AICGS ISSUE BRIEF

APRIL 2014 46

German/U.S. Data Transfers

Crucial for Both Economies, Difficult to Regain Trust

BY AXEL SPIES

Can the U.S., Germany, and the EU come to a broad agreement on privacy regulation?

What privacy issues should be prioritized in order to rebuild trust and confidence across the Atlantic?

U.S.-German disagreements over data privacy and security came to the forefront of the bilateral relationship after the 2013 revelations of the National Security Agency's (NSA) widespread data collection program. The program, leaked by Edward Snowden, allegedly included Chancellor Angela Merkel's cell phone as an NSA target. Such clandestine activity against a major European ally, an ally that places a high value on personal privacy, has strained the relationship between the two countries. However, the dispute is much larger than one of simply spying, and unveils disagreements on how to regulate international data flows in general. These data flows are crucial for both economies. Recent activities of the U.S. Trade Representative, the European Parliament, and the German government indicate that this conflict remains unresolved.

This Issue Brief sheds some light on the underlying data transfer issues, why international data transfers have grown significantly, the trials and tribulations German and U.S. companies encounter with transatlantic data transfer(s), and the privacy traditions in Germany that are often misunderstood in the United States.[1] It concludes with two concrete measures that are needed at this juncture to rebuild trust between governments and to create a safe legal environment for the private sector.

A World Full of Transborder Data Flows

Over the last decade or so, the amount of data crossing the border has steadily increased.[2] There are various factors that have contributed to this development. First and foremost, increased globalization and its advances in technology and liberalization of trade has allowed companies to expand internationally. Global companies require global data flows. To achieve this, centralized databases save companies money and help them provide better and less expensive services. Transborder data flows may also attract business to a country (such as call centers in countries with lower wages). Nowadays, international companies demand global storage of data to compete and manage their data flows, and many corporations have mirror servers at various locations for disaster prevention and backup.

The growing economic importance of data processing adds to this trend of international data transfers. Personal data have become a commodity. Big data and data mining are vital components of economic growth. For instance, car makers in Germany and the United States invest heavily in collecting data with geo-location tools to prevent theft, reduce maintenance costs, and help make traffic systems more efficient. Companies invest heavily in targeted advertisement to market and deliver their goods and services online. From the user's perspective, the increasing social importance of online activities is evident—emails and social media have all become indispensable tools for global communication among individuals; one of the largest social networking sites allegedly has more than 1 billion users.

Cloud computing, virtual backups for media files, and machine-to-machine communication imply and encourage data flows across borders even without the intervention of humans.

These data flows of course do not stop at the border. The very architecture of the Internet is an open network that allows for transborder data flows. Cloud computing, virtual backups for media files, and machine-to-machine communication imply and encourage data flows across borders even without the intervention of humans.[3] Adding to this demand is an increase in data transfers on the national level. The exchange of information between state agencies for monitoring terrorism and other criminal activities, as well as for research, fighting diseases, international litigation, and regulatory proceedings, are rapidly expanding. In U.S. civil litigation or government investigations, the exchange of thousands of documents between the parties (e-discovery) has become the standard. The same is true for government investigations under the Sarbanes Oxley Act,[4] international anti-trust proceedings, and counterterrorism efforts such as the exchanges of passenger data (PNR) and account data (SWIFT).

From the technical viewpoint, the advanced fixed and wireless broadband networks all over the world support a growing capacity to carry data and lead to a diminishing role of geography. Mobile devices and new technologies—cloud computing, online shopping, mobile banking—no longer depend on a certain location of the data or of the user. Rather, companies follow an organizationally-based approach, i.e., they organize their data sets and information worldwide by who may need the data within the organization and no longer distinguish between the territories where the data are collected, stored, or otherwise processed. By the same token, the costs for data storage have decreased dramatically over the last few years. Fixed and mobile devices store and transfer more personal data due to their increased storage capacity. Creating a mirror of a data file in the "iCloud" or elsewhere is a matter of seconds. Wal-Mart, for example, handles more than 1 million customer transactions every hour, feeding databases estimated at more than 2.5 petrabytes—167 times the contents of all books in the U.S. Library of Congress. Global traffic over the Internet has increased eightfold over the last five years. Mirror servers are becoming more and more a standard. However, increased data flows may also endanger individuals' privacy, for example, by selling customer data to unreliable third parties or data security breaches (including hacking and intentional data destructions).[5]

Increased Data Flows Raise New Legal and Regulatory Issues and Challenges

The increased quantity of international data flows raises new questions that are not simple to answer. For instance: What is a data transfer? Is it already a data transfer if personal data in the EU are simply being made available to recipients in other countries?[6] Is it appropriate that European data protection laws regulate the transfer of personal data to third parties nationally, apart from transborder data flows? What role do industry standards play?

There are no simple answers, but the bigger picture is clear: one significant underlying issue of this debate is that many countries believe that uncontrolled data flows out of the countries will lead to their loss of control over the storage of their citizens' personal data that these citizens expect them to protect. This is a particularly important aspect in those countries where data protection is enshrined directly or through court interpretation in the national constitution. This is the case in Germany, where decisions made by the Federal

Constitutional Court (*Bundesverfassungsgericht*) state that data protection ("the right of informational self-determination") of each citizen is a human right deriving from Articles 1 and 2 of the German Basic Law. On top of this, legislatures and judicial bodies face a challenge: how do they balance "data protection" as a constitutional right against the freedom of commerce and freedom of information, which are also legally protected? According to the Council of Europe Convention 108 and the German Basic Law, data protection is regarded as a fundamental human right and considered as a general principle of EU law, against which all regulation must be evaluated. The consequence is that this principle forces national governments to mandate continued and effective protection of their citizens' personal data under their home law. But where does the protection end? Does it continue to apply to the full extent once the data have left the country? Most countries, in particular in the EU, believe that the application of current data protection laws do not depend on the nationality of the individual, but on where the data are collected and stored, and that the reach of those laws do not end at the border.[7]

This issue of the reach of the German data protection law—does it end at the German border?—has been further complicated by the current NSA scandals and the spying on individuals and politicians outside of the U.S. Data sharing between government entities for law enforcement purposes significantly increased following the terrorist attacks of 9/11. The U.S. and the EU have enacted a series of mandates to share certain personal data to defend against common threats (for example, exchanging passenger PNR or financial data). European agencies tap into databases that are located in the U.S. The EU has also established various systems between the relevant law enforcement agencies for sharing data (such as the Schengen Information System).[8] Encryption that is demanded by many in Germany to fend off illegal access to their personal data is not a panacea. While national data laws may encourage encryption, it cannot protect against all threats. The security of encryption depends on who holds the encryption key and does not prevent illegal use by authorized recipients. Encryption also makes the data less valuable for the company that stores them because the company may not be able to process them.

How do they balance "data protection" as a constitutional right against the freedom of commerce and freedom of information, which are also legally protected?

And so, many jurisdictions use different approaches to regulate transborder data flows to protect their own "sovereignty" over the data that leave their territories. This leads to a fragmentation with different "data protection agencies" or to other regulatory bodies being involved for standard-setting and enforcement actions. Although many of these rules are not mutually exclusive, they make it difficult for individuals (in the EU, the so-called "data subjects") and companies ("data controllers") to determine which rules apply.

Data Exporters/Data Importers: Risks and Uncertainties

Multi-national corporations and small businesses that rely on global data flows face various risks and uncertainties. One is the unintentional non-compliance with applicable national law. If a global cloud computing provider promises to store the customer data only in a certain country/region, it must ensure that authorities from a third country do not have access to personal data and are not allowed to demand that the data will be transferred to them. Another issue multi-national corporations and small businesses must struggle with is ignorance of where their data are physically stored. They may lose this knowledge through outsourcing and the popular international cloud computing that is offered by various large providers at competitive rates—far lower than any system that the business could afford to operate itself. Another uncertainty they must also deal with is discrepancy between the laws in the countries involved in the transfer.

Furthermore, these companies face the risk that foreign agencies (law enforcement or intelligence) gain access to these data. U.S. service providers are learning this lesson the hard way through the NSA scandal: Some of their German customers prefer local storage and data processing solutions due to concerns that their data may be accessed by the NSA or other foreign bodies and then used to spy on their businesses. Recent demands by the European Parliament and others to "suspend" data transfers to the U.S. under the U.S.-EU Safe Harbor framework contribute to this risk.[9] To make matters worse for companies doing international business, overseas judicial orders from the United States may force them to disclose their data that they are supposed to keep secret under the laws of the country in the EU where a litigation or investigation is pending (for example, as part of an e-discovery process for U.S. litigation). Many international corporations struggle to ensure the same level of data protection in the receiving countries, for instance, if EU personal data are transferred to the United States.

The EU has sought to provide some level of data protection. The 1995 EU Data Protection Directive requires that there is no free flow of data to countries that have not been determined by the EU to provide an "adequate level of data protection." The current legal tools for EU/U.S. data transfers to ensure compliance are cumbersome and expensive (Binding Corporate Rules), bureaucratic (EU Standard Contractual Clauses), or

lack legal certainty (U.S.-EU Safe Harbor). Being based on rules in place for almost twenty years, they have become insufficient to cope with the almost exponential growth and the complexities of transborder data flows.

Concerns of the large and small companies that receive European data and could become liable to ensure their adequate protection, as well as the insistence of the German authorities to enforce their own data protection laws, must be weighed against a widespread lack of users' interest (data subjects) in where their personal data are stored. Available evidence suggests that individuals are largely unaware of transborder data flows and their regulation, do not often complain about potential violations, are unsure about the applicable laws, and misunderstand privacy policies of companies. In most cases, EU authorities are unwilling or unable to enforce their own data transfer rules due to a lack of administrative resources. It is difficult for these authorities to understand the complexity of the transfers and requirements. Finally, national regulators and legislatures are reluctant to enforce strict privacy standards that may scare away potential investors and new technologies, and may hurt their own economies.

To summarize: Data controllers (the companies that rely on the data flows and control it) risk being caught in the middle of compliance requirements set forth by German or EU law. Their decisions to transfer data and to make investments are motivated not solely by existing or future data transfer rules, but by other compliance and cost factors, including storage costs, compliance costs, corporate organization, location of customers, and size of the data transfers. We are seeing a disproportionate relationship between the enforcing activities and the increasing amounts of data transfers in and out of a country. There are not many incentives offered by the regulators to mitigate the compliance problems.

Future Harmonization of the Data Protection Laws Currently Unlikely

A number of data protection principles are widely accepted in most jurisdictions. However, the likelihood that the United States and Germany will reach a Convention on the Use of Personal Data[10] is slim because the data protection regimes in individual countries outside of the EU widely differ. Furthermore, there is no obvious international organization or forum that would promote such a Convention. Global solutions appear to be difficult as some countries prefer a low level of data protection requirements for companies in order to attract more business. Companies are concerned that such a Convention, if it is ever reached, may merely "paper over" core differences or disputes about how to protect privacy, for instance in the context of the current Transatlantic Trade and Investment Partnership (TTIP) negotiations. Industry players would not be helped should TTIP negotiators reach an agreement on certain privacy principles if the underlying data transfer rules remain unclear and leave the companies exposed to liability claims under the EU data protection rules. A bad compromise hurts more than it helps.

Global solutions appear to be difficult as some countries prefer a low level of data protection requirements for companies in order to attract more business.

There are also political reservations: the U.S. government is concerned that the EU will extend its "top-down" data protection approach to the rest of the world (the modern privacy Domino Theory). Such a move would encroach on the U.S. approach that is based on industry solutions and sector-specific rules. There is a concern voiced by the U.S. that pushing the EU approach on other countries—to accept certain EU standards for data transfer—is really a vehicle to further promote the national sovereignty or the national economic interest of EU member states. One recent example for this is the so-called Schengen Cloud: Chancellor Merkel has called for European data networks to be built out in which citizens' communications "need not cross the Atlantic with their emails and other things, but we can also build communications networks within Europe."[11] While it remains unclear what this "Schengen Cloud" really means and how the Germans can achieve it, the U.S. Trade Representative recently entered the fray voicing public criticism that a Schengen Cloud may violate international trade law:

"The United States and the EU share common interests in protecting their citizens' privacy, but the draconian approach proposed […] appears to be a means of providing protectionist advantage to EU-based [Internet-based service] suppliers. Given the breadth of legitimate services that rely on geographically-dispersed data processing and storage, a requirement to route all traffic involving EU consumers within Europe would decrease efficiency and stifle innovation. For example, a supplier may transmit, store, and process its data outside the EU more efficiently, depending on the location of its data centers. An innovative supplier from outside of Europe may refrain from offering its services in the EU because it may find EU-based storage and processing requirements infeasible for nascent services launched from outside of Europe."[12]

Whether the U.S. government will lodge a complaint at the WTO in Geneva or take political counter-measures (such as delaying the TTIP negotiations) remains open.

On top of it, there is also much trepidation, in particular from the United States, that restricting law enforcement's access to data would undermine the prevention of terrorist attacks and the prosecution of criminal activities. The real risks of foreign agencies spying on other countries may be exaggerated, while those concerning data protection nationally may be underplayed. The NSA scandal in Germany is a good example of this. The uproar over the NSA spying on Chancellor Merkel leaves various questions unanswered: Are the allegations true? Are Russia, China, France, or others also spying on Merkel's (or other German politicians') cell phone(s)? Why was the German secret service unable to protect the chancellor?

A potential solution to this mess would be to allow transborder data flow by default, instead of requiring an adequate level of data protection for the receiving country. In other words, data transfers to other countries should generally be allowed; any restriction of the transnational data flow would require a justification that must be clear and explicit so that businesses know in advance, with some degree of certainty, what the rules are. The current EU approach, by contrast, is that "adequacy of data protection" is the result of a lengthy and cumbersome bureaucratic process; adequacy must first be "gained" from the European Commission by the country receiving the personal data. Another option for the Europeans would be to acknowledge private sector arrangements (industry standards, codes of practices developed by the industry sector in cooperation with the relevant data protection agencies) on transborder privacy. These ideas are unpopular in Brussels or Berlin.

The real risks of foreign agencies spying on other countries may be exaggerated, while those concerning data protection nationally may be underplayed.

Specific German Concerns

When searching for transborder solutions, U.S. politicians and media outlets sometimes forget or underestimate Germany's perspective. Germany was one of the first countries with extensive "data protection laws" for the public and private sector and significantly influenced the 1995 EU Data Protection Directive. Germans are proud of this tradition. Germany will not easily give up its approach to privacy or its data protection achievements. There is a long history of court decisions since the Federal Constitutional Court's Census Decision enshrined the "right of informational self-determination" and more recently (in 2008) a "right of confidentiality and integrity of IT systems."[13] Germany defines privacy (using the term "data protection," which has a much narrower meaning in the United States) as a right that the government must protect under the Basic Law, even between companies and consumers. This is different from in the United States, where privacy as a concept is mainly used to avoid intrusions by the government under the Fourth Amendment.

Germans also resent spying by government agencies, a reaction to Germany's recent history when the East German spying agency, the STASI, collected intelligence on its citizens. Concerns remain that the desire of the government to control its citizens may undermine or render inefficient an individual's right "to be left alone." The Germans also fear that excessive data collection may create a "digital twin" or a "digital shadow" that may have little to do with the actual individual.[14] President Gauck explained this concern in his speech marking German Unity Day on 3 October 2013, highlighting the importance of this issue: "Many do not realize, or simply do not want to know, that they are complicit in the creation of the virtual twin to their real life self—their alter ego who reveals, or could reveal, both their strengths and weaknesses, who could disclose their failures or deficiencies, or who could even divulge sensitive information about illnesses. This makes the individual more transparent, readily analyzed, and easily manipulated by agencies, politics, commerce, and the labor market."[15]

Germany will not easily give up its approach to privacy or its data protection achievements.

The NSA scandal has generated widespread distrust and disappointment, as promoted by various German media outlets, against "friends and allies who spy on Germany's political leaders," a reference to the NSA tapping Merkel's cell phone. Excessive data inspection by the NSA, as disclosed by Snowden, nurtures a general suspicion that every citizen is deemed a potential supporter for terrorism. But this is not the entire story. There is also widespread concern that the information collected by government agencies is used for economic espionage against Germany and German companies—an allegation fervently denied by the U.S. government. If this allegation is true, German industry would lose out against U.S. conglomerates. Many Germans also believe these U.S. companies will thrive on the data they receive from Germany, treating the data as a commodity—using and sharing them in ways they could not do in Germany. On a broader level, unrestricted data inspection on a global scale may degrade the individual to a mere object of consumerism and lead to an authoritarian regime, as was exemplified by the Manchester capitalism in the nineteenth century that exploited the workers, states Martin Schulz, the current President of the European Parliament, who calls for further government intervention to protect the privacy of citizens.[16]

Regaining Trust: Focusing on Practical Steps

Many of these German concerns and the issues and dilemmas that companies with business in Germany and in the United States are facing are difficult to address since many of them are irrational. They are based on a fear of clandestine surveillance by a government agency or large private entities ("Big Brother is watching you") that has nothing to do with the reality, but is hard to overcome. The actual polls in the EU and in the U.S. on whether privacy is an important issue for citizens are not much different. What both sides can probably agree on is that international data transfers require an environment of trust and legal certainty. This is not just a German-American problem—although both countries are important global players in addressing it—even though they have different privacy regimes and traditions. Ironically, data protection reform currently is driven forward by the European Commission, a body many Germans distrust or resent.

What both sides can probably agree on is that international data transfers require an environment of trust and legal certainty.

The debate is not only between the U.S., Germany, and the European Commission. Germany is also facing a challenge from other European allies. A new French/German initiative for a Schengen-Internet, with no routing via the U.S., may exclude some EU member states (primarily the UK). This may not only be technically impossible, but also legally questionable. According to the report from the United States Trade Representative, mentioned above, such European or national-only networks would "decrease efficiency and stifle innovation" and "raise questions with respect to compliance with the EU's trade obligations with respect to Internet-enabled services."[17] On the other side of the Atlantic, some German agencies are reportedly investigating whether companies that provide services in Germany for U.S. agencies or the U.S. armed forces are involved in spying activities on their behalf on German territory.[18] Due to the increased tension, data privacy threatens to become a major stumbling block in the already halting progress of negotiating the Transatlantic Trade and Investment Partnership.

Whatever the outcome of the debate, all this indicates that it will be a long process for the United States to regain the trust of one of its closest allies. Europeans clearly expect "something" for the perceived violation of their privacy by U.S. agencies, such as a revision of the U.S.-EU Safe Harbor framework or a "No-Spy-Agreement." It is important for the Obama administration to realize this concern when cooperating with Germany. Otherwise, no trust will be regained.

A first step toward advancing the debate would be a joint U.S.-German statement on the core issue of data protection. Both President Obama and Chancellor Merkel have a joint interest in defusing tensions and preventing further damage to the prospects of a free trade agreement. Some sensational reports from the press have unfortunately blurred the lines between the privacy and cybersecurity topics, pointing toward U.S. malfeasance when much more threatening acts of cyber espionage and crime occur on a daily basis. This breeds uncertainty of whether European data is safe from those "outside" Europe. At the same time, the U.S. government's intelligence services have collected so much information in pursuit of their mission that they have found it difficult to limit the scope, access, and processing of the data and fully comply with existing U.S. laws. Foreign individuals outside the United States are not fully protected from excessive data collection, but spying overseas must not be an excuse for the NSA to avoid strict U.S. rules on data collection. The Obama administration should be able to acknowledge that more transparency and better enforcement of existing law is needed.

Neither intergovernmental talks on privacy nor TTIP negotiations will likely lead to a transatlantic "grand bargain." **A more practical step would be to focus on reforming or updating the U.S.-EU Safe Harbor framework on international data transfers—not eliminating it.**[19] Even this narrow process will take time. As a first step, this requires that both sides acknowledge that the long-standing U.S.-EU Safe Harbor framework and the NSA spying issues are not connected. The former is a longstanding agreement that allows both U.S. and European companies to adhere to EU privacy law when exporting data to the United States. The latter is about how to defend the freedom of the internet while clarifying how it can be exploited (not just by whom, but also why). The often emotional discussion must be brought back on track—not an easy task while the European Parliament is calling for its "suspension" that would be a train wreck for the industry. It is important that there be an open discussion between the German and U.S. governments, including the European Commission, about what works and what does not under the current Safe Harbor framework. That could have been done much earlier since the framework came into effect thirteen years ago—but better late than never.

It is clear that neither Germany nor the United States will be able to just sweep these issues under the rug. Edward Snowden's revelations and the accompanying uproar may have distracted leaders from many other pressing issues, but simply wishing it away is not a solution. The competing frameworks and attitudes on either side of the Atlantic toward data privacy threaten to erode the trust at the core of bilateral relations, despite enduring and mutually beneficial intelligence and business relationships. In the end, the United States and Germany must work together in establishing new rules of the road.

1 See Jim Harper and Axel Spies, "A Reasonable Expectation of Privacy? Data Protection in the United States and Germany," *AICGS Policy Report* 22 (Washington, DC: AICGS, 2006), <http://www.aicgs.org/publication/a-reasonable-expectation-of-privacy-data-protection-in-the-united-states-and-germany/>.

2 See Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford: Oxford University Press, 2013), chapter 1.

3 This has been part of the controversial concept called the "Internet of Things" (i.e., machines), which some fear could lessen people's control over their own lives.

4 The Sarbanes Oxley Act (SOX) is a United States federal law that sets enhanced standards for all U.S. public company boards, management, and public accounting firms. U.S. authorities, such as the Securities and Exchange Commission (SEC), issue rulings on requirements to comply with the law and prosecute companies that violate SOX.

5 A recent example of this is the investigation against the serious data breaches at the U.S. company Target. See <https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ>.

6 ECJ Case C-101/01 In re Lindquist. See <http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en>.

7 Art. 4 (1) EU Data Protection Directive 95/46/EC: Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

8 The Schengen Information System (SIS) allows Schengen States to exchange data on suspected criminals; on people who may not have the right to enter into or stay in the EU; on missing persons; and on stolen, misappropriated, or lost property.

9 EU Parliament's Resolution adopted 12 March 2014: "U.S. NSA: stop mass surveillance now or face consequences, MEPs say," <http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38203/html/US-NSA-stop-mass-surveillance-now-or-face-consequences-MEPs-say>. This resolution is legally not binding but is meant to send a powerful signal to the U.S.

10 Similar to the Council of Europe Convention 108.

11 Quote by Ulrich Clauß, "So würde Europas 'Schengen-Internet' funktionieren," *Die Welt*, 31 March 2014, <http://www.welt.de/politik/deutschland/article126343060/So-wuerde-Europas-Schengen-Internet-funktionieren.html>. Many experts in Germany believe that a Schengen Internet is not a realistic goal, given the open structure of the Internet.

12 Office of the United States Trade Representative, "2014: Section 1377: Review On Compliance with Telecommunications Trade Agreements," available at <http://www.ustr.gov/sites/default/files/2013-14%20-1377Report-final.pdf>.

13 See, for instance, the very informative blog of the German Federal Data Protection Officer (in German) with excepts at <http://www.datenschutzbeauftragter-online.de/das-bundesdatenschutzgesetz-bdsg/urteile-des-bverfg-zur-informationellen-selbstbestimmung/>.

14 Frank Schirrmacher, "Rede des Bundespräsidenten: Vom digitalen Zwilling," *FAZ.net*, 3 October 2103, <http://www.faz.net/aktuell/feuilleton/debatten/rede-des-bundespraesidenten-vom-digitalen-zwilling-12602600.html>.

15 Speech available at <http://www.bundespraesident.de/SharedDocs/Reden/EN/JoachimGauck/Reden/2013/131003-Day-of-German-Unity.html>.

16 Martin Schulz, "Technologischer Totalitarismus: Warum wir jetzt kämpfen müssen," *FAZ.net*, 6 February 2014, <http://www.faz.net/aktuell/feuilleton/debatten/technologischer-totalitarismus-warum-wir-jetzt-kaempfen-muessen-12786805.html>.

17 Office of the United States Trade Representative, "2014: Section 1377: Review On Compliance with Telecommunications Trade Agreements," available at <http://www.ustr.gov/sites/default/files/2013-14%20-1377Report-final.pdf>.

18 Ralf Neukirch, "Reaktion auf Spionage: Bundesregierung nimmt US-Firmen ins Visier," *Spiegel Online*, 18 March 2014, <http://www.spiegel.de/politik/deutschland/nsa-affaere-bundesregierung-erhoeht-druck-auf-us-firmen-a-959039.html>.

19 This appears to be the approach of the Article 29 Working Party, the body of national data protection representatives advising the EC on data transfer issues. See the letter of 10 April 2014 to EU Commissioner Reding regarding EU-U.S. Safe Harbor, available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf>.

Questions for Further Debate

- Do Americans and Europeans have fundamentally different values when it comes to data privacy and protection?
- Are there better ways to identify and share information across the Atlantic?
- If government is increasingly dependent on the private sector, who should ultimately be in control of collecting and using data?
- What are the economic incentives for business to join the public forum on these issues?
- How can policymakers learn more about technical issues in order to make sound decisions?
- What privacy issues should be prioritized in order to rebuild trust and confidence across the Atlantic? Should there be increased integration or privacy? Do you improve existing infrastructure or rebuild it in a different way?
- What should be the final goal and how should it be articulated?

German and U.S. Approaches to Protecting Privacy and Information

There has been a heated transatlantic debate on cyber issues since Edward Snowden's release of classified National Security Agency (NSA) documents last year that described various surveillance activities, including the collection of information from Chancellor Angela Merkel's cell phone. These revelations have strained the relationship between the two countries and have sparked an emotional debate.

U.S. and German governments and businesses alike are struggling to balance privacy demands with the opportunities and risks associated with the exponential increase in internet users and the ever-expanding flow of data between states. Some reports estimate more than a 30 percent increase in global data traffic every year. Meanwhile, civil society actors have also struggled to clearly articulate the problems and costs associated with this rapid change and its impact on privacy.

This is not just a German-American problem, but both countries are crucial to addressing it—even though they have different privacy regimes and traditions. A lot of trust has been lost, especially in Germany, and it will take a long process for the United States to regain this trust. Europeans clearly expect "something" for the apparent violation of their privacy, such as the revision of the U.S.-EU Safe Harbor framework. Yet this will not necessarily lead to a transatlantic "grand bargain."

Part of AICGS' Foreign & Domestic Policy Program, this Issue Brief is the result of an AICGS workshop on data privacy, held on March 12, 2014. AICGS is grateful to the Louis R. and Candice A. Hughes Charitable Foundation and to the Transatlantic Program of the Federal Republic of Germany with funds from the European Recovery Program (ERP) of the German Federal Ministry of Economics and Technology (BMWi) for their generous support.

Dr. Axel Spies is a German attorney in Bingham McCutchen's Washington, DC office and co-publisher of the German journal ZD (*Zeitschrift für Datenschutz*).

American Institute for Contemporary German Studies
JOHNS HOPKINS UNIVERSITY

1755 Massachusetts Ave., NW
Suite 700
Washington, D.C. 20036 – USA
T: (+1-202) 332-9312
F: (+1-202) 265-9531
E: info@aicgs.org
www.aicgs.org

German/U.S. Data Transfers
Crucial for Both Economies, Difficult to Regain Trust

Located in Washington, DC, the American Institute for Contemporary German Studies is an independent, non-profit public policy organization that works in Germany and the United States to address current and emerging policy challenges. Founded in 1983, the Institute is affiliated with The Johns Hopkins University. The Institute is governed by its own Board of Trustees, which includes prominent German and American leaders from the business, policy, and academic communities. Please visit our website at www.aicgs.org.

Providing Knowledge, Insights, and Networks for the Future.