Center for
Technology Innovation
at BROOKINGS

May 2014

Missed Connections: Talking With Europe About Data, Privacy, And Surveillance

Cameron Kerry

Cameron Kerry joined Governance Studies and the Center for Technology Innovation at Brookings as the first Ann R. and Andrew H. Tisch Distinguished Visiting Fellow in December 2013. He is also a visiting scholar with the MIT Media Lab. Kerry served as General Counsel and Acting Secretary of the United States Department of Commerce, where he was a leader on a wide of range of issues laying a new foundation for U.S. economic growth in a global marketplace, including privacy and data security, intellectual property, and international trade.

The conversation between the United States and Europe about data privacy has been through many twists and turns over the past year.

This has never been an easy conversation. Despite a great deal in common, differences in attitudes and legal systems have accentuated the differences that exist around privacy. And the Snowden disclosures turned the conversation into more of a scolding. But as the initial anger subsides and the Administration takes steps to affirm America's commitment to protecting privacy at home and abroad, it may be possible to resume a genuine give-and-take.

There is a great deal at stake, because the transatlantic economy accounts for 50 percent of the world's GDP. Digitally-enabled trade flows in and out of the United States amount to more than $500 billion, a rough measure of the value of data flows, and the largest share of these by far is with Europe.[1] This is why discussions of the Transatlantic Trade and Investment Partnership (TTIP) and mechanisms for the flow of digital information and protection of private data are significant. The profound reaction to the Snowden disclosures in Europe, Brazil, and elsewhere have brought home just how large these issues loom on the global stage.

THE SITUATION BEFORE SNOWDEN

It is conventional wisdom in Europe that Americans do not care about privacy. This view is embedded in Europe's ambitious legal regime for protection of data privacy. The Lisbon Treaty declares "data protection" to be a fundamental right. The comprehensive 1995 European Union Privacy Directive (reinforced by more specific directives like one aimed at cookies) strictly regulates all data collection and use by

the private sector and prohibits the transfer of data on EU citizens to any country that does not have privacy protection deemed "adequate" by the European Commission. Although both Facebook and Google (among many other U.S. companies) have hundreds of thousands of users in Europe, many Europeans view their success as well as their collection of personal data through various lenses of envy and alarm.[2]

The United States and the European Union have bridged their differences on privacy and avoided restricting the flow of digital commerce by adopting the US-EU Safe Harbor Framework in 2000.

The United States has no single law addressing privacy. What it does have is a body of laws. These include requirements in specific sensitive sectors—health records, credit reports, financial information, communications, student records—as well as Federal Trade Commission enforcement against unfair and deceptive acts in violation of companies' privacy policies or other promises and data breach laws in 47 states. This has led to the professionalization of privacy: the International Association of Privacy Professionals, the trade association for privacy officers and privacy lawyers, now has exploded to more than 15,500 members, of which over two-thirds are American. Privacy scholars Deirdre Mulligan and Kenneth Bamberger have called this mosaic of compliance "privacy on the ground" compared to European "privacy on the books;" their extensive empirical study of U.S. business practices found its elements "interacted in reconstructing privacy norms in consumer terms, and participated in the diffusion and institutionalization of these norms," and that chief privacy officers in U.S. companies have become more integral to corporate strategy and risk-management than are more compliance-and-reporting focused European data protection officers.[3]

The United States and the European Union have bridged these differences and avoided restricting the flow of digital commerce by adopting the US-EU Safe Harbor Framework in 2000.[4] This framework declares a set of principles for privacy protection presumed "adequate" by the European Commission, and allows U.S. companies to self-certify that they will adhere to these principles subject to enforcement by the Federal Trade Commission. More than 3,000 companies on both sides of the Atlantic are using this framework.[5] Some privacy advocates in Europe have questioned its adequacy, and a 2008 report suggested that companies were not living up to their self-certifications. But the FTC stepped up enforcement in recent years—most notably, its high-profile consent decrees with Google[6] and Facebook[7] included a charge that these companies failed to live up to Safe Harbor commitments. In 2012, EU Vice-President and Justice Commissioner Viviane Reding and Commerce Secretary John Bryson reaffirmed the Safe Harbor Agreement.[8]

The latter events took place while review of privacy policy and law was under way in both the United States and Europe. The European Commission in 2012 proposed a privacy regulation that would unify the different regimes of member states while also adding significant new regulatory requirements that up the ante on the 1995 European Privacy Directive. As a regulation, this proposal would bind member states directly rather than needing to be "transposed" into the law of member states as a directive does—an important step in the EU's post-Lisbon intention to develop a "single market." Businesses on both sides of the Atlantic have welcomed this "one-stop-shop" approach but expressed concern about additional regulatory burdens and potential fines of up to two percent of global turnover (scaled back from five percent in a draft). Along with the regulation, the Commission also proposed a new directive that—for the first time—would extend its privacy oversight to the public sector, obligating member states to adopt laws consistent with the directive and reflecting the new ordering of power in the EU after the Lisbon Treaty.

The White House privacy blueprint articulated a new and comprehensive framework centered on a Consumer Privacy Bill of Rights, seven principles that adapted Fair Information Practice Principles—originated in the U.S. in the 1970s and incorporated into privacy protection around the world—to current technology and usage in easily understandable terms.

At the same time as the European Commission was drafting its regulation and directive, the Obama Administration was preparing its consumer privacy policy statement, *Consumer Data Privacy in a Networked World*, issued almost simultaneously in 2012.[9] This blueprint articulated a new and comprehensive framework centered on a Consumer Privacy Bill of Rights, seven principles that adapted Fair Information Practice Principles—originated in the U.S. in the 1970s and incorporated into privacy protection around the world—to current technology and usage in easily understandable terms.

The blueprint also called for international engagement on privacy, and such engagement was especially active with the EU. As a leader in this effort, I found President Obama's signature on the document to be a powerful calling card: his forward was a strong affirmation of ways that privacy is embedded in American values and law and, along with description of the Consumer Privacy Bill of Rights, provided an affirmative story that helped clarify American attitudes and legal protections on privacy. This message and additional description of the number of ways American law protects privacy chipped away at European perceptions, at least among opinion leaders.

The U.S. engaged actively with EU institutions and stakeholders where the proposed regulation and directive could have an impact on the U.S. interest in the free flow of information across borders. These were focused especially on maintaining the US-EU Safe Harbor agreement as well as law enforcement and regulatory sharing of information under existing treaties and conventions. When a leaked draft of the regulation and directive contained a section (known from the draft as Article 42) that would have put a sunset on Safe Harbor and various provisions that appeared to abrogate treaties and conventions (a concern shared by other countries including EU member states), instead interposing review by European data protection authorities, U.S. agencies produced a set of comments in the space of two weeks that were delivered to various members of the European Commission.

This U.S. engagement was controversial in some quarters. One senior EU official evidently sniffed, "Since when did the United States become the 28th directorate-general of the European Commission?" and complaints about "lobbying" by the U.S. government as well as U.S. companies later generated prominent headlines.[10] Nonetheless, when the Commission submitted its official proposal, it contained neither the Safe Harbor sunset nor the problematic Article 42.

Although the U.S. government left most concerns about regulatory scope to private sector advocates, it did call attention to two areas of contrast with the White House blueprint. The first was to press for greater opportunity to recognize codes of conduct developed by the multistakeholder process advocated in the blueprint and also in OECD recommendations to which EU member states are parties. The second was to suggest that the EU's adherence to a hard-and-fast requirement of explicit consent to collection of personal information in all circumstances is excessively rigid in today's computing environment, and point to the more flexible, contextual approach recommended in the Consumer Privacy Bill of Rights.

The U.S. also confronted "the Patriot Act issue"—the widely held perception that various legal authorities conflated under the USA-PATRIOT Act label give U.S. law enforcement and intelligence agencies unfettered access to communications. To support a fact-based discussion of what these legal authorities actually do and how they are more protective than those of most other countries, the State and Justice Departments produced a white paper aimed at dispelling myths about the Patriot Act.[11] This paper (focused on law enforcement rather than intelligence access, for reasons now obvious) documented ways in which U.S. due process protections exceed those in most European countries. While it is correct that non-citizens outside the United States are less protected under current American law than are American citizens, the relevant question for most Europeans is really whether in using American online services they enjoy less protection from the American government than they do from their own.

As the European legislative process moved forward, proponents of the regulation and directive struggled to meet their timeline of final passage within the mandate of the current Parliament and Commission and before the 2014 parliamentary elections. Even after a push during the Irish presidency of the European Council in the first half of 2013, representatives of the member state governments were not ready to negotiate with the Parliament and Commission. Meanwhile, the parliamentary committee reviewing the measures faced more than 3,000 amendments and complained about the amount of "lobbying" by U.S. companies and the government. Actually, amendments did not come from the U.S. government and the number had more to do with the ambition and complexity of the regulation and directive—the scope of their regulation of business including small and medium enterprises, the number of acts delegated to the European Commission, and the reordering of authority between the European Union and member states. In any event, the committee postponed anticipated action several times—the last time shortly before the first Snowden stories.

THE SNOWDEN FIRESTORM

The Snowden disclosures gave the pending legislation a new surge of momentum. They erased any progress in changing perceptions about America with a vengeance, feeding with steroids the perceptions about "the Patriot Act" and unfettered access to online communications, and hardening the European conventional wisdom.

The greatest impact may have been political: the disclosures hardened European views on the flow of data to the United States, and undermined global trust in the model of Internet governance that evolved in the United States.

Both America's brand and the brand of American companies were damaged in the process. The potential economic fallout has been cause for alarm. Early estimates of the economic losses American companies range from $22 billion[12] to $180 billion[13] over the next three years, and survey research as well as individual anecdotes reflect increased reluctance on the part of non-US businesses to entrust data to U.S. cloud services and other ICT providers. These sentiments have been reflected in concrete reports of business losses and delays of deals due to fear that the NSA might gain access to data entrusted to U.S. providers.

But the greater impact may have been political: the disclosures hardened European views on the flow of data to the United States, and undermined global trust in the model of Internet governance that evolved in the United States.[14] More narrowly, this has fueled efforts to suspend the Safe Harbor Framework and led to calls for some form of "European cloud" that would keep data on European citizens within the boundaries of the European Union.

On July 4—a date surely chosen for maximum in-your-face effect—the European Parliament voted overwhelmingly for a nonbinding resolution condemning U.S. spying and calling for stepped up efforts to protect the data of European citizens in law enforcement agreements and the Transatlantic Trade and Investment Partnership, review of the Safe Harbor agreement, reinstatement of Article 42, and for the European Council to accelerate work on the proposed regulation.

Such a hard line might be expected from the Parliament. But even officials who had been reserved about the European Commission's proposals warned of fast action as a response to U.S. government surveillance and fears that data in the hands of U.S. companies may be available to the NSA. A European minister attuned to US concerns disclosed that a summit of EU leaders scheduled for October would express the political will to get the legislation done, which could have forced the hand of the European Council that is the voice of the member states in the EU. Commission Vice-President and Justice Commissioner Viviane Reding had been pragmatic about maintaining trade and innovation and blunting private sector anxiety about proposals in the Commission regulation and, in October 2012, was forceful in declaring that "Safe Harbor will stay."[15] But last July, she declared that "maybe Safe Harbor is not so safe anymore."[16] This sharp turn reflected a new center of gravity in European opinion. Thus, as European institutions departed for their August vacations last year, it looked like they might be poised to act on the proposed regulation during the fall and throw the book at the United States with every measure that raises anxiety about the continued flow of data across the Atlantic.

THE AFTERMATH

As things have played out since, there are signs the firestorm has abated somewhat, but there are still fires burning. With the passage of some time, Europe is not speaking as much with one voice as it was in the immediate reactions to the early Snowden stories. While the European Parliament has continued on the course it charted in July with votes on legislation and other action in advance of parliamentary elections this May, as the smoke has cleared the member states and other actors have operated on a different calendar with different interests.

As things have played out since, there are signs the firestorm has abated somewhat, but there are still fires burning.

When EU leaders met in October (right after controversy about eavesdropping on Chancellor Merkel's cellphone flared up the Snowden fires), they expressed a desire for "timely adoption" of a data protection framework to achieve a digital single market across the EU "by 2015"[17]—a date past the parliamentary elections and the mandate of the current Council and Commission. Although this statement was somewhat

ambiguous ("by 2015" could include before elections in 2014), in fact the European Council has not arrived at a mandate for negotiation with the Parliament and Commission and has made only modest progress on the draft regulation since the Irish Presidency of the Council ended in mid-2013.

Parliament, however, has forged ahead. Last November, the Civil Liberties, Justice, and Homeland (LIBE) Committee issued its report proposing some 207 amendments to the Commission's proposed regulation. Much in line with the parliamentary vote the previous July 4, these included reinstating Article 42 (somewhat modified and renumbered as Article 43) as well as a provision that would sunset the Safe Harbor Framework two years after the regulation takes effect unless it is amended, replaced, or repealed in the meantime. The committee also proposed moving the maximum fine back to the original five percent of turnover worldwide. Last March, by a lopsided 621-10 vote (10 abstentions), the full Parliament adopted this text on first reading. At the same time, by a much closer vote of 371-276 (30 abstentions) it also adopted the proposed public sector directive even though the Council has given it scant attention.

This was not the only action the Parliament took affecting the United States and privacy issues. It also took up another report of the LIBE Committee, this one on surveillance of European citizens both by the NSA and by intelligence services of EU member states. By a 544-78 vote (60 abstentions), the Parliament adopted a resolution condemning "mass surveillance." It called on the Commission to conduct "a comprehensive assessment of the U.S. privacy framework" and to suspend the Safe Harbor Framework and the Terrorist Finance Tracking Program (TFTP) pending complete reviews. It also threatened to withhold approval of any TTIP agreement that does not adequately protect EU privacy rights.[18] And, while giving a nod to avoiding government control, censorship, or balkanization of the Internet, Parliament adopted an amendment calling on the Commission to propose a legal framework for "a European routing system … that will be a substructure of the existing internet and will not extend beyond EU borders."[19]

Because the Parliament's term has expired and a new Parliament is being elected May 25, these votes have no immediate effect. Instead, the adopted regulation and directive text will provide a foundation that the Parliament can move forward on rather than choose to go back to a first reading. For now, the votes have allowed proponents of the regulation and directive to bank their gains and send a message, not only to voters at home but also to the European Council and to member states for future give-and-take.

THE ROAD AHEAD

What that future holds has a number of uncertainties. The Parliament's action on the privacy regulation and directive puts the ball in the court of the European Council. According to a key player in the latter's deliberations on these measures, the Council will try to develop a position

on the legislation in the second half of this year. This would put the Council in the position to begin the process of "trialogue" negotiations among the Parliament, the Council, and the Commission once both the Parliament and Commission have organized themselves under their new mandates.

That means the discussion will move forward with a number of new players in place in two corners of the trialogue. The Parliament also will change some faces to reflect changes in membership and ideological groupings in the May election. The next Commission president, with the input of member states and Parliament, will choose a new set of commissioners. In any event, Viviane Reding will not return to the Commission and instead has run for the European Parliament in her home country of Luxembourg. She has been a pivotal force in shaping the legislation and moving it forward; her political skill, clout, determination, and negotiating got the proposals out of the Commission despite negative comments from other directorates-general and she has been relentless in pushing member states to move the Council process along and working out deals to make that possible. She will be a tough act to follow. But Reding could have a different seat at the table: there is speculation that she could wind up as chair of the next LIBE Committee. It was perhaps with such a role in mind in addition to protecting a legacy that she declared that the Parliament vote "is set in stone."[20]

The EU member states represented in the Council bring a different outlook to the table than does parliamentary leadership.

One of Reding's lieutenants told me when the legislation was still in draft form that "the Parliament will take it one direction, the Council will take it in the other direction, and it will come out close to the way we proposed it." Whether another Commissioner at DG-Justice (or another directorate if privacy issues are reassigned) will bring to the regulation and directive the same outlook and same drive is unknown. Given the vote for the regulation in the current Parliament, it is unlikely that the outlook in the next one will change substantially, but changes in leadership or line-up could affect how the parliamentary side acts whenever triangular negotiations begin.

Meanwhile, the Council will work during Italy's presidency in the second half of 2014 to be in a position to begin those negotiations. The EU member states represented in the Council bring a different outlook to the table than does parliamentary leadership.

First, national government representatives involved are more attuned to concerns about regulatory burdens—for example, the level of fines or an inflexible requirement of explicit

consent to data collection in every circumstance. This is especially true of economically liberal governments in the UK, Netherlands, and Sweden that have stated their reservations about the regulation explicitly. But representatives of other large member states share these reservations to some degree as well. Just as state governors in America have shown themselves to be more pragmatic than their party members in Congress, national governments in the EU are less ideological than their parliamentary representatives. They are more visible and directly accountable for the state of the national economy than parliamentarians away in Brussels and Strasbourg, and so they are more sensitive to concerns about the impact of the regulation on innovation and business growth.

Even more, the member states have sovereign interests at stake. The proposed regulation, the directive, and Parliament's actions on surveillance all present the prospect of a significant increase in European Union authority over the operations of member governments. Thus, the Council has treated the draft public sector regulation something like a dead rat, scarcely touching it. The swing of more than 250 votes from the regulation to make a relatively close margin for the directive reflects a substantial number of parliamentarians supporting their home governments on the latter proposal. Moreover, although member state governments subscribe on some level to the single market drive, some are reluctant to substitute a regulation for a directive, preferring the flexibility to adopt less prescriptive policies (the UK) or maintain their own stricter protections (Germany). This suggests a difficult road in any negotiations with the Council, especially over a directive on public sector privacy rules.

Such negotiations play into a broader tug-of-war between the European Union and its members. Since the initial European furor over the Snowden disclosures focused on the collection of metadata under the Section 215 and Section 702 programs and the initial defense of these programs as not spying on any Americans, the spotlight has broadened to questions about what European countries are doing by comparison. And, sure enough, press reports in France, Germany, and Brazil disclosed surveillance that, while perhaps not on the same scale as NSA surveillance, was at least as intrusive and less protective of both citizens and foreign nationals. The European Parliament stepped into the fray, with the LIBE Committee conducting a study (mostly secondhand from press reports rather than direct oversight) of intelligence-gathering by major member states, leading up to the report adopted by the Parliament. Although initially focused on the NSA, that report focused at least as much on member states as on the United States. On April 10, the "Article 29 Working Group," composed of all the data privacy authorities of EU countries, weighed in with an opinion that took aim not just at U.S. surveillance but also that of member states, calling for greater transparency, oversight, and protection.

The member states, however, maintain that the European Union lacks authority over their law enforcement and intelligence-gathering, that EU treaties and practice reserve such authority

to the several states. This is also at play with regard to the provision of the regulation reinstated by Parliament that would require approval by data protection commissioners of any private company transfers of personal data to "third countries" (Article 43), because it would affect law enforcement and intelligence cooperation.

With these interests at stake, the slow pace of the Council and the timetable set by European summit leaders for a data protection framework "by 2015" seem to reflect a desire to be the cooling saucer. It appears they prefer to see the Council to take the legislation up with a new Parliament and Commission in an atmosphere further removed from the first flush of Snowden disclosures and the run-up to elections, when it may be easier to protect their sovereign and policy interests.

The time since last July has enabled President Obama to engage the United States and the highest levels of his administration in "a national conversation about privacy" that helps to get the international conversation back on track.

CONSEQUENCES ON THIS SIDE OF THE ATLANTIC

The United States has benefitted from the same cooling period. Above all, the time since last July has enabled President Obama to engage the United States and the highest levels of his administration in "a national conversation about privacy"[21] that helps to get the international conversation back on track. The President in his January 17 address and policy directive made explicit and binding the limits that the United States places on foreign intelligence collection and took "the unprecedented step of extending certain protections that we have for American people to people overseas."[22] The Director of National Intelligence and Attorney General will give specific form to this new protection in the coming months. The President's declaration goes a significant way toward putting most foreign citizens on a par with Americans and, in turn, affords them greater protection against surveillance from the United States than from other countries, including in most cases their own. The steps taken with regard to surveillance involving U.S. citizens also resonate globally. The Big Data working group led by Counselor to the President John Podesta took a further step by recommending that federal Privacy Act protections apply regardless of nationality.[23]

In addition, the passage of time has afforded the opportunity to put NSA surveillance into perspective. The increased (if belated) transparency provided by declassification of FISA Court decisions and other intelligence materials has helped to clarify how the United States governs foreign intelligence collection and show that NSA surveillance has not been as

all-encompassing as some fear and initial news stories made it sound. The widened focus to include European surveillance coupled with more information about how the United States governs foreign intelligence collection is helpful, not just because they create an equivalency, but because the legal regimes in most other countries do not stand up well to comparison.

Even though the atmosphere has cooled compared to last summer, it remains charged. Edward Snowden took the same virtual media tour that had him appearing remotely at the South x Southwest and TED conferences "on the road" to the EU. In February, he submitted a written statement and answers to questions from LIBE committee, and in March he appeared by video before the European Council. His submissions included allegations that the NSA circumvented European privacy laws by seeking out loopholes and gaming jurisdictions, what he described as "a European bazaar." Asked about the involvement of EU states, he implied that journalists are working on additional disclosures. Snowden has a receptive audience in Europe; one European parliamentarian retweeted a comment about Chancellor Merkel's May visit to Washington that she was off to see *Großen Bruder* (Big Brother).

In this atmosphere, the United States faces three concrete challenges for the transatlantic digital economy. These are (1) maintaining the Safe Harbor Framework, (2) negotiating provisions of TTIP that may affect the flow of digital information, and (3) broadening support for non-governmental, multistakeholder governance of the global Internet.

In this atmosphere, the United States faces three concrete challenges for the transatlantic digital economy. These are (1) maintaining the Safe Harbor Framework, (2) negotiating provisions of TTIP that may affect the flow of digital information, and (3) broadening support for non-governmental, multistakeholder governance of the global Internet.

SAFE HARBOR. The Safe Harbor Framework remains a target. In response to the Parliament's prodding last summer, the Commission's Directorate General–Justice issued report on the framework that was in the works well before the Snowden stories broke but became more fraught in their wake. Moreover, although the European Privacy Directive carves out national security, critics of Safe Harbor contended that U.S. company compliance with the Section 215 and 702 programs amounted to data transfers in violation of Safe Harbor obligations and expressed concern about the amount of data the companies collect that can become exposed to government access.

Given these sentiments and parliamentary support

for putting a sunset on the Safe Harbor framework, the Commission was under pressure to get out its report. That report, issued last December, declared that "due to deficiencies in transparency and enforcement … specific problems still persist and should be addressed," but were not as aggressive as might have been feared. A key element of these recommendations is increasing accountability, and few would debate that companies that make commitments to the Safe Harbor principles should comply with such commitments. Since the issuance of this report, the FTC and Department of Commerce have met several times with DG-Justice on updating Safe Harbor and made good progress to meet the recommendations. Perhaps the most difficult issue is dispute resolution mechanisms, where DG-Justice wants the FTC or Commerce Department to mediate (as a panel of European data protection authorities does in many instances), a role the U.S. agencies believe should be left to nongovernmental entities like the Better Business Bureau.

Looming over the Safe Harbor discussions is the European desire for a form of administrative or judicial redress for Europeans in the context of data collected under TFTP, Passenger Name Records, and other agreements involving the sharing of law enforcement data. Indeed, the DG-Justice Safe Harbor recommendations had almost as much to say on these issues as on Safe Harbor itself. It is difficult to disentangle the law enforcement and surveillance discussions because they have unavoidable impacts on each other. But, just as DG-Justice has only indirect involvement in these issues, there is little the FTC or Commerce Department can do on these fronts, both because they fall under law-enforcement-led discussions with the EU of an "umbrella agreement" on data sharing and because, even in that context, a judicial remedy would require congressional action.

At the US-EU Summit in March, leaders committed "to strengthening the Safe Harbor Framework in a comprehensive manner by summer 2014, to ensure data protection and enable trade through increased transparency, effective enforcement and legal certainty when data is transferred for commercial purpose."[24] They also affirmed a commitment to resolving the issues on the law enforcement front. Consistent with this statement, a final outcome of the Safe Harbor discussions is expected sometime this summer.

Whenever that is done, it will surely precipitate further debate in Europe about the adequacy of Safe Harbor, since any revised agreement will need to go through a public consultation process and review by Parliament and leading member states. These processes undoubtedly will feed into the give-and-take on legislation and what it says about agreements like Safe Harbor.

TTIP NEGOTIATIONS. Discussion about what TTIP might accomplish with regard to data flows and privacy have tracked the ebbs and flows of the privacy conversation. In the run-up to negotiations, when that conversation was going moderately well and negotiating objectives

were being shaped, Trade Representative Ron Kirk and his successor Michael Froman, then still Deputy National Security Adviser, publicly suggested that TTIP should address "data flows."[25] In turn, voices on the European side objected to taking these issues up in TTIP as a U.S. effort to undermine European data protection standards. After Snowden, the shoe was on the other foot, as some Europeans began to call for injecting privacy into TTIP as a way of protecting European citizens from U.S. public or private surveillance; the Parliament's vote opposing any TTIP agreement that does not protect the data of EU citizens could be read as adopting such a position. Trade Commissioner Karel DeGucht, the EU's negotiator, ultimately has taken a defensive position, declaring that data protection is not up for negotiation.[26]

One promising avenue for building bridges is in the development of codes of conduct.

As a practical matter, given the scope of the issues and the differences in legal systems, there is a limited amount TTIP can accomplish on this front beyond simple reaffirmation of Safe Harbor. TTIP does provides a vehicle to address the Internet issues discussed below and related efforts to regulate where information and communications technology can be located; early in April, the United States Trade Representative issued its annual report of telecommunications trade barriers, which flagged proposals for a Europe-only cloud computing network or Internet as "a troubling new and potential trade barrier."[27] And a trade deal conceivably might reach agreement to build on Safe Harbor by increasing the interoperability of privacy systems and establishing mechanisms to do so.

One promising avenue for building bridges is in the development of codes of conduct. The White House consumer privacy blueprint calls for the adoption of codes of conduct to implement the Consumer Privacy Bill of Rights and designates the National Telecommunications & Information Administration of the Department of Commerce to work with industry and civil society stakeholders to develop voluntary, consensus codes of conduct. NTIA has facilitated one such code, on transparency for mobile apps, and has begun another multistakeholder process on facial recognition. The text adopted by the EU Parliament renews a provision that by its terms "encourages" adoption codes of conduct in specific areas to be approved by data protection authorities. The development of codes of conduct involving stakeholders on both sides of the Atlantic would expand the NTIA process and provide an avenue the EU to make concrete its encouragement of such codes.

THE GLOBAL INTERNET. European nations were aligned with the United States in resisting efforts at the 2012 Information and Communication Technologies World Congress led by Russia and China to bring global Internet governance under the aegis of the International

Telecommunications Union, a United Nations agency. On a number of occasions, EU nations and leaders have affirmed a commitment the global free flow of information and a limited role for states in the governance of the Internet led by a network of multistakeholder institutions.

The most disconcerting reaction to the Snowden disclosures is the degree to which important European voices have wavered in commitments to an open Internet."

The most disconcerting reaction to the Snowden disclosures is the degree to which important European voices have wavered in these commitments. Chancellor Angela Merkel lent support to the Parliament's call for some form of European Internet, expressing the desire to speak with French President Hollande about "about building a European communication network to avoid emails and other data passing through the United States."[28] Viviane Reding suggested the same, declaring that that European data must be "only stored in clouds to which EU data protection laws and European jurisdiction applies."[29]

The routing protocols and peering arrangements of the Internet are indifferent to borders and send information packets by diverse routes depending on the most efficient path at that instant. I know no Internet engineers who believe that a "European cloud" could be achieved without defeating advantages of cloud computing, or that a "European Internet" could be achieved without filters and firewalls like those of China's Great Firewall. Thus, these notions are antithetical to the open, universal, and nongovernmental Internet that Europeans claim they support. Indeed, Edward Snowden's fundamental argument in his public appearances, including those in Europe, has been that broad surveillance by democratic states sets a dangerous example for authoritarian governments; a European firewall would do the same. I expect that, when push comes to shove, liberal democracies in Europe will be unwilling to pay so high a price.

The recent Netmundial conference in Brazil is heartening in this regard. This conference was an outgrowth of President Dilma Rousseff's outrage at learning she had been a target of foreign intelligence collection and her call at the United Nations General Assembly for "multilateral" Internet governance (connoting multinational governmental institutions or alliances and a significant change from the "multistakeholder" structure that has grown up organically).[30] The statement of high-level principles that emerged, however, amounted to a rejection of multilateral governance, instead strongly affirming the multistakeholder, non-governmental institutions of the Internet.

The U.S. government understood the pitfalls and made the wise choice to embrace the

As Internet governance debate continues in other forums, the United States and likeminded stakeholders will need to maintain and expand engagement from the global Internet community.

Netmundial conference as an opportunity to build support for this form of governance. It demonstrated commitment to this approach by announcing ahead of the conference its intention to transition the Internet Corporation for Assigned Names and Numbers (ICANN), which administers Internet addressing functions, to international multistakeholder oversight. The United States was well-represented in São Paulo and worked effectively with allies from across the spectrum of stakeholders—including European governments.

In the end, however, the outcome was less a product of successful advocacy or strategy by the United States than of cohesion in the international Internet community. Indeed, the Brazilian Internet community became deeply involved in Netmundial and helped structure it as a genuine multistakeholder discussion in which governments were on a par with academics, companies, and civil society. That community also saw that Brazil's new Internet law, the *Marco Civil da Internet*—signed by President Rousseff at the opening of the conference with great flourish—did not include her provision requiring providers to locate facilities in Brazil. Netizens around the world can be effective when they perceive a threat to the Internet as they know it: U.S. policymakers got a lesson in that from online protests against the Stop Piracy Act and Protect Intellectual Property Act (SOPA-PIPA), as did Europeans from mass protests against the Anti-Counterfeiting Trade Agreement (ACTA).

As Internet governance debate continues in other forums, the United States and likeminded stakeholders will need to maintain and expand engagement from the global Internet community. To do so, the Administration will need to keep building its relationships in this space.

LESSONS FROM THE CONVERSATION

The national conversation that ensued after the Snowden disclosures has brought high-level attention to privacy and data collection—Presidential speeches and roundtables, numerous principals' meetings and other interagency reviews, and many hours of John Podesta's and other White House staff's time preparing their reports on big data, among other things. All this has helped to move the conversation with Europe to a better place than last summer; the President's January speech and extension of protections to foreign citizens was generally well-received in Europe, though regarded as one step.

Regaining trust for the United States and online institutions that emerged from the U.S. will

take continued high-level engagement. Data issues have been high on the agenda for the U.S. Mission to the EU and, with experience handling European affairs on the national security staff as well as in business in Europe, newly-installed U.S. Ambassador Anthony Gardner is well-equipped to deal with that agenda. But he and others on the ground within the EU will need ongoing air support from Washington. Subcabinet officials at the Commerce Department will continue to be engaged and the designation of Under Secretary of State for Economic Growth, Energy, and the Environment Cathy Novelli as that agency's Senior Coordinator for International Information Technology Diplomacy will elevate the level of engagement by the State Department, but getting the message across will take continued engagement at the highest levels.

In that engagement, here are a few lessons from what has worked up to this point.

Regaining trust for the United States and online institutions that emerged from the U.S. will take continued high-level engagement.

THE UNITED STATES SHOULD NOT BE DEFENSIVE ABOUT ITS PROTECTION OF PRIVACY. America has a good story to tell when it comes to privacy. In a real sense, privacy law has American origins: the Fourth Amendment and Due Process, the famous Warren and Brandeis article on *The Right to Privacy*, the 1974 Fair Information Practice Principles – these are all wellsprings of privacy protection not just in the United States but in Europe and elsewhere. The current legal protection of privacy in America has real strengths, and differences between it and the European approach are more a function of differences between our common law system and their civil code system than of differences in values. Just as the FISA regime was put in place response to address domestic surveillance and insure that American citizens are adequately protected, President Obama has taken the next step, assuring citizens around the world that they are adequately protected. Both sets of protections underscore that privacy matters to Americans. And repetition helps.

THE UNITED STATES SHOULD BE OPEN AND FORTHRIGHT ABOUT ITSELF AND ABOUT EUROPE. The most effective response to the Snowden disclosures has been more disclosure and engagement about surveillance authorities and practices. In his "exit interview" on NPR former NSA Deputy Director Chris Inglis said that in hindsight he wished the agency had been more transparent much earlier. That lesson was taken to heart last January when Alex Joel, Chief Civil Liberties Protection Officer for the Director of National Intelligence and an architect of many of the checks placed on NSA's use of its bulk collection, ventured to Brussels to the international Computers, Privacy & Data Protection conference. Providing clear

information about U.S. law enforcement surveillance and access to electronic records enables a conversation about practices in other countries. In the long run, especially in the wake of Presidential Policy Directive 28, the United States can stand up to that comparison.

THE UNITED STATES SHOULD STRENGTHEN ITS OWN PRIVACY PROTECTION. Part of being open and forthright is to recognize that notwithstanding the strengths of U.S. privacy protection, it has gaps. And a significant and growing part of our economy – most e-commerce and the exploding collection of data from an increasing array of devices – falls into these gaps. The report by the Podesta working group calls for advancing the Consumer Privacy Bill of Rights and preparing legislation for the President to send to Congress. Making this bill of rights legally enforceable by the Federal Trade Commission would provide a foundation of trust by establishing a set of broad principles for businesses and consumers. Trusted online brands have nothing to fear from consensus principles that are consistent with best practices that good stewards of data follow today. The experience with NSA's collection shows that trust is a necessary enabler of responsible data collection and use, because it is an antidote to fear.

IT'S ABOUT THE ECONOMY. In blunt statements that would have been inconceivable a few months earlier, Neelie Kroes, the EU Vice-President in charge of the "digital agenda," posted a comment on the World Economic Forum blog in December entitled "Europe needs data protection, not data protectionism." In it, she urged Europeans to be "mature about data" and "not sit like rabbits in the face of scandals." Europe will not be "connected, competitive, open and secure …if we run away from data."[31] The Safe Harbor framework is certainly a special arrangement Europe has with the United States, but it is not a gift to the United States. Rather, it is an accommodation with mutual benefits between two trading partners joined in a broad alliance and the world's largest trading relationship. Neither the United States nor the European Union can afford a transatlantic data war.

ENDNOTES

1 Jessica R. Nicholson and Ryan Noonan, "Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services," *Economics and Statistics Administration*, January 27, 2014.

2 Mathias Döpfner, "Why we fear Google," *Frankfürter Allgemeine*, April 17, 2014

3 Kenneth Bamberger and Dierdre Mulligan, "Privacy in Europe: Initial Data on Governance Choices and Corporate Practices," *George Washington Law Review*, Volume 81, Page 1529, September 20, 2013.

4 "Export.gov – U.S.-EU Safe Harbor Overview," *International Trade Administration*, December 18, 2013, http://export.gov/safeharbor/eu/eg_main_018476.asp.

5 "Restoring Trust in EU-US data flows - Frequently Asked Questions," *European Commission*, November 27, 2013.

6 "In the Matter of Motorola Mobility Limited Liability Corporation and Google Incorporated," *Federal Trade Commission*, July 24, 2013.

7 "In the Matter of Facebook Incorporated," *Federal Trade Commission*, August 10, 2012.

8 "U.S.-EU Joint Statement on Privacy from EU Commission Vice-President Viviane Reding and U.S. Commerce Secretary John Bryson," *Department of Commerce*, March 19, 2012.

9 "Consumer Data Privacy in A Networked World: A Framework for Protecting Privacy and Promoting Innovation in The Global Digital Economy," *White House*, February, 2012.

10 James Fontanella-Khan, "Washington Pushed EU to Dilute Data Protection," *Financial Times*, June 12, 2013; Jennifer Baker, "EU Data Protection Reform: Lead MEP In 't Veld Criticises Undue Lobbying by US Authorities," Vieuws, March 14, 2013, http://www.vieuws.eu/citizens-consumers/eu-data-protection-reform-lead-mep-in-t-veld-criticises-undue-lobbying-us-authorities/.

11 "Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the European Union and the United States," *U.S. Department of State*, December, 2012.

12 Daniel Castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry," *ITIF*, August 5, 2013.

13 James Staten, "The Cost of PRISM Will Be Larger Than ITIF Projects," *Forrester Research*, August 14, 2013.

14 Peter Singer and Ian Wallace, "Big Bets and Black Swans 2014: Secure the Future of the Internet," Brookings Institution Press, January 25, 2014.

15 Viviane Reding, European Parliament Committee on Civil Liberties Justice and Home Affairs, October 9, 2012, http://www.europarl.europa.eu/ep-live/en/committees/video?event=20121009-1500-COMMITTEE-LIBE, Timecode 15:53:18.

16 "Informal Justice Council in Vilnius," *European Commission*, July 19, 2013.

17 "European Council Conclusions," *European Council*, October 25, 2013.

18 "On the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs," *European Parliament*, February 21, 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//EN.

19 "Amendment 5 US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Impact on EU Citizens' Fundamental Rights," *European Parliament*, 3 May, 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+AMD+A7-2014-0139+005-011+DOC+PDF+V0//EN.

20 Jennifer Baker interviews Viviane, "Reding, Safe Harbor: Reding warns US that progress is needed before sum-

mer" *EU Views*, March 26, 2014, http://www.vieuws.eu/ict/safe-harbor-reding-warns-us-that-progress-is-needed-before-summer/.

21 Charlie Rose Interviews President Obama, June 16, 2013, http://www.charlierose.com/watch/60230424.

22 Barack Obama, "Remarks by the President on Review of Signals Intelligence," *White House*, January 17, 2014.

23 "Big Data: Seizing Opportunities, Preserving Values," Executive Office of the President May, 2014.

24 EU-US Summit: Joint Statement, 26 March 2014. <http://www.whitehouse.gov/the-press-office/2014/03/26/eu-us-summit-joint-statement>

25 "Press Briefing Via a Conference Call with US Trade Representative Ron Kirk and Deputy National Security Advisor Michael Froman," *Office of the United States Trade Representative*, February 13, 2013

26 "Stepping up a Gear: Press Statement by EU Trade Commissioner Karel De Gucht following the Stocktaking Meeting with USTR Michael Froman on the Transatlantic Trade and Investment Partnership (TTIP)." *European Commission*, 18 February, 2014.

27 "USTR Targets Telecommunications Trade Barriers," O*ffice of the United States Trade Representative*, May 8, 2014.

28 "Merkel and Hollande to Lay Foundation of 'protected' EU Internet," *EurActiv*, February 17, 2014.

29 Danny Hakim, "Europe Aims to Regulate the Cloud," *The New York Times*, October 6, 2013.

30 Dilma Rousseff, *UN General Assembly*, 24 September 24, 2013.

31 Kroes Neelie, "Europe Needs Data Protection, Not Data Protectionism," World Economic Forum Blog, December 4, 2014, http://forumblog.org/2013/12/europe-needs-data-protection-not-data-protectionism/.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
brookings.edu/governance.aspx

Editor
Joshua Bleiberg

Production & Layout
Beth Stone

EMAIL YOUR COMMENTS TO GSCOMMENTS@BROOKINGS.EDU