congress with a perfect opportunity to voice the importance of the Safe Harbor and cross-border data flows, educate them on the oversight Congress exercises over U.S. intelligence and law enforcement agencies, and to ensure they understand the difference between commercial and national security and law enforcement related issues. We encourage you all to seize this opportunity.

Above all, as we have indicated, we urge U.S. and EU officials to move swiftly to put in place a revised Safe Harbor that addresses the concerns that have been raised.

The Chamber greatly appreciates the opportunity to provide these comments to the committee. We stand ready to assist in any way possible to ensure data flows can continue across the Atlantic.

[7] The Economic Importance of Getting Data Protection Right; https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf