TRANSATLANTIC DIGITAL DIALOGUE

Rebuilding Trust through Cooperative Reform

G|M|F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

stiftung | neue verantwortung

Please direct inquiries to:

The German Marshall Fund of the United States
1744 R Street, NW
Washington, DC 20009
T 1 202 683 2650
F 1 202 265 1662
E info@gmfus.org

The Transatlantic Digital Dialogue was supported by a grant from the German Federal Foreign Office.

This publication can be downloaded for free at http://www.gmfus.org/listings/research/type/publication.

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF contributes research and analysis and convenes leaders on transatlantic issues relevant to policymakers. GMF offers rising leaders opportunities to develop their skills and networks through transatlantic exchange, and supports civil society in the Balkans and Black Sea regions by fostering democratic initiatives, rule of law, and regional cooperation. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

About stiftung neue verantwortung

The stiftung neue verantwortung (snv) is a Berlin-based non-profit think tank that brings together expertise from politics, research institutions, NGOs and businesses in order to foster the development, discourse, and publication of non-partisan policy proposals to address current political debates. The policy research at snv is organized around three central themes: Digitalization, Energy and Resources, as well as the Future of Government. The snv produces analysis, publishes policy recommendations, and builds inter-sectoral coalitions. The goal is to combine the knowledge and experience of governmental, business, academic, and civil-society stakeholders in order to inform and co-create policy solutions. The independent approach of the snv is made possible by a mix of funding from non-profit foundations, public institutions, and businesses as well as oversight by a diverse and representative board of directors.

Transatlantic Digital Dialogue

Rebuilding Trust through Cooperative Reform

November 2015

Executive Summary 2
Framework of Deliberation 4
Oversight and Transparency 6
Extraterritorial Access to Data 10
Cyber-Security Cooperation and Strong Encryption. 16
Conclusion 19
Appendix 20

Executive Summary

The Transatlantic Digital Dialogue is a multi-stakeholder working group of experts from Germany and the United States. It was assembled and stewarded by the Stiftung Neue Verantwortung and the German Marshall Fund of the United States to develop a constructive agenda for the modernization of privacy/security policy that begins to address the global debate over digital surveillance.[1] The findings presented here are rooted in three convictions shared by all of the participants in the project: 1) that transatlantic relationships have weakened as a result of the fractious and inconclusive debate between the EU and the U.S. over surveillance practices; 2) that a multinational modernization of a rights-based framework for privacy and security policy is needed to address these challenges; and 3) that solutions should be aligned with principles of human rights, responsive to the complex political economy of surveillance policy, and premised on common interests and values.

The Transatlantic Digital Dialogue presents this report as a framework of analysis for re-building trust and democratic legitimacy in the transatlantic relationship in cyberspace. The agenda we present here offers three areas of policy recommendations with clear opportunities for reform. In some cases, the primary objective is a bilateral or multilateral agreement on international standards of practice. In some cases, the focus is more specifically on harmonizing domestic law around a common framework.

1) *Oversight and Transparency* — In order to restore trust and legitimacy to the law governing surveillance practices in all security services, standards for authorization, oversight, and transparency need to be modernized. In this area, the U.S. government has published several expert reviews and enacted practical reforms that could serve as the baseline for a new framework for both sides of the Atlantic. Most important here are new restrictions on the scope of authorized data collection, transparency in decision-making, and stronger independent review. To inform what new elements a transatlantic framework might include, we conclude that reform proposals under consideration in the German Parliament would represent groundbreaking steps toward strengthening democratic oversight. At the center of this proposal are a major expansion in the judicial review of surveillance authorization and greatly increased capacity for oversight bodies. These initiatives on both sides of the Atlantic call for a greater exchange of ideas and could position Germany and the U.S. as global leaders in the development of new international standards for oversight and transparency.

2) *Extraterritorial Access to Data* — National laws and international agreements regulating government access to commercial data, such as Mutual Legal Assistance Treaties, have failed to adapt effectively to technology development on the Internet. As the recent EU court ruling on data exchange with the U.S. shows, there are divergent views on the alignment of law and technology. Consequently, there is an urgent need to resolve conflicting national laws by developing common rules among countries for how law enforcement practices in one nation will apply to the data of citizens from other nations. Both government and businesses need a clear framework for how to handle requests for legitimate access to user data.

[1] Participants are listed in the appendix of this report. All of the participants in this working group contributed ideas, analysis, and intense deliberation to this process. This report is a summary of the discussion and conclusions of the working group sessions prepared by rapporteurs in the hosting institutions. However, participation by a company, institution or individual in the working group does not imply endorsement of any particular proposal or statement in this report.

And citizens deserve to know how and when the law is applied. The existing agreements on law enforcement cooperation — including the Budapest Convention on Cybercrime, the EU system for law enforcement coordination, and the newly signed U.S./EU Umbrella Agreement — could provide a useful foundation for this process of harmonizing policy. However, both sides must agree to modernize standards for which laws will apply when, how, and to whom.

3) *Cyber-Security and Strong Encryption* — Both the United States and European Union share an interest in establishing stronger frameworks for collaboration in cyber-security to protect critical infrastructure and data assets from cyber-attack and espionage. Technologists argue that strong cryptography is crucial to protect communications from digital assailants with increasing sophistication. Thus many experts in the U.S. and Germany regard strong encryption as a central element of cyber-security. The German government in particular has made commitments to strong encryption that — if adopted by the United States — could serve as the trust anchors for the cooperative development of new transatlantic systems of secure communications. We conclude that a common position on strong encryption creates the basis for more collaboration on a variety of issues from security certification standards to threat intelligence to protection against cyber-crime and industrial espionage.

Taken as a package of issues, there is a symmetry of corresponding strengths and weaknesses between the two countries. A focused bilateral engagement could seek to set standards based on the strengths of each side and in so doing raise the quality of policy for both as well as establish a model for other nations to follow in their own modernization efforts. The bilateral engagement between the United States and Germany is a test case in this regard for the possibility of broader agreement at the EU level (both within the EU and between the EU and the United States).

The discussion and recommendations provided here reflect the views of the working group that restoring trust in transatlantic digital practice will require policies drawn from principles of human rights, civil liberties, security, and the rule of law. Moreover, we emphasize that the controversy over security and privacy policy has strong economic components as well — with costly consequences for both the United States and the EU if they remain unresolved. Although we expect there will long remain areas of disagreement between the United States and Germany (as well as the broader European Union), these will be vastly outweighed by common values and common interests. The more constructive the policy engagement and cooperation we can build in the areas where we agree, the more likely it is we will be able to address those areas where we do not.

The discussion and recommendations provided here reflect the views of the working group that restoring trust in transatlantic digital practice will require policies drawn from principles of human rights, civil liberties, security, and the rule of law.

1 Framework of Deliberation

The central political issue is the expectation of data privacy rights and an apparent divergence of values over the rights-based limits on surveillance for security purposes. This is not only about the scale of data collection enabled by modern technology, it is also about the norms of legitimacy and the enforcement of laws governing surveillance.

In the course of the debate over rights, liberties, and security in the two years since the Snowden disclosures, public opinion and national politics in Europe and the United States have been sharply divided. While the initial outrage over U.S. surveillance activities in Europe has largely passed, it is clear that the breach of trust will pose an enduring challenge for transatlantic cooperation. The relationship rests on decades of close alignment and partnership, but in cyberspace this alliance is now fraught with concerns that will not easily be resolved. These concerns are about the U.S. surveillance practices that continue (relatively unabated) despite the political debate; but they are also about the consequences of Europe's response to those practices. In some ways, the current challenges reflect a broader strategic and historical context in which the United States has taken a more offensive approach to cyber-capabilities while the EU has focused on strengthening its internal security.

The central political issue is the expectation of data privacy rights and an apparent divergence of values over the rights-based limits on surveillance for security purposes. This is not only about the scale of data collection enabled by modern technology, it is also about the norms of legitimacy and the enforcement of laws governing surveillance. These critiques are directed at governments in the EU as well as in the United States, particularly as the extent of transatlantic cooperation between security services becomes more evident. The gap between the growing power of digital technology and the inadequacy of existing laws to contain it has emerged as a common theme on both sides of the Atlantic. However, the size and scope of U.S. capabilities revealed in the Snowden documents focuses most of the attention on Washington.

This debate has led to a variety of proposals in Europe to push back on U.S. surveillance. Several of these have fostered a second set of concerns shared by both U.S. and EU stakeholders. Some of the policy responses contemplated in European capitals would decisively change the markets for transnational data flow, the architectures of distributed computing, and the legal regimes that govern them within and between countries. For example, the recent decision from the European Court of Justice invalidates existing agreements for transatlantic data flow and demands modernization.[2] This ruling creates renewed urgency for negotiating new agreements and revisiting a discussion about norms. Embedded in any such reform process are high-level disagreements over the application of international law, violations of sovereignty, and the appropriate criteria to legitimize surveillance as necessary and proportionate in democratic nations. Both the critique of current surveillance practices and the proposed reactions to them boil down to deep concerns about how the laws governing surveillance on one side of the Atlantic will treat the rights of citizens on the other.

Despite the intensity of the debate, the most significant reforms of U.S. surveillance practice enacted in the last two years have not directly addressed the core issues in the dispute with the EU. However, neither the EU or any member states have taken major countermeasures against the United States — though this may change in the wake of the court decision on transatlantic data flows. Meanwhile, the impact of the distrust is felt in market distortions and in an increasingly cynical public opinion. The most recent Transatlantic Trends survey of the German Marshall Fund reported a "cooling" relationship between Germany and the United States since 2013. From 2013 to 2014 the approval rating of President Obama in Germany fell by 20%. At the same time, the share of German respondents who called for a

[2] Court of Justice of the European Union. Case C-362/14. *Maximillian Schrems v Data Protection Commissioner.* October 6, 2015.

more independent approach in the transatlantic relationship rose from 40% to 57%.3 And while the transatlantic alliance proceeds with business as usual in many respects, the signs of fracture over data policy appear consistently — for example in the public debate over the Transatlantic Trade and Investment Partnership.4 The lack of interest in Washington and the impotence of Europe to produce a viable reform agenda deepens a normative pessimism about the Internet that will be difficult to reverse, if it remains unaddressed. Organized efforts within civil society and business on both sides of the Atlantic have begun seeking change in the courts and in market practice — as well as before legislatures. Meanwhile, the discussions between governments on surveillance policy have gone relatively quiet.

The United States and Europe need to reboot a common strategy for the Internet — a harmonization of foreign policy through parallel domestic policy change. Quiet acquiescence to the status quo will not suffice to realign interests and bridge the divides that have opened in the last two years. The United States and the EU will benefit from a resolution both politically and economically. But conversely, political leaders on both sides are wary of the political risks involved and the consequences of trying and failing. This project seeks to assemble the voices of civil society, academia, and business from the United States and Germany to serve as a catalyst for this necessary engagement. We intend here to set an agenda of constructive policy recommendations that unite the United States and the EU around common interests while achieving reform of data privacy/security policy.

We start from the premise that modernizing data policy for the digital age must begin with the human rights and civil liberties that embody our democratic values. These principles must be applied in practice in ways that support security interests without being eclipsed by them. Herein lies the essence of democratic legitimacy — the assurance that the power of the state will be applied judiciously, with transparent adherence to the law, and within the constraints of liberal social values. Further, we recognize that the practice of security policy in the digital age necessarily implicates economics. The owners of most digital networks and the controllers of most of the world's data are private companies. And sustaining the growth of digital commerce (which requires restoring trust in secure communications) is a strong transatlantic interest, joined as we are by a multi-national supply chain and networked global markets.

The stakes of these debates are therefore very high — testing our commitments to democratic principles, public safety, and economic prosperity. These challenges will not be solved quickly — and they will not be solved by governments alone. We believe the inclusion of multi-stakeholder participants in these dialogues and a transparent process of deliberation will give governments impetus to act, strengthen the quality of proposed solutions, and achieve that which has eluded us for over two years — progress toward common goals. Therefore, we present this analysis and policy agenda with the intention to initiate a reform process around the three major issues of oversight/transparency, extraterritorial access to data, and cyber-security and encryption, which combine political, economic, and social interests at the center of the transatlantic relationship.

The United States and Europe need to reboot a common strategy for the Internet — a harmonization of foreign policy through parallel domestic policy change. Quiet acquiescence to the status quo will not suffice to realign interests and bridge the divides that have opened in the last two years. The United States and the EU will benefit from a resolution both politically and economically.

[3] German Marshall Fund of the United States. 2014. "Transatlantic Trends: Key Findings 2014." p23-24. http://trends.gmfus.org/files/2012/09/Trends_2014_complete.pdf

[4] Jeremy Fleming. 2013. "TTIP: Data is the elephant in the room." *EurActiv.* http://www.euractiv.com/specialreport-eu-us-trade-talks/ttip-data-elephant-room-news-530654 ; European Parliament. 2015. "TTIP: Trade agreements must not undermine EU data protection laws, say Civil Liberties MEPs." *Civil Liberties Committee.* http://www.europarl.europa.eu/news/en/news-room/content/20150330IPR39308/html/TTIP-Trade-agreements-must-not-undermine-EU-data-protection-laws-say-MEPs

2 Oversight and Transparency

Summary

Germany and the United States should use the work of this Dialogue as a starting point to develop best practices regarding the structure and methods of oversight and transparency. These policies hold security agencies to the standards, criteria, and procedures under which domestic laws authorize surveillance and restrict the operation of such programs. Oversight and control over the application of "digital power" are critical for restoring legitimacy in the public eye. In both the European Union and the United States, there are structural weaknesses in the legal systems for authorization and review of surveillance practices because the laws and institutions established to govern these powers predate the advent of digital technology. Technical expertise is often in short supply; resources are insufficient to provide for meaningful accountability; and transparency is avoided in pursuit of efficacy and secrecy.

The most significant public policy reforms in the post-Snowden era have been initial steps to address these problems. We find that contrary to popular representation, U.S. laws on oversight of surveillance contains myriad constraints on the security services. And while they may be considered modest in impact, they are more comprehensive than similar laws in Germany. Further, the Obama administration has expanded these oversight provisions to tighten restrictions on authorization and operation of surveillance practices as well as to increase transparency. None of these reforms has yet been pursued in Europe. However, the German government is debating a set of procedural reforms that would set a new global standard for democratic oversight of surveillance programs.[5] We conclude that these efforts represent an alignment of interests and should function as a basis of further modernization and subsequent harmonization of law governing surveillance practices across all security services — including intelligence agencies.

In both the European Union and the United States, there are structural weaknesses in the legal systems for authorization and review of surveillance practices because the laws and institutions established to govern these powers predate the advent of digital technology. Technical expertise is often in short supply; resources are insufficient to provide for meaningful accountability; and transparency is avoided in pursuit of efficacy and secrecy.

Discussion

Pragmatic discussions over domestic legal reform in both the United States and Germany have focused on issues of standards, oversight, and transparency of digital surveillance programs. Among the commitments in Presidential Policy Directive 28 (the Obama administration's formal response to the Snowden debate), the White House ordered U.S. intelligence agencies to improve standards of transparency, internal oversight and accountability.[6] The White House Review Group[7] and the Privacy and Civil Liberties Oversight Board[8] have been only the most prominent of numerous expert inquiries offering sharp critique and practical recommendations for reform on procedural issues. These reforms are also core components of the USA Freedom Act — the legislation signed into law by U.S. President Barack Obama in June 2015.[9] For example, the USA Freedom Act creates a panel of experts on privacy, civil liberties, and technology to offer consultation and guidance to the FISA Court (the panel of judicial review for surveillance authorized by the Foreign Intelligence Surveillance Act). The new law

[5] Georg Mascolo. 2015. "Dem BND droht eine Revolution." *Süddeutsche Zeitung*. http://www.sueddeutsche.de/politik/bundesnachrichtendienst-unter-freunden-1.2679411

[6] The White House. 2014. "Presidential Policy Directive — Signals Intelligence Activities." https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

[7] The White House. 2013. "President Obama's Meeting with the Review Group on Intelligence and Communications Technologies." https://www.whitehouse.gov/the-press-office/2013/12/18/president-obama-s-meeting-review-group-intelligence-and-communications-t

[8] Privacy and Civil Liberties Oversight Board. https://www.pclob.gov/about-us.html

[9] USA Freedom Act. H.R. 2048. http://judiciary.house.gov/index.cfm/usa-freedom-act

requires the declassification of FISA Court opinions that contain novel interpretations of law, including the defined scope of search terms. These procedural reforms are important and could serve as a model for parallel efforts in Europe.

In Germany, oversight and transparency are central themes in the debate over surveillance. Ironically, the German parliamentary investigation into the National Security Agency (NSA) has uncovered little new information about the NSA, but a great deal about the cooperation of the German intelligence agency (BND) with the NSA. Many of the critiques leveled at BND practices focus on oversight and accountability. Warnings about the inadequacy of the oversight mechanisms in Germany have come directly from the members (past and current) of the oversight bodies (G10 Commission and Parliamentary Control).[10] In addition, prominent legal scholars and former judges have concluded that the application of surveillance policies on non-citizens is likely unconstitutional.[11] Finally, scrutiny of the cooperation between the BND and the NSA (now a central issue in the German debate) is fundamentally concerned with whether these programs were properly authorized and reviewed.[12] At issue is the legitimacy of surveillance programs that operate with the imprimatur — but not the reality — of informed and competent oversight.

In the last months, the German government has begun a serious debate about whether to take steps to set the world's highest standard of surveillance oversight.[13] In response to the work of the Inquiry Committee, the Social Democratic Party (the coalition partner of the ruling Christian Democrats in the current government) published a policy paper outlining a reform agenda.[14] Central elements of the proposal focus on a broad expansion of the capacity in the authorization and oversight of BND surveillance. Some parliamentary leaders have called for quasi-judicial review of all surveillance programs, including the foreign-to-foreign communications that do not currently require external authorization. Increased oversight and transparency is seen as a direct path back to legitimacy. Thus far, these efforts have not resulted in a legislative draft, but that is expected either later this year or in 2016. Representatives from both parties in the coalition government are still negotiating main components of the reform. They have already agreed to strengthen parliamentary oversight. The parliamentary oversight committee will be supported by a commissioner with staff consisting of legal, data protection, and technical experts who will be responsible for examining any aspect of the work of the intelligence agencies on behalf of the parliament. Other issues such as a broader application of constitutional privacy protections and higher standards for the authorization and review of surveillance programs are more controversial and still hotly debated.

Recommendation

The similarities between the German and U.S. systems of legal authorization for surveillance —

[10] Berthold Huber. 2013. "Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite." *Neue Juristische Wochenschrift 2013.* p. 2572

[11] Matthias Bäcker. 2014. "Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes." *Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014.* https://www.bundestag.de/blob/280844/35ec929cf03c4f60bc70fc8ef404c5cc/mat_a_sv-2-3-pdf-data.pdf

[12] Stefan Wagstyl. 2015. "Revelations of role in spying on allies turn tables on Berlin." *Financial Times Europe.* http://www.ft.com/cms/s/0/3bf16734-fd5d-11e4-b072-00144feabdc0.html

[13] Georg Mascolo. 2015. "Dem Bundesnachrichtendienst droht eine Revolution." *Süddeutsche Zeitung.* http://www.sueddeutsche.de/politik/bundesnachrichtendienst-unter-freunden-1.2679411

[14] SPD-Bundestagsfraktion. 2015. "Rechtsstaat wahren – Sicherheit gewährleisten!." http://www.spdfraktion.de/sites/default/files/2015-06-16-eckpunkte_reform_strafma-r-endfassung.pdf

The similarities between the German and U.S. systems of legal authorization for surveillance — and the parallels in the oversight structure — open an opportunity for working on common types of reform proposals. Drawing from the ideas and actions of the Obama administration as well as the current debate in the German parliament, the options on the table are already very significant.

and the parallels in the oversight structure — open an opportunity for working on common types of reform proposals. Drawing from the ideas and actions of the Obama administration as well as the current debate in the German parliament, the options on the table are already very significant. The two governments should explore a variety of proposals for the improvement of oversight as a means to limit surveillance and to reestablish public legitimacy. These could include:

- Governments should publish an official interpretation of legal authority under specific statutes to authorize specific types of surveillance. This should include a list of the delimited purposes for which surveillance is authorized. It should identify the procedural/operational restrictions on authorized surveillance programs. And it should clarify the requirements for reporting to oversight bodies, the rights/duties of those oversight bodies, and the mechanisms for correcting noncompliant practices. Even if this publication represents no change to existing practices, the act of codification is beneficial because it establishes an opportunity for public evaluation.
- The institutions of authorization and oversight of surveillance programs should receive substantial increases in the size of staff and budget allocations. In particular, decision-makers should have access to technologists, attorneys, and analysts (with appropriate security clearances) sufficient to evaluate fully the claims made by the requesting agency concerning the necessity and proportionality of a particular surveillance operation.
- Governments should create/enhance mechanisms for permanent, independent oversight. These might include examples such as the Privacy and Civil Liberties Oversight Board in the United States or the commissioner for the oversight of security services proposed in Germany. The professionalization and maintenance of oversight activities that inform policy decisions will support evolving reform over time.
- Authorization and oversight proceedings should include adversarial counsel so that decision-makers may hear views independent of those offered by the government.
- Governments should set and implement public standards for the publication of all non-classified elements of authorizing decisions and oversight reports — including the numbers of errors in the minimization process. In particular, all novel interpretations of law in the authorizing process should be available for public review (with appropriate redactions for sources and methods). Elements of these standards were codified in the USA Freedom Act.[15]
- Governments should require regular public reporting by all public agencies (and strongly encourage the practice in the private sector) about the number, type, and purpose of interception requests, the number of people/communications affected, as well as the criteria cited to authorize surveillance.
- Governments should have explicit and published restrictions/rules on intelligence acquisition from foreign agencies in order to respect national laws. Raw intelligence may not be accepted from a partner country that would have been illegal to gather at home, and vice versa.

[15] USA FREEDOM Act of 2015. TITLE VI: FISA Transparency and Reporting Requirements. Section 602.

- Governments should define public standards for the rights of non-citizens subjected to surveillance programs. Ideally these standards should be identical to those offered to citizens. However, if there is differentiation, that should be explicit in the law.
- Governments should establish an effective form of judicial (or quasi-judicial) review of *all* surveillance requests evaluated against the same rights-based standard and interpreted on necessary/proportionate criteria.
- Governments of allied countries that share intelligence and defense resources should initiate inter-parliamentary dialogue between oversight committees of surveillance programs. These exchanges should be designed to share best practices and to anticipate emerging problems.

If a number of these policies were implemented by countries on both sides of the Atlantic, this would represent a major reform of surveillance policy. It would also mark significant progress toward addressing the issue of adequate fundamental rights protections identified in the ECJ decision on Safe Harbor. What we propose here is that the starting point for bilateral engagement is to identify a baseline of practices that already exist in at least one country, engage directly on common incremental reforms, and contemplate a path forward to systematic change and harmonization of standards for authorization, oversight, and transparency.

3 Extraterritorial Access to Data

The problem of access to data is a fundamental one for U.S.- EU economic relations. Firms on both sides of the Atlantic routinely share data within corporate subsidiaries, to vendors, suppliers, and customers. Moreover, in modern cloud computing architectures, data may not be exclusively stored in one location — but rather in many locations.

Summary

Germany and the United States should explore a bilateral (or multilateral) framework to regulate governmental access to extraterritorial commercial data for legitimate law enforcement purposes.[16] This framework should first seek to address two problems.

The first is Europe's concern that U.S. law enforcement may access the data of European citizens (even when on servers located in Europe) by presenting a U.S. company with a lawful order. The criteria for this warrant are a matter of U.S. law. Notification (much less preauthorization) to the European government is not required. The result is often a conflict between national laws that puts the data-holding company in a difficult position and triggers calls for the localization of data storage and routing. The central question here is how to harmonize the laws from different countries that govern the legitimate interception or retrieval of data associated with a particular end user, originating from a particular location, regarding a national or transnational law enforcement investigation.

The second problem is in some ways the reverse of the first. EU law enforcement authorities seeking access to the data held by U.S. firms (on servers in the United States) must proceed through MLATs (Mutual Legal Assistance Treaties). These require a process of coordination with U.S. law enforcement to reach the data-holding company. The critique of this system is that it is far too slow and overwhelmed by the quantity of requests. This leads to pressure for data localization and a short circuit of the MLAT process by companies that in theory should require an MLAT proceeding (because data is stored abroad) but in practice do not. Substantial reforms to the MLAT process — or its replacement — will be required to resolve the problem.

The rules governing national law enforcement agencies' access to the data of foreign citizens require urgent reform. Both government and businesses need a clear framework for how to handle requests for legitimate access to user data. And citizens deserve to know how and when the law is applied. The following questions are at the center of the reform effort. What are the circumstances under which transnational data is determined to be subject to the national law of one country versus another? What laws apply to data that is stored outside of the jurisdiction of governments that seek access to it? When and how should law enforcement agencies be permitted to access the data of foreigners? What are the criteria deemed legitimate to grant that access?

The problem is a fundamental one for U.S.-EU economic relations. Firms on both sides of the Atlantic routinely share data within corporate subsidiaries, to vendors, suppliers, and customers. Moreover, in modern cloud computing architectures, data may not be exclusively stored in one location — but rather in many locations. For many companies, it is no longer accurate or relevant to discuss a single location for particular data as the trigger for engagement of a specific national legal regime. As these technologies develop further, it will become more and more urgent to define a common legal regime between countries. Otherwise, we should expect to see the nationalization of cloud infrastructures to optimize for security interests at the expense of technical

[16] In this section, we are explicitly excluding the governance of signals intelligence (SIGINT) collection from this recommendation. This not because the problem does not apply to SIGINT. However, intelligence agencies are governed by different legal regimes in this respect. And we conclude nations are unlikely in the near term to reach bilateral or multilateral agreement on *transparent* standards for data privacy restrictions applied to extraterritorial access to data by intelligence services. By contrast, law enforcement cooperation has a clear precedent. However, we strongly encourage the United States and Germany (and other nations) to discuss a similar type of agreement with respect to SIGINT through appropriate channels.

innovation, commercial efficiency, and the free flow of information.

To avoid this balkanization of the Internet infrastructure, nations will require a functional set of standards to govern extra-territorial access to data. We find that the EU has an existing system of law enforcement coordination that — while imperfect and in need of improvement— could serve as a baseline for transatlantic reform. In addition, the Budapest Convention on Cybercrime offers a decade of cooperation in related practices. Furthermore, the recently signed "Umbrella Agreement" — setting the terms for US and EU law enforcement data exchanges — offers another avenue to develop constructive, harmonizing reforms.[17] However, there remains much work to be done.

Discussion

We are now experiencing an international legal, commercial, and moral dispute over whether and how global IT companies must respond to the legal requests from one government for data stored in an international location and/or belonging to an international customer. The debate has two key elements — 1) clarity/legitimacy in the laws that apply; and 2) effective procedure for the transparent implementation and enforcement of the law.

The problem of legitimacy in the laws that apply to extraterritorial data access begins with asymmetry in the global digital market of data storage and processing. The simple fact is that a small number of American companies control a vastly disproportionate quantity of global data than any other nation. As a result, the U.S. government has access to much of this data through lawful court orders issued to these U.S. companies. U.S. courts have also held that US companies are compelled to provide data to law enforcement even if it is stored abroad, provided they have technical access to it. This requirement holds irrespective of whether doing so violates the law of the country in which the data is stored and absent any notification of the foreign law enforcement authorities. (This interpretation of the law is currently being challenged.[18] And some argue that companies can evade this requirement by structuring foreign operations as independent subsidiaries.[19]) This asymmetric access of U.S. law enforcement to the data of foreigners is seen by other countries as a challenge to their sovereignty and a violation of domestic law. They have no role in the compulsion of data that belongs to their own citizens; they have no influence over the criteria used to judge the law enforcement purpose for the data request; and they have no recourse in U.S. courts.

The implications of these circumstances were amplified in the public eye by the Snowden disclosures. The consequent debate fueled a push to reach an agreement — at least on the law enforcement issues, if not the intelligence agencies — between the EU and the United States to settle some of the issues involved. The result was the so-called Umbrella Agreement. This agreement offers a new baseline of transatlantic rules and expectations for law enforcement access to data. However, it only applies standards of privacy

The debate over access to data held by companies has two key elements: clarity/legitimacy in the laws that apply and effective procedure for the transparent implementation and enforcement of the law.

[17] European Commission. 2015. "Agreement between The United States of America and The European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses." http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf

[18] This interpretation of the law is currently being challenged by Microsoft in a high profile case in the United States Court of Appeals for the Second Circuit, see: Alex Ely. 2015. "Second Circuit Oral Argument in the Microsoft-Ireland Case: An Overview." *Lawfare.* https://www.lawfareblog.com/second-circuit-oral-argument-microsoft-ireland-case-overview

[19] For an interesting analysis of this question of separate legal entities, see: Orin Kerr. 2015. "Does it matter who wins the Microsoft Ireland warrant case?" *The Washington Post.* https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/07/23/does-it-matter-who-wins-the-microsoft-ireland-warrant-case/

Harmonizing transatlantic data protection rules is a complex enterprise because it involves the interaction of laws that apply to commercial entities, law enforcement agencies, and intelligence services. The system established by the U.S. and EU for commercial data protection rules — Safe Harbor — essentially came undone before the Court because of the methods of U.S. government access to commercial data.

protection to data exchanged between U.S. and EU law enforcement authorities; and it does not focus on the reach of U.S. warrants to foreign data via U.S. companies. Further, recent legal analyses of the Umbrella Agreement have presented a strong critique that the new rules do not meet EU standards of data protection.[20] The need to address this gap has been highlighted by the recent European Court of Justice decision that effectively invalidates the Safe Harbor agreement governing commercial data exchange with the United States. The ruling emphasizes that data transfers between the EU and the US can only occur if U.S. law meets the EU standards of protection of fundamental rights.

To be clear, the violations of rights cited by the Court involve a mix of laws and practices in the United States that the judges found insufficient. These include both law enforcement access to data and surveillance by national security agencies. We expect that the issues of law enforcement and intelligence agency data collection will be addressed separately. However, a common framework for law enforcement access to data (governing data exchanged between agencies as well as foreign data acquired via a domestic company) would constitute a significant step forward. We do not underestimate the significance of the challenge to achieve even modest progress. According to a recent legal analysis prepared for the European Parliament, even if the U.S. government were to give Europeans the privacy protections granted to US citizens, these would still be insufficient to meet EU standards.[21]

Harmonizing transatlantic data protection rules is a complex enterprise because it involves the interaction of laws that apply to commercial entities, law enforcement agencies, and intelligence services. The system established by the U.S. and EU for commercial data protection rules — Safe Harbor — essentially came undone before the Court because of the methods of U.S. government access to commercial data. Under Safe Harbor, U.S. companies that do business in the EU can transfer data of European citizens to the U.S. for storage and processing, if they certify compliance with the Safe Harbor agreement. The Safe Harbor rules catalog the measures of privacy and security protection that must be provided for commercial data in the U.S. in order to meet EU standards. However, the Safe Harbor framework grants primacy for national security, public interest, or law enforcement requirements over the Safe Harbor principles. The Court of Justice of the EU ruled that such general exemptions are invalid as they provide no adequate protection of the fundamental rights of EU citizens from the U.S. government.

At the center of the Court's arguments about the violation of European rights are surveillance practices (revealed in the Snowden documents) conducted by U.S. national security agencies for intelligence collection purposes. However, the Court also cites problems with the rules governing law enforcement access to data. Though related, of course, these can be treated as separately addressable problems. For the purposes of the recommendations in this paper, we will set aside the SIGINT issues — even as we recognize their importance — and focus on the rules governing law enforcement access. With regard to the operation of their intelligence agencies, it seems questionable whether all members of the EU would meet the standards laid out by the Court with respect to other member states. A comprehensive resolution of the problem would require a multilateral

---

[20] Douwe Korff. 2015. "EU-US Umbrella Data Protection Agreement : Detailed analysis by Douwe Korff." European Area of Freedom Security & Justice http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/

[21] Franziska Boehm. 2015. *A Comparison Betwen US and EU Data Protection Legislation for Law Enforcement*, Prepared for the LIBE Committee, European Parliament, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf

agreement on rules for data collection and processing for national security purposes. Such an agreement requiring changes to domestic security policy does not seem feasible in the short term. However, a starting point would be the rules of the road governing extraterritorial access to data and the coordination of international law enforcement.

When it comes to the process of international law enforcement coordination, there is a long history with respect to accessing international communications data as a part of an investigation. In the telephone era, law enforcement data requests with targets outside the legal jurisdiction of a nation were coordinated through Mutual Legal Assistance Treaties (MLATs). In the Internet era, technology has changed faster than the law. The scale of data requests by law enforcement has expanded dramatically, and the traditional MLAT process is easily overwhelmed. These channels tend to be slow, intransparent, and cumbersome for all parties involved. In their current form, MLAT procedures are no longer viable instruments to coordinate law enforcement across borders. However, the function they were designed to serve is perhaps more relevant than ever before. And if it were reformed into an effective regime for law enforcement coordination, such a solution could help solve for the problem of extraterritorial access to data in this context by establishing common rules.

Recommendations

The objective of government engagement on these issues should be to establish a path to resolve at a bilateral (and ultimately multilateral) level how law enforcement requests for extraterritorial private sector data should be treated under the law. A successful transatlantic solution could establish a common policy to address these underlying issues.

Governments must coordinate and set common policies to determine how the law applies in circumstances with conflicting laws. The alternative (currently the status quo) is placing private sector companies in the position to decide for themselves which laws to honor and which to violate. This is poor policy, undemocratic, and unsustainable. This conflict should not be left to IT companies to adjudicate. Instead, it needs to be addressed and resolved on an inter-governmental level to restore legitimacy and trust. In part, this problem must be solved through coordination and notification among governments. But, it will likely also require a harmonization of national standards and criteria for when law enforcement access to data is deemed legitimate under the law. One approach is represented in the LEADS Act— a bill introduced in the U.S. Senate that would permit U.S. law enforcement to reach content outside the United States (with a lawful warrant) only if the data is in an account held by a "U.S. person" (defined as a U.S. citizen or permanent resident).[22] If the account is held by a non-US person, the US law enforcement agency would have to comply with the laws of the country where the data resides via an MLAT (the bill also provides for streamlining that procedure from the US side). There are very legitimate concerns about the bill, and it will likely undergo significant change if and when it moves through the Congress.[23] However, its introduction highlights support for a solution in Washington from a bipartisan group of lawmakers and a host of business and civil society interests.[24]

In the Internet era, technology has changed faster than the law. The scale of data requests by law enforcement has expanded dramatically, and the traditional Mutual Legal Assistance Treaties process is easily overwhelmed. These channels tend to be slow, intransparent, and cumbersome for all parties involved.

[22] Law Enforcement Access to Data Stored Abroad Act. S.512. https://www.congress.gov/bill/114th-congress/senate-bill/512

[23] See, for example: Greg Nojeim. 2014. "LEADS Act Extends Important Privacy Protections, Raises Concerns." *Center for Democracy and Technology.* https://cdt.org/blog/leads-act-extends-important-privacy-protections-raises-concerns/

[24] Grant Gross. 2015. "Lawmakers introduce two bills to protect email privacy." *Computerworld.* http://www.computerworld.com/article/2884018/lawmakers-introduce-two-bills-to-protect-email-privacy.html

Governments must coordinate on a modernization (or the replacement) of MLATs. An obvious starting point is the current system that exists among EU countries. Currently, law enforcement agencies across the EU are (relatively) efficiently coordinated when it comes to extraterritorial data access. This is done through different mechanisms, including the European Judicial Network, which establishes points of contact for law enforcement that facilitate investigation and prosecution of criminal activities across the member states.[25] Another important institution is Eurojust — which actively coordinates the exchange of information between member state law enforcement systems.[26] Eurojust already coordinates with the United States, and this system should be examined for ways in which the existing cooperation might be extended between the United States and the European Union to address more specifically the data access and privacy issues. The goal should be accelerating the process of legitimate data request and retrieval across borders while maintaining common standards of privacy protection. The Budapest Convention on Cybercrime offers another model of existing cooperative agreement to examine and build upon.

Governments should build on the U.S.-EU "Umbrella Agreement" for the protection of data shared between EU and US law enforcement agencies. This agreement — completed in September 2015 — establishes rules of the road for how law enforcement agencies will handle data transferred to them during the course of a transatlantic criminal investigation.[27] These rules include limits on how the data may be used, restrictions on data transfer and retention, rights to access/verify/correct data, notification of security breaches, and judicial redress for citizens of the EU in U.S.courts if data is mishandled. This right of legal redress already exists for U.S. citizens in EU courts. In order for EU citizens to enjoy this right in U.S. courts, Congress must pass legislation known as the Judicial Redress Act.[28] This bill remains pending in the U.S. Senate (after passage in the House of Representatives); it has the support of both business and civil society stakeholders.[29]

Taken together, these recommendations (either at the bilateral or multilateral level) would establish a set of mutually granted privacy rights among nations, offer certainty to both companies and consumers in the market, and set clear rules and expectations among law enforcement agencies about which laws apply in different circumstances. As a concluding note, we emphasize here that this analysis and recommendations deal only with the question of law enforcement access to data, rather than intelligence agencies. But that does not mean that such reforms would be irrelevant for signals intelligence. With policy changes vis-a-vis law enforcement, we are resetting norms and expectations across a sector of security services that will alter practices that have carry-over effects to intelligence agencies over time. Further, we strongly encourage governments to have bilateral reform efforts along similar lines to deal with extraterritorial data access outside of the law enforcement context.

[25] European Judicial Network (EJN). http://www.ejn-crimjust.europa.eu/ejn/EJN_StaticPage.aspx?Bread=2#

[26] History of Eurojust. http://www.eurojust.europa.eu/about/background/Pages/History.aspx

[27] European Commission. 2015. "Questions and Answers on the EU-US data protection 'Umbrella agreement'." http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm

[28] Judicial Redress Act. H.R.1428. https://www.congress.gov/bill/114th-congress/house-bill/1428

[29] Open letter from the Information Technology Industry Council to the Judiciary Committee in support of the Judicial Redress Act. http://www.itic.org/dotAsset/d/6/d6445b59-2508-45ab-a4ba-6d731bb53b39.pdf ; Sarah St. Vincent. 2014. "Privacy Act Reforms Would Promote US Respect for Human Rights." *Center for Democracy & Technology.* https://cdt.org/blog/privacy-act-reforms-would-promote-us-respect-for-human-rights/

4 Cyber-Security Cooperation and Strong Encryption

Summary

Germany and the United States should conduct bilateral engagement on two sets of related cyber-security issues: 1) common policies of cooperative cyber-security for critical infrastructure; and 2) the dilemma of strong encryption. Recent intrusions into the networks of the Office of Personnel Management[30] in Washington and the servers of the German Parliament[31] have re-emphasized the vulnerability of sensitive data and communications for both governments. In the private sector, the estimated losses of cyber-espionage is measured in the billions of dollars/euros per year.[32]

Meanwhile in the United States, the strong encryption technologies that could prove the best protection for sensitive data in our information systems are the focus of a dispute between law enforcement,[33] technology companies, and other parts of the government.[34] Technologists argue that strong cryptography is crucial to protect communications from digital assailants with increasing sophistication. However, widespread implementation of strong encryption effectively limits some forms of legitimate law enforcement access to data. Governments must decide how to maximize the economic and security benefits of encryption while managing competing law enforcement priorities. Recently, after deliberation, the Obama administration announced it would not seek legislation to mandate backdoor access to communications technologies with strong encryption.[35] This indicates de-escalation of this debate and a move toward common ground with Germany — which has long argued for strong encryption without mandatory backdoors.

If the encryption debate concludes with a transatlantic alignment around strong encryption and secure communications, these cryptographic standards and implementations could become a plank in a platform of cooperation on cyber-security. Security policy is ultimately a national concern, but building resilient defenses against global threats is a mutual interest and could be a constructive arena for reestablishing trust. In this context, the United States brings to the table strong capabilities in Information Assurance that would benefit European partners. Meanwhile, the German government's policy commitment to strong encryption is exemplary and the global credibility of German data security could lay the groundwork for new standards that benefit all participating countries.

Discussion

The debates over global surveillance in the last two years have driven two important trends in cyber-security — a political focus on so-called "technological sovereignty" in cyber-security policy and an increase in the commercial deployment

If the encryption debate concludes with a transatlantic alignment around strong encryption and secure communications, these cryptographic standards and implementations could become a plank in a platform of cooperation on cybersecurity.

[30] Kim Zetter. 2015. "The Massive OPM Hack Actually Hit 21 Million People." *Wired.* http://www.wired.com/2015/07/massive-opm-hack-actually-affected-25-million/

[31] Anton Troianovski. 2015. "German Parliament Struggles to Purge Hackers From Computer Network." *The Wall Street Journal.* http://www.wsj.com/articles/german-parliament-struggles-to-purge-hackers-from-computer-network-1434127532

[32] Ellen Nakashima and Andrea Peterson. 2014. "Report: Cybercrime and espionage costs $445 billion annually." *The Washington Post.* https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html

[33] Cyrus R. Vance Jr. et al. 2015. "When Phone Encryption Blocks Justice." *The New York Times.* http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=2

[34] Terrell McSweeny. 2015. "Worried About Your Data Security? How Encryption Can Help Protect Your Personal Information." Huffington Post. http://www.huffingtonpost.com/terrell-mcsweeny/worried-about-your-data-s_b_8083756.html

[35] Nicole Perlroth and David Sanger, 2015. "Obama Won't Seek Access to Encrypted User Data,"*The New York Times.* http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html

We focus on strong encryption solutions as a tenet of a cyber-security strategy and a basis for a cooperative cyber-security policy. Recognizing that the dilemma of encryption and law enforcement access does not have a technical solution, the clear path forward is to embrace the technology.

of strong encryption technologies. The first of these trends has been especially prominent in Germany where outrage over the transgressions of allied intelligence services and foreign companies drives a new focus on national-level solutions. Meanwhile, the question of sovereignty in cyber-security policy is not a prominent debate in the United States. The second trend, however, has been central in the U.S. debate as major Silicon Valley firms (e.g. Apple and Facebook) have implemented strong encryption on popular services as a means to restore confidence with customers that data is secure. By contrast, in Germany, a commitment to unbreakable encryption is the stated position of the government (although concerns have been raised at high levels).[36] Moreover, the German cyber-security agency (BSI) has issued recommendations on personal communications and strong encryption.[37] While most implementations of encryption leave metadata open for intercept, the increase in security provided by increased use of these technologies would be substantial.

If governments join together in a common embrace of encryption policy for data security (coupled with a commitment to expanding other methods of law enforcement), this policy could release some of the pressure to create nationalized regimes of security (i.e. technological sovereignty) by establishing a basis of trusted computing on mathematics rather than on nationality (e.g. sourcing hardware and software exclusively from domestic providers). A robust agreement on technical standards could facilitate greater cooperation in conventional cyber-security policies such as threat intelligence sharing, resilience in critical infrastructure, mutual protection against industrial espionage, and stability through norms and codes of conduct. Differentiated national level defensive strategies will always be a priority for both countries (including against one another's cyber capabilities), but a far higher security policy concern for both nations is the common threat they face from hostile actors.

Recommendation

Acknowledging the needs of citizens, firms, and governments to communicate securely, we focus on strong encryption solutions as a tenet of a cyber-security strategy and a basis for a cooperative cyber-security policy. Recognizing that the dilemma of encryption and law enforcement access does not have a technical solution, the clear path forward is to embrace the technology. This is not to dismiss the central challenges and grave threats faced by law enforcement agencies, but it does mean that increasing the capacity of security agencies will require other methods beyond communications intercept. While national governments could mandate that companies provide keys for legitimate law enforcement inquiries (and some are considering this),it appears unlikely that the genie will return to the bottle because so many products are already available in the market.[38] Moreover, if one government mandates a backdoor to digital services, all governments are likely to do so — placing technology service providers on untenable legal and moral ground.[39] And finally, the near-consensus view of cryptography experts is that vulnerabilities created for law enforcement access will ultimately

[36] Deutscher Bundestag. 2015. Drucksache 18/5144. http://dip.bundestag.de/btd/18/051/1805144.pdf

[37] Bundesamt für Sicherheit in der Informationstechnik. 2015. "Wie verschlüsselt kommunizieren." https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/Verschluesseltkommunizieren/Einsatzbereiche/einsatzbereiche.html

[38] David Kravtes. 2015. "U.K. prime minister wants backdoors into messaging apps or he'll ban them." *ars technica.* http://arstechnica.com/tech-policy/2015/01/uk-prime-minister-wants-backdoors-into-messaging-apps-or-hell-ban-them/

[39] Kevin Bankston. 2015. "Hearing on 'Encryption Technology and Possible U.S. Policy Responses'."*US Congress IT-Subcommittee.* http://oversight.house.gov/wp-content/uploads/2015/04/4-29-2015-IT-Subcommittee-Hearing-on-Encryption-Bankston.pdf

be exploited by adversaries as well.[40] Consequently, we recommend the following steps:

First, rather than arguing for "master key" government access to encrypted data, the German and the U.S. government should explore how they can strengthen cryptography and thus make everyone's communications more secure — including their own. This should include robust engagement with technology experts to raise the level of informed debate and to help policy-makers coalesce around realistic options.

Second, a unified approach to strong encryption (normative practice, standard setting, and interoperability) would provide a basis for both common security and economic policy as these technologies will be a central part of the global cloud computing market. Different regimes of security standards in the United States and Europe would introduce costs for both sides. Here, the German geopolitical brand (backed up by its technical track-record) for data privacy suggests that Berlin could deliver a strong contribution to a multilateral standard for secure communications that carries global credibility.

Third, for both governments the discussion about strong encryption could provide a jumping off point for a broader engagement about cyber security cooperation, including:

- *Threat Intelligence*: Effective mechanisms to promote the transatlantic sharing of critical information about cyber incidents;
- *Industrial Espionage*: Coordinated protection against common threats of cyber-attacks against private sector targets;
- *Transnational Cybercrime*: Coordinated approach to updating the Budapest Convention on Cybercrime to match technological developments in the ten years since implementation;
- *Critical Infrastructures*: Policies and practice to increase resilient security and thwart attacks more efficiently through closer cooperation;
- *Certification standards*: Common commitments to building trust in IT-security products through revised security certification processes;
- *Norms*: Partnership in promoting international cyber norms and codes of conduct to fight cybercrime and cyberespionage;
- *Zero-days*: Commitments between governments to reject agency stock-piling of zero-day vulnerabilities (undiscovered security holes), a practice that only strengthens the viability of the zero-day black market.

[40] Ellen Nakashima. 2015. "Tech giants don't want Obama to give police access to encrypted phone data." *The Washington Post*. https://www.washingtonpost.com/world/national-security/tech-giants-urge-obama-to-resist-backdoors-into-encrypted-communications/2015/05/18/11781b4a-fd69-11e4-833c-a2de05b6b2a4_story.html

Conclusion

The central conclusion of the Transatlantic Digital Dialogue working group is that there is broad support in both countries across the private sector, academic, and civil society for a pragmatic reform agenda. Furthermore, the reform agenda we propose squarely addresses the economic consequences of the transatlantic division while grounding its recommendations in a rights-based framework. The breadth of support that unites the private and civic sectors of the United States and Europe contrasts with the division between the governments and indicates the opportunity for viable political discussions that lead to policy change.

Our major conclusions are organized around three areas of policy reform — oversight/transparency, extraterritorial data access, and cyber-security. Taken as a whole, we demonstrate that each side has something to offer to the other; and each side has comparative advantages and disadvantages in the current state of law and policy with respect to modernization and reform.

On the issues of oversight and transparency of surveillance practices, it is EU states that may find useful examples of reform in the U.S. system. Though to be clear, we see substantial work to be done to modernize the U.S. system as well, even if it offers a useful starting point. We offer a variety of steps that both countries could take in parallel — ranging from simple methods of enhancing oversight to comprehensive reform of authorization procedure.

On the issue of extraterritorial access to data, the EU has a relatively well functioning system of coordination among law enforcement agencies. By contrast, the U.S. system is the subject of significant international mistrust, which creates challenges for U.S. businesses operating in foreign markets. The failure of MLATs and the breakdown of the Safe Harbor rules for EU/U.S. data sharing create a new urgency for problem solving. We identify a number of starting points for resolving these problems with a focus on aligning standards and criteria for law enforcement access to data.

Finally on the issues of cyber-security, there is a clear chance for mutual benefit in collaboration. Here each side has a comparative advantage to share with the other. The United States — with its extraordinary capabilities in identifying cyber-security weaknesses — could provide a wealth of knowledge to strengthen the resilience of critical infrastructure. However, the United States has yet to set a clear policy embracing strong encryption. By contrast, Germany unequivocally backs strong encryption without mandates for backdoors. A dialogue that leads to a common standard of strong encryption could produce a trusted framework around which to build a wider structure of common cyber-security policies.

We offer these analyses and recommendations with full recognition that this is the start of a long process of policy modernization. We do not presume to prescribe a comprehensive reform agenda addressing all elements of the transatlantic privacy/security debate. And we do not attempt here to document precise changes to policy and practice for particular governments. Rather, we seek to set an agenda of starting points. We see stagnation in bilateral dialogue between governments, and we hope that the engagement of a multi-stakeholder group from both countries — including industry, civil society, and academia — will signal political support for reform, offer a narrative of consensus around key issues, and create much-needed momentum to make change.

Appendix A — Participants in the Transatlantic Digital Dialogue

Germany

Mike Cosse, Vice President, Government Relations in Middle & Eastern Europe, SAP

Klaus Landefeld, Board Member, Association of the German Internet Industry eco, e.V.

Professor Christoph Meinel, Scientific Director and CEO, Hasso Plattner Institute for Software Systems Engineering

Professor Ingolf Pernice, Director, Humboldt Institute for Internet and Society (HIIG) and the Walter Hallstein-Institute for European Constitutional Law.

Matthias Spielkamp, Managing Editor iRights.info, Founding Partner iRights.Lab

Annegret Bendiek, Deputy Head, External Relations Research Division, Stiftung Wissenschaft und Politik (SWP)

Ansgar Baums, Director of Corporate Affairs, Hewlett-Packard Germany, EMEA

United States

Greg Nojeim, Senior Counsel, Center for Democracy & Technology; Director, Freedom, Security & Technology Project

Frank Torres, Director of Consumer Affairs and Senior Policy Counsel, Microsoft

Eric Wenger, Director for Cybersecurity and Privacy, Cisco, Global Government Affairs

Cynthia Wong, Senior Researcher on Internet and Human Rights, Human Rights Watch

Alvaro Bedoya, Founding Executive Director, Center on Privacy & Technology, Georgetown University Law School

Kevin Bankston, Policy Director, Open Technology Institute, New America

Participants from Hosting Institutions

Sudha David-Wilp, Senior Transatlantic Fellow, German Marshall Fund (GMF) of the United States

Markus Löning, Senior Fellow, stiftung neue verantwortung

Stefan Heumann, Director, European Digital Agenda Program, stiftung neue verantwortung

Ben Scott, Managing Director, stiftung neue verantwortung, rapporteur

G | M | F OFFICES

Washington • Berlin • Paris • Brussels
Belgrade • Ankara • Bucharest • Warsaw

www.gmfus.org