MAY 2016

BRIDGING PERSPECTIVES:
Data Protection, Privacy, and Security In The U.S. & Germany

Capstone Team:
Erica Cottingham, Meghan DeAmaral, Colin Gary, Lisa Harst,
Gabriel Murgas, Jingyi Xiang, and Yilan Zhou

George Bush School of Government & Public Service
Texas A&M University

Advisor: Dr. Mary Hilderbrand
Client: Computer Sciences Corporation (CSC), Public Sector-Europe

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In 2000, the US and the EU signed the Safe Harbor agreement that allowed US companies to move EU citizens' personal data as long as they self-certified compliance with EU standards. For fifteen years the Safe Harbor agreement served as the framework to allow the transfer of private data from the EU to the US. In October 2015, the Safe Harbor framework was invalidated by the European Court of Justice, leading to confusion on both sides of the Atlantic on how private data should be handled. Safe Harbor's potential successor, the newly negotiated Privacy Shield, adds extra layers of protection for EU citizens, including judicial redress in US courts and an ombudsman mechanism, but still faces further discussion.

The Safe Harbor dispute brought to the forefront differing perspectives on data protection and privacy. While the US prioritizes security due to the attacks of 9/11, Germany's history of government spying on its own citizens led the country to value privacy as a basic human right. Differing perspectives on data protection and privacy between the US and Germany resulted in distrust, impacting both economic and political interests.

This project, requested by CSC-Public Sector Europe, seeks to gain a better understanding of US and German data privacy perspectives and identify steps to improve future cooperation. The research consisted of two phases: secondary research and semi-structured interviews with stakeholders from different sectors.

During the interview process, the researchers identified and contacted 40 stakeholders from government agencies, private sector and academia in both the US and Germany. In all, 13 interviews were conducted. From the research and interviews conducted, the team reached the following conclusions:

1) There are differences, but each country maintains a disposition open to negotiation.
2) There are areas of mutual agreement.
3) The current state of Privacy Shield is not agreeable to all entities.
4) Perspectives on privacy mold each country's policies and protocols.
5) Media plays a significant role in shaping the narrative of the data privacy dispute in Germany and the US.

These conclusions then led to three recommendations aimed at cultivating trust between the US and Germany:

1) Reshape the narrative on data protection through media engagement.
2) Expand and strengthen people-to-people relationships.
3) Foster a multi-stakeholder partnership culture.

INTRODUCTION

Different approaches to data privacy between the United States, on one hand, and the European Union (EU) and its member countries, on the other, complicate the transfer of private information and strain transatlantic commerce and diplomatic relations. Efforts to bridge the gap resulted in 2000 in the US-EU Safe Harbor Framework, allowing US companies to transfer data by self-certifying compliance with stricter EU privacy laws. For fifteen years, the Safe Harbor agreement provided businesses a low-cost and legal way to move private data across the Atlantic.

The effectiveness of the Safe Harbor agreement was tested in 2012 when a privacy activist, Maximillian Schrems, filed a complaint with the Irish Court that Facebook was abusing user data. Then in 2013, former US government contractor Edward Snowden exposed the US National Security Agency's (NSA) massive surveillance programs. The events that unfolded in the wake of Schrems and Snowden drove a wedge into the trust between the US and the EU. The Safe Harbor agreement was a casualty of these events: in October 2015, the European Court of Justice (ECJ) declared Safe Harbor invalid. The ECJ ruling left both government agencies and international firms with uncertainties about transatlantic interactions and once again brought into light the US and EU's different approaches to protecting private data.

The dispute over data privacy has been especially significant for relations between the US and Germany. As allies and major trading partners, the two countries have a warm relationship overall. But disagreements over the linked issues of data privacy, security, and surveillance have been a source of tension over the past several years and continue to be. The data protection dispute has contributed to souring of negotiations over trade pacts and other agreements. Therefore, gaining a better understanding of the perspectives of the two countries regarding data protection and identifying steps that can be taken to improve understanding between the two on this issue is important. That is the purpose of this study and report.

I. ABOUT THE PROJECT

Purpose

This study has been conducted for our client, the Public Sector-Europe office of CSC, a US-based IT services company. Reflecting concerns among a transatlantic community of IT and government professionals over the current tensions in the relationship over data protection, the client requested research that might improve understanding and dialogue between the US and Germany. Coming out of further discussion with the client, we chose to focus on the Safe Harbor agreement as a touchstone for understanding the US and German approaches to and perspectives on data protection.

In this study, we analyze US and German perspectives on data privacy, in order to better understand each of them and to use that understanding as the basis for recommending steps that

can help bridge the differences in the discourse and in the relationship between the two countries over data privacy.

Data Collection

The project's data collection process consisted primarily of two parts: 1) research using secondary sources, documents, news reports and other published sources; and 2) semi-structured interviews.

During the first phase of the research, the team assessed the history, data privacy laws and regulations of the US, EU, and Germany; reviewed previous academic and professional literature on data privacy and security; and followed the latest information in the wake of Safe Harbor's invalidation, including the negotiations on Safe Harbor's replacement, the Privacy Shield. This research provided the basis for the details of the Safe Harbor case study and for the different legal frameworks and regulatory approaches in the two countries.

The second phase involved interviewing individuals from key stakeholder groups as identified in our stakeholder analysis in Appendix A from both countries, including US and German government officials, private sector executives, and academic experts. These were for the purpose of getting perspectives on the Safe Harbor situation and insights from the interviewees' experience and knowledge of the issues. Of forty potential interviewees contacted, thirteen agreed to be interviewed. Interviews were about one hour in length. The interview protocol is included in Appendix B.

Data collection was limited in large part by the significant number of officials who declined to be interviewed. While many gave their reasons for declining as not having time, others refused based on the sensitivity of the topic given their position or involvement in it. As a result, findings were based on a limited number of interviews and thus a small sample size; the views expressed by those we interviewed may not be representative in general or of the views of others in specific stakeholder groups. While the interviews we did conduct covered relatively well the range of groups we intended to cover, it is necessary to be cautious in drawing conclusions from the findings of the interviews because of the small number interviewed.

In accordance with human subjects research guidelines and also due to the sensitive nature of data privacy-related subject matter, interviewees are not identified in the report.

The conclusions and recommendations are based on the overall research, including both the secondary research and the interviews.

II. THE SAFE HARBOR DISPUTE

This section discusses the evolution of Safe Harbor, its invalidation, and the negotiations for a replacement.

Necessity for the Safe Harbor Agreement

EU laws and policies are far more comprehensive, and in some ways, significantly stricter than similar policies in the US. The EU's Data Protection Directive (Directive 95/46/EC) specifies that "personal data can only be transferred to countries outside the EU and the European Economic Area (EEA) when an adequate level of protection is guaranteed" (European Commission 2015). For US organizations whose activities rely upon transatlantic data transfers, meeting this standard may imply extra compliance costs.

As a result, the US Department of Commerce (DoC) developed the Safe Harbor Framework in consultation with the European Commission, enabling US companies to cost-effectively satisfy the EU's standard (export.gov 2013). Under the agreement, US companies could voluntarily join a cohort of companies eligible to engage in US-EU data exchange by self-certifying—through a number of predetermined criteria and steps for which they were accountable— that EU citizens' personal data was adequately protected.

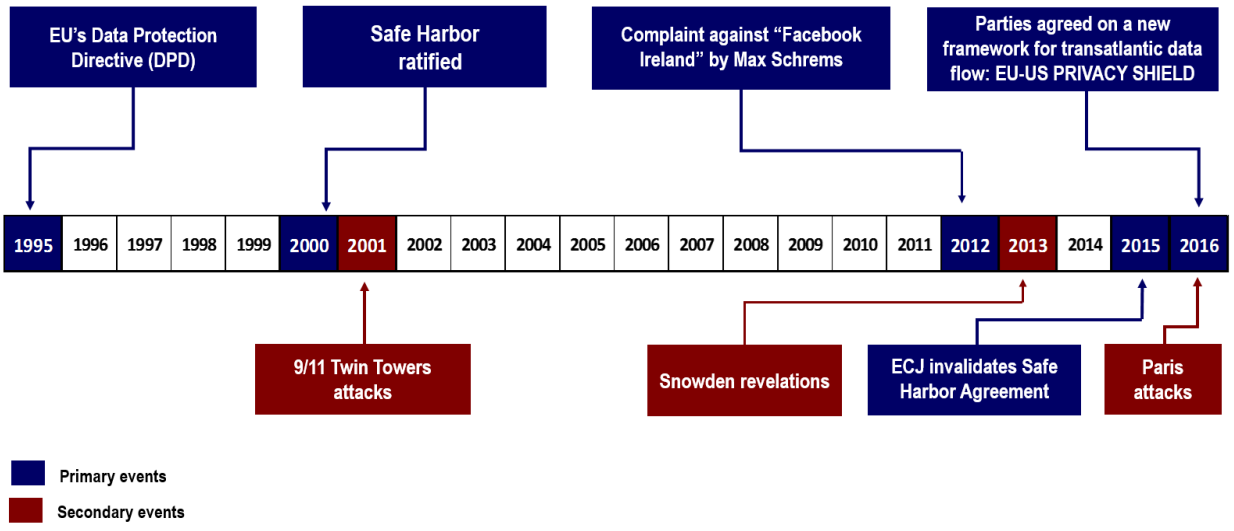

**Figure 1*- Timeline of Significant Milestones Affecting Data Protection Regulations

Problems with Safe Harbor

In 2012, Maximillian Schrems was the first to identify loopholes in Safe Harbor's framework (Hill 2012). As a privacy activist, Schrems complained to the Irish Data Protection Commissioner that Facebook was abusing user data, which Facebook claimed as intellectual property. The complaint was initially rejected.

In 2013, Edward Snowden, a former NSA contractor, leaked classified documents of the NSA's mass surveillance programs (EU Center of North Carolina n.d. 1). In essence, the documents revealed that US laws permitted the NSA greater authority to examine communications from non-US citizens than from Americans. The NSA's controversial program PRISM allegedly allowed agents to collect data held by US companies (Goldfarb 2015, 211). Snowden further drove a wedge into US-EU relations when he revealed that the NSA bugged German Chancellor Angela Merkel's phone. The revelation dealt "a significant blow to transatlantic unity" (EU Center of North Carolina n.d. 5). Some Germans called for subsequent increased regulation and others demanded disassociation of German and US relations entirely (Hall 2014, 4).

Safe Harbor Declared Invalid

The Schrems case soon resurfaced. In 2015, Schrems applied to have the case subject to judicial review in the Irish High Court, whose justice referred the questions to the ECJ for preliminary ruling (EPIC n.d.). Ultimately, Safe Harbor was invalidated by the ECJ on October 6, 2015. The ECJ cited in its decision several loopholes found in the US' regulatory structure. To start, US intelligence agencies and public authorities were able to access EU citizens' personal data and "process it in a way incompatible...with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security" (ECJ 2015). Moreover, the court found that European citizens could not seek redress if they suspected that their personal data was being mishandled by the US. The European Commission expressed concern that Safe Harbor lacked secure data protections, did not ensure transparency, and did not offer mechanisms for EU citizens to enforce their privacy rights against the US government and US companies (Ash, Mann, & Sloan 2016, 1).

Privacy Shield Negotiations

Both the EU and US have recognized the importance of secure data transfers in transatlantic commerce and share a mutual interest in developing a successful framework. Thus, in early 2016, the US and EU negotiated a new data protection framework: *Privacy Shield*. Under this agreement, US companies wishing to receive EU data will be required to commit to more stringent obligations regarding the process of obtaining, storing, and using citizens' personal data.

New elements of the Privacy Shield include an independent ombudsman, the Judicial Redress Act, and added oversight protections. The US ombudsman is tasked with reviewing all EU citizen complaints, while the Department of Commerce is responsible for monitoring corporate obligations to publish data protection commitments (Glazer 2016, 2). Signed into law in February 2016, the Judicial Redress Act extends to EU citizens the right to redress violations of privacy in the US. Hence, Privacy Shield introduces new contractual privacy protections and "oversight for data transferred by participating companies to third parties or processed by those companies' agents to improve accountability and ensure a continuity of protection" (Jones Day 2016).

Implementation of the Privacy Shield arrangement will be subject to annual joint reviews by the European Commission. The US Department of Commerce, national intelligence experts, and European Data Protection Authorities will also be invited to participate in the annual reviews (US DoC 2016). However, on 13 April 2016, EU data protection regulators (in the form of the Article 29 Working Party), announced that it "has strong concerns on both the commercial aspects and the access by public authorities to data transferred under the Privacy Shield." (WP29, 2016). Thus, the approval and implementation of Privacy Shield -- currently pending June 2016 -- remains in question.

Governmental departments that negotiated the EU-US Privacy Shield provide a clue as to how both sides understand the Safe Harbor agreement and insight as to why there might be disputes over the nature of data transfer. The presence of the Federal Trade Commission and the Commerce Department as principal negotiators for the US[1] indicate America's view of data transfer as more of a business matter than one of privacy rights. Meanwhile, the UK Information Commissioner - a role for which there is no clear equivalent in the United States - is one of the key European individuals handling negotiations (Tomaszewski 2016, 1). "Information" and "justice" in the names of the European department representatives negotiating for a new agreement frame the discussion as an issue of privacy rights. Different conceptualizations of the problem have not only led to misunderstandings on how to proceed with a new agreement but may also result in future discordance once the Privacy Shield is fully implemented.

III. REGULATORY ENVIRONMENT

Differing Perspectives

Different regulatory environments of the US and Germany are a reflection of national priorities and historical influence. The US considers privacy primarily a consumer protection issue and adopts a piecemeal approach to regulate the collection of personal information. On the other hand, Germany--like the EU--views privacy as a fundamental human right and has thus established an umbrella structure protecting private data.

Core disputes surrounding Safe Harbor reflect the two governments' contrary attitudes regarding data privacy. Germany's perspectives are in line with those of the EU Generally, the EU is skeptical of US willingness to minimize the interference of American public authorities with European citizens' personal data. Self-regulation -- as established in Safe Harbor -- allowed American companies to facilitate the transfer of data as efficiently as possible with little oversight from the EU, which Europeans viewed as being in the best interest of US corporations rather than EU private citizens. Most recently, Europe's impression of the US approach has been adversely impacted by calls from US officials to arm intelligence agencies with encryption keys in order to

[1] US Secretary of Commerce Penny Pritzker was involved in Safe Harbor 2.0 negotiations and was joined by Edith Ramirez, US Chairwoman of the Federal Trade Commission (FTC) (Pearce 2016, 2; Tomaszewski 2016, 1)

enable agents to retrieve information at will (Ullman 2016, 2). These encryption keys, if permitted, would provide the US government with a "back door" to conduct surveillance on individuals.

US: Privacy & Terrorism

The US has historically acknowledged freedom and the idea of basic human rights. In the US, the Bill of Rights covers several aspects of privacy, most notably through the Fourth Amendment that protects citizens from unreasonable search and seizure (Linder 2015). The First Amendment also holds that "Congress shall make no law…abridging the freedom of speech, or of the press." It directly addresses Congress but actually applies to the government in its entirety—meaning federal, state, and local; and legislative, executive, or judicial (Stone and Volokh 2015). In today's context, the legal interpretation extends further than just the interaction between the speaker and the press.

In the early stages of the computer age, the Privacy Act of 1974 came into effect. This policy directs agencies to implement consistent "fair information practices" in the handling of private data and allows American citizens to sue the government if they feel their private data has been used in violation of the law (EPIC 2016). In addition, a handful of privacy-related sectoral laws, including the Health Insurance Portability and Accountability Act (HIPAA) and Electronic Communications Privacy Act (ECPA), also place restrictions on how sensitive personal information is gathered and used under specific categories (Jolly 2015). However, this array of policies designed to ensure data privacy and the protection of private citizens contributes to a piecemeal approach to the task. There is no single, central umbrella for privacy regulation.

The attacks of 9/11 struck the country with fear and a firm resolve to combat terrorism -- even at the cost of private citizens' personal information. As a result, the US commenced controversial surveillance activities and shifted institutional infrastructure to ensure a similar attack would never happen again. Congress passed the Patriot Act, and under the leadership of President George W. Bush, the Department of Homeland Security was created (Kurra 2011). US national security has since become a top-level policy priority, engendering further collection and utilization of personal data. The USA Patriot Act was also signed into effect shortly after 9/11 and partially renewed in June 2015. This legislation granted the government authority to monitor individual citizens and collect private information (Berkman Center, n.d.).

Following Snowden's revelations, many US officials and citizens were upset that the intelligence community collected data on US citizens, leading to the passage of the USA Freedom Act in 2015 that "limits the NSA's ability to collect domestic metadata and increases transparency and accountability in the Foreign Intelligence Surveillance Court (FISC)" (Sykes and Hansel 2015 para. 3). This act reduces the extent of the Patriot Act by protecting citizen privacy rights, but still allows foreign surveillance and "preserve[s] the government's capability to retrieve the metadata of communications by suspected terrorists" (Center for National Security Studies n.d.).

Germany: Right to Privacy Embedded in History

Germany has a history of surveillance by a repressive state, dating back to the Nazi regime but most recently by the Communist state of East Germany (Hall 2014, 4). Intelligence systems operated by the Gestapo under Nazi rule and, later, the extensive files collected on both East Germans and West German citizens by the Stasi affect the way Germans value privacy today. The Stasi are said to have "roped in an estimated 190,000 part-time secret informants and employed an additional 90,000 officers full time [to gather personal information] — in total, more than one in every 50 adult East Germans as of 1990" (Birnbaum 2013).

The first data protection law in the world, the Hesse Act, was passed in the state of Hesse in West Germany in 1970; it expresses common regulative philosophy in Germany and sets basic themes for subsequent German and European legislation (Burkert n.d.). But, in response to a clear need for more stringent protection of private citizens' data, the Federal Data Protection Act (*Bundesdatenschutzgesetz*) (BDSG) was passed in 1990 to serve as a primary legal source of privacy protection in Germany. The BDSG aims to shield personal data from unauthorized processing and use by public authorities and private bodies (Jansen & Hinzpeter 2015). Moreover, the Telemedia Act and the Telecommunications Act also apply to respective sectors of electronic service providers.

The Federal and State Data Protection Commissioners are responsible for guaranteeing independence through this process. For that reason they are usually elected by their relevant parliaments and "are not subject to directions from political organs; their offices and personnel are separate from administration" (Korff 2014, 48). The Federal Commissioner has wide power to investigate and enforce the compliance of the Federal Protection Act. For example, the Act establishes that any supervisory authority has the right to "demand of a private-sector controller, without cause, any information which supervisory authority needs for the fulfilment of its tasks" (Korff 2014, 52). However, this process must comply also with legal requirements to ensure safety, security, and confidentiality. At the State level, the State Data Protection Authorities also have that responsibility. In 2011, the German Data Protection Authority (DPA) released guidelines and instructions to users and businesses to ensure legal compliance.

In addition, Germany respects the right of "informational self-determination", a decision made by the Federal Constitutional Court (*Bundesverfassungsgericht*) in 1984 that annulled the federal government's planned general population census due to its invasion of privacy (Hornung & Schnabel 2009). The result was a stricter interpretation of data protection in Germany than in most other EU member states.

Data protection in Germany also falls under the purview of the EU. At the EU level, the Data Protection Directive sets up a comprehensive regulatory framework that "seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the EU" (EUR-Lex n.d.). These legislations fostered an environment where data collection and use is prohibited unless permitted by law or consented to by the subject (Library of Congress 2015).

Public Opinion in the US and Germany

Studies have found that privacy is a concern both in the US and Germany. A Pew Research Center survey found that in the US only 6% of the adults feel confident that government agencies can keep their records private and secure, and 9% think they have control over how much of their information is collected in daily life (Madden & Rainie, 2015). In Germany, the Symantec State of Privacy Report (2015) indicates that 62% of Germans are worried their personal information is not safe, and 30% believe that the government can keep the data completely secure. In sum, although laws and regulations potentially set a safety net for personal data, privacy remains a concern among the public.

The Snowden revelations act as a major factor that raised people's concern. German public opinion shifted as "six out of 10 Germans consider Edward Snowden, the man responsible for opening the rift between their country and the United States, a hero. Only 14 percent believe Snowden is a criminal" (Francis 2015 para. 3). Still, in a 2015 poll conducted by the Pew Research Center, over half of all Germans and Americans surveyed viewed the other as a reliable ally. Americans, however, viewed Germans more favorably by a margin of 10 percent, and 31 percent of Germans viewed the US as an "unreliable ally" (Pew Research 2015).

IV. THE INTERVIEWS

The team interviewed a total of thirteen individuals from nine different organizations and occupations, four from Germany and five from the US. Individuals were contacted on the basis of involvement in or knowledge of data protection and privacy issues from different sectors, such as officials of government agencies, representatives of private companies, and persons in academia. Interviews with these stakeholders, although limited in number, offered the team a range of experience and opinions on the research topic, allowing us to gain insight into US and German data privacy perspectives.

Three out of the seven US interviewees were top-tier government officials with extensive knowledge on this topic. They were directly involved in Safe Harbor-related issues, either through negotiations and discussions at the diplomatic level or through policymaking. Two other interviewees were a professor with extensive knowledge of German history and a private manufacturer that conducts high volumes of transatlantic business, from which Germany is one of its largest buyers. While none of the non-government officials possessed in-depth knowledge about the Safe Harbor agreement, they had been involved in US-German information exchange.

One German interviewee was a parliamentary member directly involved in data protection regulations both at the EU level and national level in Germany. In addition, the team spoke with two stakeholders from private companies engaged in data transfer across the Atlantic. Their respective levels of understanding regarding Safe Harbor provisions varied based on work responsibility, but both maintained enough knowledge to engage in conversation about the topic. Another German interviewee was a scholar who worked for a research organization that uses cloud services and storage systems provided by US technology companies.

Findings

The following section summarizes major findings from the research.

1. Efficacy of Safe Harbor

US and German stakeholders have contrasting views as to the efficacy of Safe Harbor in regards to providing adequate data protection. While the US stakeholders tend to look more so at the economic benefits brought by transatlantic data flow, Germans focus more on how their personal data is handled.

Interviews with US officials revealed that the majority felt the Safe Harbor agreement was sufficient to protect European citizens' personal data and is crucial for transatlantic trade activities in a digitized economy. US government officials viewed the ECJ's decision to invalidate the framework as a lack of understanding of how personal data is collected and handled by US government agencies. One interviewee pointed out that the US and EU have different forms of governance, therefore will "never have the same system for data protection." Some officials cited that Snowden's revelations only exacerbated the misinformation problem and had long-lasting impacts on how the German public perceives US government and data collection activities.

On the other hand, German interviewees considered the Safe Harbor agreement to be both ineffective and inadequate. One German official specifically emphasized the lack of legal protection, not only in Safe Harbor but also in the US Constitution, for EU citizens to seek redress in US courts against the activities and alleged abuse of US government and law enforcement agencies. Employees of German private firms also questioned whether companies joined under the self-certification mechanism truly meet the data protection standard maintained in the EU. A private sector manager in Germany stated to the team that Safe Harbor was largely an agreement that worked on paper for lawyers only.

2. Privacy Shield and provisions to be included in future negotiations

When asked about the newly negotiated Privacy Shield, stakeholders from the US and Germany again revealed differing views. In general, US officials believe this new agreement is sufficient and fulfills the EU's requirement while Germans still see no significant improvements in Privacy Shield.

Awareness of the Privacy Shield agreement was limited. Knowledge of its provisions was almost entirely confined to high-level policy makers, lawyers, and legal experts, which was a point of contention. Though the stakeholders interviewed were are significantly involved with transatlantic data issues, their understanding of Safe Harbor, Privacy Shield, and data privacy law varied. As one German government official interviewee observed, Privacy Shield works on paper at the legal level, but "real changes" will not occur at the lower levels of industry. All three US government officials asserted that Privacy Shield was adequate, especially for economic reasons,

as it fosters trust between countries. Moreover, the officials concluded that Privacy Shield is "more than sufficient" to meet the EU data protection standard.

Conversely, German interviewees expressed that Privacy Shield offered insufficient protection and the data protection policy making process is failing to keep up with the pace of technology development. Most stated that new provisions should include increased scrutiny to determine reasons and motivations for collection of personal data. One German Member of Parliament (MP) held the opinion that Privacy Shield was insufficient, even given the newly-added ombudsman mechanism. The German MP added that, unless amended to grant EU citizen's legal access to redress in US courts, Privacy Shield will likely face a fate similar to that of Safe Harbor. Other German interviewees concluded that Privacy Shield will not make a substantial difference and will fail to change data privacy behaviors.

3. Interviewees' perspectives on US-German disagreement

Interviews with US and German stakeholders exposed some similarities and some contrasting ideas regarding the main points of disagreement between the US and Germany. While most interviewees from both the US and Germany suggested that Germany's history was a primary source of tension, there was nearly no mention from either side regarding the purpose of US data collection programs following the attacks of 9/11.

One German interviewee reflected on the effects of East German history and how it still shapes German privacy perspectives today. Another German interviewee stated that the EU views on privacy resulted from laws under which privacy is the most protected human right. Similarly, US interviewees noted that the EU thinks of privacy as a human right and in the US it is seen at the commercial level. US officials pointed out that Germans were far more suspicious of government intervention into the lives of private citizens. These different understandings contributed to the repeal of the Safe Harbor agreement.

US interviewees highlighted the impact of Snowden revelations and stated that the leaks "created anti-American sentiment, damaged trust, and caused Germans to question US intentions," which made it even harder for German citizens to trust the US. One German interviewee pointed out that while the German public is aware of (and against) the NSA's data collection programs, it is still relatively active in data-sharing activities. Similarly, one US government official observed that while US citizens are willing to freely post personal information on social websites, they are unwilling to provide information to their own government. The former behavior could compromise their security, while the latter could in fact increase personal and national security. Likewise, a German interviewee said that if you ask a German citizen their opinion on privacy matters, they say they are sensitive, but if you look at their practices, they use a lot of data. Thus, although the public in both countries expresses a desire to increase protections for its personal data, individuals generally do not take the easily-accessible measures to protect themselves.

4. General recommendations from interviewees to both countries

At the conclusion of the interviews, team members asked interviewees for any further thoughts on US-German data privacy perspectives or related topics. Though the majority of US interviewees were government officials, these stakeholders tended to relay opinions based on economic or business perspectives. In terms of behavioral change, a US interviewee from the private sector posited that EU citizens need to be more willing to provide basic information, otherwise conducting business in Germany might become economically and fiscally inefficient.

Most comments from each set of interviewees involved attempts to understand each side's views and practices on data protection. For example, a US government official talked about his hope that the EU might understand that they can be partners with the US, and that with the right policies on both sides of the Atlantic, digital economies can continue to grow. On the other hand, one US government official said that the US must invest time and resources in explaining their laws on data privacy, as well as enhance diplomatic engagement to foster stronger relations in the post-Cold War era. As one US interviewee stated, the media has a large effect on the public, and pointed to misinformation as a main contributor to the contention between the US and Germany.

German interviewees focused on suggestions that the US look to current data protection frameworks in Europe as a model to implement at home. One of the German interviewees mentioned setting up uniform rules to speak on behalf of the 28 members of the EU on data issues. This has already been adopted and will go into effect in 2018. They also suggested setting up a neutral commission, perhaps in the UN, to listen to ideas from both sides and recommend approaches for future action. Another German interviewee stated that they thought it was a good public relations move for an American company to let a German data company keep custody of data on German citizens. These preceding interviewee recommendations reflect sentiment from several German interviewees to set up some sort of neutral entity to oversee issues of data privacy and data transfer.

V. ANALYSIS AND CONCLUSIONS

1. There are differences, but each country maintains a disposition open to negotiation. The disparity between US-German policies and perspectives may not be as wide as once thought, although a *perception* that there are significant differences may prove an obstacle to collaboration. Many German interviewees and some American interviewees believe the differences are not that great, while a few US interviewees still believe there is still a lot of distrust that hinders the success of a new agreement.

2. There are areas of mutual agreement. There is a willingness to work together on intelligence/security in light of recent European terrorist attacks. The two countries have a history of cooperation. Interviewees from both countries recognize the importance of cooperatively gathering intelligence, especially in light of increased incidents of transnational terrorism. Additionally, the digital economy of both countries stands to

benefit from more integrated data transfer policies by ensuring that thousands of businesses and millions of individuals can continue to access services online.

3. The current state of Privacy Shield is not agreeable to all entities. There was almost universal agreement of US interviewees that Privacy Shield is adequate and will withstand judicial scrutiny. Conversely, German interviewees viewed the agreement as inadequate and destined to meet strong objection from the ECJ.

4. Perspectives on privacy mold each country's policies and protocols. US interviewees viewed data transfer as an economic/public relations matter, while German interviewees viewed it as an issue of protection of privacy. German citizens' history of dealing with invasion of privacy under Communist rule in East Germany and under the Nazi regime have led modern citizens to be more sensitive to issues of personal privacy, whereas the US interviewees did not have similar histories affecting their perspectives.

5. Media plays a significant role in shaping the narrative of the data privacy dispute in Germany and the US. Several US interviewees pointed out the negative effect on German citizens' public opinions by German media, which contributed to an unfavorable context for the transatlantic data negotiations. Interestingly, German interviewees expressed no hesitance in absorbing the information provided by the media but expressed obvious concern and distrust in information communicated by the government.

VI. BRIDGING THE DIFFERENCES

Putting Safe Harbor in Context

Safe Harbor and Privacy Shield represent larger transcending issues of cultural differences and data privacy perspectives between the United States and Germany. Individual cases such as Max Schrems or Edward Snowden only catalyzed the discussion of data protection and security and emphasized existing disparities. Though the actual magnitude of variation between the US and Germany is contested, differences in culture are certainly at the core of the dispute. To begin bridging the gap in data privacy perspectives, it is critical to first determine at exactly what level differences occur and identify short-term steps to achieve long-term results.

Fundamentally, the US-German relationship has long been a strategic alliance. The two remain close allies engaged on many levels, including diplomacy, security, and various economic treaties and agreements. The US and Germany developed different governing systems over time, and major events such as 9/11 and Germans' experiences with repressive states shaped their policies. Both countries are fervently committed to preventing similar events in the future. The US and Germany will never have the same approaches to privacy; consequently, there is no single "right way." Mechanisms can be used to increase understanding and help construct viable compromises in the future.

Identifying the Next Steps

Bridging differences is not a government-to-government issue but rather about engaging the public to build consensus and understanding. Misinformation and disinformation rapidly spread among the German public after the Snowden revelations. Though US-German relations have since improved, a slight disparity between the US and German public still remains. Traditional bilateral diplomacy cannot address the full range of actors now engaged on these issues; therefore, public diplomacy efforts to combat misinformation and improve the public sentiment should begin through increased and diversified engagement. Efforts and resources should be provided by both the US and German governments. US and German governments can move towards bridging their differences beginning with three steps:

1) Reshape the narrative on data protection through media engagement;

2) Expand and strengthen people-to-people relationships;

3) Foster a multi-stakeholder partnership culture.

If these measures are adopted in the short-term, long-term benefits -- such as increased understanding of the other country's perspective -- are likely to be realized. Other benefits to follow include more trust between the two countries and increased engagement at the diplomatic and cultural levels beyond that of data protection.

STEP 1: Utilize media engagement to reshape the narrative.

- *Establish a media personnel exchange program.*
  Increasing the exchange of journalists between the US and Germany allows for journalists to travel to the other country and facilitates more direct face-to-face interaction. Additionally, increasing the number of prominent US experts and senior leadership who engage with German opinion leaders and media on cultural differences will allow each side to hear the other's perspectives.

- *Expand other platforms for information exchange.*
  Expanding the traditional and innovative information platforms to develop targeted media engagement will shape global dialogue. Utilize new media sources to ensure US and German perspectives are heard in cyberspace so as to provide a counterpoint to public misinformation and allow each side to gain accurate, first-hand. This can be done through social media accounts, country-specific websites, and multimedia interactive products. As one German interviewee remarked, most people in the US do not understand German laws on data privacy, which can be frustrating when negotiating topics related to information exchange. Such efforts will lead the way in plans to strengthen ability to shape the narrative and proactively present the respective views of the US and German public. Information

provided on the websites could then be used by Public Affairs officers to quickly counter false claims in the media.

ACTION	WHO?	HOW?	POSSIBLE BARRIERS
Utilize media engagement to reshape the narrative. - Establish a media personnel exchange program - Expand other platforms for information exchange	US and German government agencies and media outlets	Traditional and non-traditional media sources	Financial backing; media incentive

**Figure 2*- Matrix of Step 1: Utilize media engagement to reshape the narrative*

STEP 2: Expand and strengthen people-to-people relationships.

- *Identify and maximize shared national interests and priorities.*
  Both the US and EU governments prioritize keeping their respective homelands safe. Germans are worried that the government will sacrifice too much privacy in pursuit of more intelligence. However, because of a spate of recent terrorist attacks tied to information and communication insecurities, sentiment in Germany may increasingly move toward a US model: one of greater emphasis on security. Under this situation, it is important to *Listen first, then attempt to negotiate.* By now, both sides know the talking points of the other and need to move beyond conventional wisdom. This will only be made possible when leaders from all industries begin listening to the opposing viewpoints and concerns, not talking past one another.

  Additionally, US and German stakeholders should expand their mutual understanding in order to maintain strong economic ties. According to the data provided by US Department of State, the US became Germany's leading export market in 2015; this trade relationship is driven by massive mutual investment and opportunities for citizens of both countries.

- *Broaden the demographic base of people with whom discussions are engaged by setting up dialogues pertaining to data privacy within and between each country.*
  Providing opportunities for more discussion will allow citizens from each sides of the Atlantic to familiarize themselves with the issues and increase the salience of the topics. Mechanisms need to be utilized to encourage a wider circle of people -- such as rural, younger, or less affluent persons -- to participate in programs and visit American and German venues. Because the goal of these dialogues is to increase discourse and critical thinking of these issues, these can even include discussions held in the US solely among

American citizens or discussions held in Germany solely among German citizens. Social networking technologies can be utilized more effectively to incorporate senior leadership in informal dialogues or non-traditional forums with these more diverse audiences.

    - It is especially important to note that if US and German youth develop favorable views of each other's countries early on, they grow up to be constructive partners. This can be done by creating platforms on various media channels for dialogue with youth networks within and between each country and engaging seriously with young journalists. As social media makes the world smaller, youth from both countries can speak to each other through video calling hangouts without even leaving their bedrooms.

- *Build mutual trust and respect through expanded Public Diplomacy programs and platforms.*
  People-to-people international exchange programs improve our understanding of different cultures and viewpoints, build language and leadership skills, and enhance economic prosperity and security. For example, expanding on programs such as the German American Partnership Program (GAPP) supports school partnerships and exchanges between high schools in the US and secondary schools in Germany. This program, like many others, allows groups of US high school students and German secondary school students to visit a secondary school in the other country for a minimum of 16 days, allowing them to experience and draw first-hand conclusions about another culture.

- *Reinvigorate cultural programming to drive engagement and collaboration.*
  Launch an initiative to rejuvenate cultural programming that presents American/German art, theater, music, dance, and literature to create a politically-neutral space for building relationships between the publics of both countries while simultaneously fostering creativity.

ACTION	WHO?	HOW?	POSSIBLE BARRIERS
Expand and strengthen people-to-people relationships - Identify and maximize shared national interests and priorities - Broaden the demographic base - Expand Public Diplomacy programs and platforms - Reinvigorate cultural programming	Interest groups, US and German government officials, professionals, and citizens	Implementing new programming and increasing efforts in existing programs	Developing and funding programs

**Figure 3*- Matrix of Step 2: Expand and strengthen people-to-people relationships

STEP 3: Foster a multi-stakeholder partnership culture.

- *Utilize public-private sector partnerships*.
  Since government budget constraints limit the ability to engage beyond traditional elites, private sector partnerships should be utilized to assist with resources and implementation of engagements and exchanges. Offering incentives to entities that contribute to building and sustaining private partnerships and collaborative initiatives is a wise solution to increase mutual understanding between people. Such partnerships are an effective mechanism that would allow both governments to achieve more with less and the private sectors to earn economic benefits while supporting social good.

- *Set up a Joint US-German Dialogue dedicated to fostering greater understanding and providing an additional platform to talk to each other and reach greater consensus.*
  CSC, in combination with think tanks and the private sector in the US and Germany could support a dialogue through seminars, conferences, and working groups that brings together all stakeholders involved for a continuous discussion on data protection and privacy issues. This dialogue has wider discretion to address a broader range of difficult issues for which a government may not want to spend political capital.

  As data privacy issues are made more salient by the dialogue, the onus is on the need to address the issues at the governmental level. In this way, the Joint US-German Dialogue serves as an agenda-setter. It can also act as a conciliator when disagreements arise and facilitator for reaching consensus by finding points of agreement. Additionally, it can serve as a repository of important information that can be used by any country seeking to learn more about data privacy and data transfer. Finally, it can serve as a ready-made forum at a moment's notice for continued conversation to bring those with differing opinions to the table to discuss ongoing issues like privacy, transatlantic data transfer, and the rise of cloud computing.

- *Engage partners early*.
  Early participation of partners ensures that the partnership is structured in a way that fully takes advantage of their capabilities, positions, interests, and strengths. It also allows the government to capitalize on the private partner's regional and sector experience by engaging it in the earliest planning and management phases.

- *Data protection issues affect every country and therefore the dialogue is not limited to Germany/EU and the US.*
  Data protection issues affect everyone. It is important for Germany and the US to remember there are other opportunities for engagement with other countries. There are opportunities to work with others in public, private, and nongovernmental sectors. Lessons learned can be shared. Good ideas can be applied elsewhere. As several German interviewees pointed out, this is not just a German issue, it is a European issue. At a broader level, this is a world issue that affects us all. Since the issue affects everyone, it will take widespread cooperation for sustainable mutually desirable agreements to make in the future.

ACTION	WHO?	HOW?	POSSIBLE BARRIERS
- Foster multi-stakeholder partnerships - Utilize public-private sector partnerships - Create a joint US-German dialogue	Governments, think tanks, and private sector	Creating inner organization programs, NGOs, and third-party efforts	Getting the stakeholders to agree to third-party efforts

**Figure 4*- Matrix of Step 3: Foster a multi-stakeholder partnership culture

WORKS CITED

Ash, James M., Aaron J. Mann, and Peter Sloan. 2016. "European Commission Announces New US-EU Safe Harbor Agreement." Lexology, February 2. http://www.lexology.com/library/detail.aspx?g=3cccd407-4588-49bf-967d-6b7bd1925e6a (February 12, 2016).

Ball, James. 2013. "NSA Monitored Calls of 35 World Leaders After US Official Handed Over Contacts." The Guardian 24.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, andRBJ Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8 (2):121-44.

Berkman Center for Internet & Society. The USA Patriot Act, Foreign Intelligence Surveillance and Cyberspace Privacy. Retrieved from Lecture Notes Online Website: https://cyber.law.harvard.edu/privacy/Introduction%20to%20Module%20V.htm.

Birnbaum, Michael. 2013. "In Germany, legacy of Stasi puts different perspective on NSA spying". The Washington Post. Retrieved from https://www.washingtonpost.com/world/in-germany-legacy-of-stasi-puts-different-perspective-on-nsa-spying/2013/11/18/a0b1b37c-4940-11e3-b87a-e66bd9ff3537_story.html. Accessed April 3, 2016.

Blue Coat. n.d. Germany Data Privacy Laws. Retrieved from https://www.bluecoat.com/resources/cloud-governance-data-residency-sovereignty/germany-data-privacy-laws. Accessed March 26, 2016.

Briscoe, B. (2014). In The Future of Privacy published by Pew Research Center.

Brookings Institution. 2014. Big Bets & Black Swans. Retrieved from http://www.brookings.edu/~/media/programs/foreign-policy/bbbs/bigbets_blackswans_2014.pdf. Accessed March 26, 2016.

Burkert, H. Privacy - Data Protection: A German/European Perspective. Max Planck Institute for Research on Collective Goods. Retrieved from https://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf.

Center for National Security Studies. n.d. "Foreign Intelligence Surveillance Act (FISA)." Washington DC: Center for National Security Studies.

Court of Justice of the European Union. 2015. The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid. Press Release No. 117/15. Retrieved from http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf. Accessed March 25, 2016.

Dworkin, Anthony. 2015. "Surveillance, Privacy, and Security: Europe's Confused Response to Snowden." European Council on Foreign Relations (January).

Ehling, Matt. 2010. Digital culture: What does it mean for the future of American privacy? Minn Post. Retrieved from https://www.minnpost.com/community-voices/2010/03/digital-culture-what-does-it-mean-future-american-privacy. Accessed March 26, 2016.

Electronic Privacy Information Center (EPIC). n.d. The Privacy Act of 1974. Retrieved from https://epic.org/privacy/1974act/. Accessed March 26, 2016.

Electronic Privacy Information Center (EPIC). n.d. Max Schrems v Irish Data Protection Commissioner (Safe Harbor). Retrieved from https://epic.org/privacy/intl/schrems/. Accessed March 25, 2016.

European Union Center of North Carolina. 2014. "The NSA Leaks and Transatlantic Relations."

European Commission. 2015. Data Transfers Outside the EU. Retrieved from http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm. Accessed March 25, 2016.

European Commission. 2016. Statement of the Article 29 Working Party on the opinion on the EU-U.S. Privacy Shield. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf. Accessed April 28, 2016.

EUR-Lex. N.d. Protection of Personal Data. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012. Accessed April 3, 2016.

Export.gov. 2013. US-EU Safe Harbor Overview. Retrieved from https://build.export.g(EPov/main/safeharbor/eu/eg_main_018476. Accessed March 25, 2016.

Francis, David. Slate. 2015. "Germany's Hypocrisy on NSA Surveillance." October 26.

Korff, Douwe. 2014. European Commission, Directorate-General Justice, Freedom and Security. Comparative Study of Different Approaches to New Privacy Challenges, in particular in the light of technological developments.

Glazer, Barry, Christopher Koa, and Ron Moscona. 2016. "EU-US Data Transfer Privacy Shield: Political Agreement Achieved Regarding "Safe Harbor 2.0."' *JD Supra Business Advisor*. February 5. http://www.jdsupra.com/legalnews/eu-us-data-transfer-privacy-shield-89859/ (February 12, 2016).

Goldfarb, Ronald, ed. 2015. *After Snowden: Privacy, Secrecy, and Security in the Information Age*. New York: St. Martin's Press.

Hall, Claire M. 2009. "An Army of Spies? The Gestapo Spy Network 1933—45." *Journal of Contemporary History* 44 (2):247-65.

Hall, Samuel. 2014. "Balance of Powers: United States of America."

Hill, Kashmir. 2012. "Max Schrems: The Austrian Thorn In Facebook's Side." *Forbes*, February 7. http://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/#540e5afd6b30. Accessed March 30, 2016.

Hornung, G., & Schnabel, C. (2009). Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination. *Computer Law & Security Review*, 25(1), 84-88.

Jansen, T. & Hinzpeter, B. (2015). *Data Protection in Germany: Overview. Data Protection Multi-Jurisdictional Guide 2014/15*.

Jolly, L. (2015). *Data Protection in the United States: Overview. Data Protection Multi-Jurisdictional Guide 2014/15*.

Jones Day. 2016. "EU-US Privacy Shield" to replace "Safe Harbor". Retrieved from http://www.jonesday.com/eu-us-privacy-shield-to-replace-safe-harbor-02-04-2016/. Accessed March 26, 2016.

Kurra, Babu. 2011. How 9/11 Completely Changed Surveillance in US *WIRED*. Retrieved from http://www.wired.com/2011/09/911-surveillance/.

Linder, D. (2015). The Right of Privacy. Retrieved from Lecture Notes Online Website: http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html.

Madden, M. & Rainie, L. (2015). Americans' Attitudes About Privacy, Security and Surveillance. Pew Research Center.

Pearce, Sara. 2016. "The Future of 'Safe Harbor.'" Society for Computers & Law, January 21. http://www.scl.org/site.aspx?i=ed46218 (February 12, 2016).

Pew Research Center. 2015. "Germany and the United States: Reliable Allies." May 7. http://www.pewglobal.org/2015/05/07/germany-and-the-united-states-reliable-allies/ (April 18, 2016).

Symantec. (2015). State of Privacy Report. Retrieved from https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf.

Sykes, Soleil, & Lars Hansel. 2015. "Privacy and Security: A Comparative Constitutional Law Conversation." Konrad-Adenauer- Stiftung e.V. (June).

State.gov. (2015). U.S. Relations With Germany. Retrieved from http://www.state.gov/r/pa/ei/bgn/3997.htm

Stone, Geoffrey R. and Eugene Volokh. 2015. "Freedom of Speech and the Press." Common Interpretation: Freedom of Speech and the Press. Retrieved from http://constitutioncenter.org/interactive-constitution/amendments/amendment-i/the-freedom-of-speech-and-of-the-press-clause/interp/33. Accessed February 12, 2016.

The Library of Congress. (2015). Online Privacy Law: Germany. Retrieved from http://www.loc.gov/law/help/online-privacy-law/germany.php.

Tomaszewski, John P. 2016. "Safe Harbor 2.0 - Is It Happening?" Lexology, January 19. http://www.lexology.com/library/detail.aspx?g=d4da2ace-a3c4-4086-a75f-7d758b48efb9 (February 10, 2016).

Troianovski, Anton. 2015. "Germany Warns US About Spying on Its Officials." *The Wall Street Journal*. July 2.

US Department of Commerce. 2016. The EU-US Privacy Shield significantly improves commercial oversight and enhances privacy protections. Retrieved from https://www.commerce.gov/news/fact-sheets/2016/02/eu-us-privacy-shield. Accessed March 26, 2016.

Ullman, Grayson. 2016 "Cisco: In 2016, uncertain tides for Safe Harbor and encryption." fedscoop, January 9. http://fedscoop.com/cisco-in-2016-uncertain-tides-for-safe-harbor-and-encryption (February 11, 2016).

Von Solms, Suné and Renier van Heerden. 2015. "The Consequences of Edward Snowden NSA Related Information Disclosures." Iccws 2015-The Proceedings of the 10th International Conference on Cyber Warfare and Security.

APPENDIX A

<table>
<tr><th colspan="2">Stakeholder</th><th colspan="2">Interest in Safe Harbor/Privacy Shield</th></tr>
<tr><th colspan="2"></th><th>United States</th><th>Germany</th></tr>
<tr><td rowspan="2">Government</td><td>Regulatory</td><td>Stance: PRO
Regulate the flow of data in relation to commercial transactions
Make sure public and private sectors are in regulation with framework</td><td>Stance: CON
Regulate the flow of data in relation to commercial transactions
Work with US to make sure public and private sectors are in regulation with framework</td></tr>
<tr><td>Diplomacy</td><td colspan="2">Stance: CON
Oversee privacy issues, data protection issues, transfer of information
Negotiate new framework
Respond to private sector and citizens' concerns</td></tr>
<tr><td colspan="2">Academic</td><td colspan="2">Stance: NEUTRAL
Study the ways in which data is transferred as well as how to increase the safety of data storage
Examine relations between two countries and consequences of new framework
Find ways to promote the use of internet where privacy is a top priority
Find and promote better ways to secure/store information</td></tr>
<tr><td rowspan="4">Private Sector</td><td>Financial</td><td colspan="2">Stance: NEUTRAL
Deal with data transfer between the two countries
Concerned with economic impact in industry and specific entities</td></tr>
<tr><td>IT</td><td>Stance: PRO
Deal with data transfer between the two countries
Concerned about free flow of information
Skeptical of more regulation</td><td>Stance: PRO
Deal with data transfer between the two countries
Concerned about free flow of information
Skeptical of more regulation
Worries about America leading IT sector</td></tr>
<tr><td>Consulting</td><td colspan="2">Stance: PRO
Assist businesses by setting up and improving their data infrastructure
Advise on compliance</td></tr>
<tr><td>Trade</td><td>Stance: PRO
Interest in spillover effect on trade relations
Concerned with compiling with two different systems</td><td>Stance: PRO
Interest in spillover effect on trade relations
Focused on integrating two different systems
Concerned with the influx of American businesses</td></tr>
<tr><td colspan="2">Citizens</td><td>Stance: PRO
Worried data is not secure
Concerned with personal privacy being breached
Interest in US and German government coming to agreement on new framework
Hold government responsible for maintaining their security</td><td>Stance: CON
Worried data is not secure
Concerned with personal privacy being breached by US
Concerned with US intelligence community accessing data
Interest in German government making sure US protects their data
Hold government responsible for maintaining their security</td></tr>
</table>

APPENDIX B

INTERVIEW PROTOCOL

Introduction

"Hello [name]. Thank you for taking the time to interview with us. As you know, we are interested in US and German perspectives on data protection, and we are focusing especially on the Safe Harbor agreement and the related issues around the transfer of data between the US and Europe. In order to analyze this issue in further depth, we are interviewing a number of people who can offer us unique insight for the project."

Consent

[If they returned a signed consent form, including agreeing to be recorded] Thank you for agreeing to be interviewed, and for us to record the interview. Is that still all right? We are only recording it so that we can check anything we missed in our notes.

[If they let you know that they preferred to give a verbal consent:] "We sent you a consent form that described the research, its benefits and potential risks, and how we would protect your confidentiality and privacy. Having reviewed that document, do you consent to be interviewed?"

"We would like to record the interview, just as a back-up to our notes. Do you consent to have the interview recorded?"

Interview Questions

1. Does the work of your organization directly involve the transfer of data between the US and Europe?
   [If yes], Can you explain how?

   [If no], In what ways are you or your organization involved in issues around transatlantic data transfer?

2. How effective do you think Safe Harbor was in providing adequate data protection?
   If they don't offer much of an explanation, ask:
   Why do you think that?
3. What were your thoughts on the October repeal of Safe Harbor by the European Court of Justice?
4. When the ECJ invalidated Safe Harbor, was your firm/organization affected or do you expect there to be any changes now that the grace period has expired?
5. What changes, if any, were made in your firm following the ECJ's ruling?
6. What do you feel were the most important factors that led the ECJ to repeal Safe Harbor? Potential follow-up -- what made this situation so exceptional?

7. In your opinion, what was the most significant obstacle hindering the US and EU from reaching a new agreement on data protection for transatlantic data transfers?
8. What do you think of the new "Privacy Shield" enforcement mechanisms, do you believe that they are sufficient?
9. What are important considerations or what must be accomplished/included in order for "Privacy Shield" to avoid the same fate as the original Safe Harbor agreement? Why do you think that?/or Explain.
10. What would you like to see the US/ Germany [the other country] do to help resolve this issue? What do you think your own country could do to help move toward a solution?
11. Do you see data protection/privacy policies affecting U.S. and German/EU interests and policies in other areas? In what way?
12. Are there any other thoughts you'd like to share with us on these topics of data protection, privacy, Safe Harbor, the Privacy Shield, etc.?

Closing

Thank you for your time…(etc.)