Atlantic Council

Building a Transatlantic Digital Marketplace: Twenty Steps Toward 2020

Report of the Atlantic Council Task Force on Advancing a Transatlantic Digital Agenda

Co-Chairs:
H.E. Carl Bildt
The Hon. William E. Kennard

Project Director:
Frances G. Burwell

Rapporteur:
Tyson Barker

Building a Transatlantic Digital Marketplace:
Twenty Steps Toward 2020

Report of the Atlantic Council Task Force
on Advancing a Transatlantic Digital Agenda

Co-Chairs
H.E. Carl Bildt
The Hon. William E. Kennard

Project Director
Frances G. Burwell

Rapporteur
Tyson Barker

ISBN: 978-1-61977-943-3

April 2016

Contents

Foreword

The global economy is in the throes of revolution. Big data, cloud computing, artificial intelligence, and the integrated networks of physical components are transforming every facet of economic life. Digitalization will upend supply chains, empower small businesses and consumers, rationalize energy use in the most efficient way, allow truly customized customer service, and build connections across vast distances. Soon everything from appliances to cars and even the clothes on our backs could be online as an Internet of Things crisscrosses every aspect of our daily lives.

Against this backdrop of enormous digital transformation, the United States and the European Union have the chance to seize a new big idea in the transatlantic relationship: the creation of transatlantic digital single market stretching from Silicon Valley to Tallinn. If they get it right, they can lead in creating a climate of digital prosperity, security, and privacy for a world where digitalization permeates everything, data is moving faster, and borders are less relevant. In short, they can give a new jolt to the transatlantic economy while—at the same time—ensuring that the global digital economy remains a space for free trade, free markets, and free people.

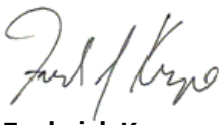
With this goal in mind, the Atlantic Council created the Task Force for Advancing the Transatlantic Digital Agenda—co-chaired by former Swedish Prime Minister and Foreign Minister Carl Bildt and former FCC Chairman and US Ambassador to the EU, William Kennard. Our goal was simple: take on this big idea and flesh it out with concrete policy steps that would make it possible. This task force brought together twenty-five of the best minds —former senior government officials, members of the business community, start up representatives and entrepreneurs, civil society leaders, academics and policy experts—to tackle these questions. They came together in Washington, Brussels, Berlin, and Warsaw for intense discussions on a range of pressing issues facing transatlantic digital policy. This report is a culmination of those efforts.

I would like to offer our particular thanks to the Co-Chairs of this Task Force, Carl Bildt and William Kennard, for their guidance and stewardship over the course of this process. They challenged the task force to think big and come up with the practical steps necessary to forge a digital single market spanning the Atlantic. We would also like to thank the brain trust—our task force members—for their vision, energy, creative thinking, and critical analysis of many nuanced issues.

A special thanks to our on-the-ground partners in this project, Digital Europe in Brussels, Aspen Berlin in Germany, and Dentons Europe in Warsaw. Their support was instrumental in facilitating the high-octane workshops that gave the task force important insight into Europe's hopes, concerns, and expectations in these key capitals. We also like to thank the numerous outside speakers from the US government, European Commission, European Parliament and other governments who helped guide us in our deliberations.

I would like to acknowledge the leadership of Fran Burwell, Atlantic Council Vice President for European Union and Special Initiatives. Tyson Barker performed his work as rapporteur with great distinction and persistence. Sarah Bedenbaugh made sure that the workshops ran smoothly, efficiently, and successfully. And thanks to Susan Haigh and Anastassios Adamopoulos for their extensive support, thorough research, and tireless dedication to this project.

Finally, we want to extend our deepest appreciation to Google for its generous support to this endeavor, and also to Telefonica and the Software and Information Industry Association. Our work would not have been possible if it were not for their recognition of the importance and urgency of this unique moment in transatlantic digital policy. In the future, our economic prosperity will depend on success in building new digital bridges between our two economies. We hope that this report can contribute to that effort.



Frederick Kempe
President and CEO, Atlantic Council

Note from the Co-Chairs

It was five years ago in 2011 at the Hanover Messe, the world's largest industrial fair, that the idea of *Industrie 4.0* first entered the political blood stream. Now, five years later, the industrial Internet, automation, big data, sensor technology, and the Internet of Things are rewiring our world.

But the policy architecture to promote and shape the space for this digital transformation continues to lag behind. The reason is simple: creating a space where innovation is dynamic, safe, accessible, and secure is not easy. When looking at the digital economy, policymakers must aim for three objectives: to increase prosperity, ensure security, and promote democratic values. Often these are mutually reinforcing. But, at times, they can also present policymakers and the wider stakeholder community—users, business, academics, media, civil society, and others—with tough choices. The question is: How will policy makers and stakeholders respond?

This report is a blueprint for tackling some of these questions and, in the process, building a seamless transatlantic digital marketplace. If the United States and Europe—as leaders in the digital economy—can establish a truly transatlantic digital market, they will help foster a global digital economy that is based on the same rules and values. The twenty steps outlined here offer a roadmap. Taken together, these steps advance the five core areas that will make an integrated market possible: enhancing digital trade; improving the building blocks of transatlantic digital regulation and standard setting; providing templates for domestic conditions that foster innovation; restoring trust in transatlantic cooperation on data protection and privacy; and advancing shared US-EU values in global Internet governance.

The ideas behind a transatlantic digital single market are ambitious but achievable. Our Task Force discussions were often lively, reflecting the plurality of views on topics as diverse as net neutrality, privacy, tech startups, competition law and freedom of speech. Of course, not every recommendation in this report fully reflects the views of this diverse group of task force members. But we believe it captures the constructive essence of a conversation that will increasingly be at the heart of the transatlantic relationship. And as task force Co-Chairs, we support both the spirit and overall findings of this document. It was a pleasure to work with this talented group of experts and we look forward to working together to advance the goals articulated in this report.

Sincerely,

Carl Bildt and William E. Kennard

Task Force on Advancing a Transatlantic Digital Agenda

Co-Chairs

* **Carl Bildt,** Chairman, Global Commission on Internet Governance, former Swedish Foreign Minister and Prime Minister, and now chairman, Global Commission on Internet Governance

* **William Kennard,** Former US Ambassador to the European Union & Former Chairman of the US Federal Communications Commission

Task Force Members:

Robert Atkinson, President, Information Technology and Innovation Foundation

* **Melissa Blaustein,** Founder, Allied for Startups

Kathryn Brown, CEO, Internet Society

* **Sarah Drinkwater,** Head, Google Campus London

* **Dean Garfield,** President and CEO, Information Technology Industry Council

* **Gerard Grech,** Chief Executive Officer, TechCity UK

* **John Higgins,** Director General, DigitalEurope

* **Paul Hofheinz,** President, Executive Director and Co-Founder, Lisbon Council

* **Jane Holl Lute,** President and CEO of the Council on CyberSecurity – Atlantic Council Board Director

Ron Klain, General Counsel, Revolution

* **Hosuk Lee-Makiyama,** Director, European Centre for International Political Economy (ECIPE)

* **Josh Meltzer,** Fellow in Global Economy and Development, Brookings Institution

* **Michael Nelson,** Public Policy, CloudFlare; Professor of Communication, Culture, and Technology at Georgetown University

* **Nuala O'Connor,** President and CEO, Center for Democracy and Technology

* **Daniel Price,** Former Deputy National Security Advisor for International Economic Affairs; now Managing Director, Rock Greek Global Advisors – Atlantic Council Board Director

* **Sean Randolph,** Senior Director, Bay Area Council Economic Institute

* **Simon Schaefer,** CEO, Founder, The Factory Berlin

* **Carl Schonander,** Senior Director, Software & Information Industry Association

* **Alfredo Timermans,** CEO, Telefonica Internacional USA

Paul Twomey, Founder, ArgoP@cific

* **Constantijn Van Oranje-Nassau,** Special Advisor & Vice Chairman of International Circle of Influencers, StartupDelta

Madeleine Gummer von Mohl, Co-Founder, Betahaus

* **Orlie Yaniv,** Director, Government Affairs and Policy, FireEye

The Atlantic Council would like to thank all the Task Force members for the insights and expertise they provided to this effort. Those members indicated with a * have endorsed the report with the following statement:

"This report reflects the discussions held by the Atlantic Council's Task Force on a Transatlantic Digital Agenda. The Co-Chairs and members of the Task Force welcome this report as an important contribution to the debate and support its overall conclusions. However, not all of the report recommendations reflect the views of all Task Force members. Individuals participated in the Task Force in their private capacity; affiliations are provided for identification purposes only."

Executive Summary

The United States and the European Union (EU) have a historic opportunity—perhaps their last—to be leaders in building the digital market of the future. To do so, they must seize this opportunity to create a transatlantic digital single market stretching from Silicon Valley to Tallinn. Together, they can give a new burst of energy to a global Internet economy centered on thriving digital commerce, innovation, creativity, online security, and citizens' rights.

It's time to take a page from Alexander Hamilton—the visionary who saw the future of the United States shaped by a shared national financial system, and who implored his fellow citizens to "learn to think continentally." The digital world is today craving its Hamilton moment, one that will force policymakers to learn to think in transatlantic or, better yet, global terms. In the coming years, digitalization will: transform the transatlantic economy and bring the promise of greater prosperity; create new threat vectors as billions of networked devices create potential vulnerabilities for economic disruption and physical harm; and open up new conundrums for fundamental rights and democracy. How will policymakers and stakeholders respond?

The EU is now on a path to creating a digital single market and rewriting its data-protection rulebook. At the same time, the United States and the EU are creating a new transatlantic bridge for the free flow of data, building fresh avenues for cooperation on law enforcement data, wrapping up a twenty-first century mega-trade agreement with the digital economy at its heart, and defending a more equitable, inclusive, multi-stakeholder model of Internet governance. All of this is taking place against the backdrop of the use of digital communication in terrorist attack planning, recruitment over the Internet by the Islamic State of Iraq and al-Sham (ISIS), the rise of online authoritarianism, increasing cyber crime, and new vulnerabilities and growing digital divides.

This report is a call to action. Now is not the time to rehash old battles or seize on minor differences that impede consensus on major issues. Today's transatlantic leaders have a responsibility to bridge differences and create the climate for tomorrow's digital prosperity, security, and privacy for a world where digitalization permeates everything, data is moving faster, and borders are less relevant.

There are no simple answers or silver bullets. The best policy cocktail will mix big ideas with small, technical steps that bridge political and philosophical differences and build on common principles. This report looks at the state of play on the most pressing digital policy issues across five interlocking areas, and identifies twenty steps that the United States and the EU can begin to take between now and 2020 to build a transatlantic marketplace, encourage trust, and preserve the Internet as a global commercial commons and a public good. That effort must begin with the mode of coordination.

- **Step 1: Launch a US-EU Digital Council.** A US-EU Digital Council—housed in the White House and at senior levels in the European Commission—would give transatlantic coordination the political weight capable of breaking bureaucratic silos and connecting dots between the broad objectives. It could proactively shape interoperable policies in the digital space, including on net-neutrality policy, data protection, the Internet of Things (IoT), broadband development, open data flows, enhanced cybersecurity, and Internet freedom.

Redefining the Rules of Digital Trade

Digital trade is slated for its biggest overhaul ever, as the Transatlantic Trade and Investment Partnership (TTIP), plurilateral Trade in Services Agreement (TiSA), and Trans-Pacific Partnership (TPP) recast the international rules for information communication technology (ICT) regulation, e-commerce, and open cross-border data flows for the twenty-first century. The United States and EU are positioned to extend their leadership in the €12 trillion global e-commerce market.

- **Step 2: Use TTIP negotiations to reduce digital barriers and broaden digitization in transatlantic and global trade.** TTIP negotiators should borrow from the TPP to create an interoperable digital space for goods and services spanning the Atlantic and Pacific, use TTIP to establish common requirements that will better coordinate e-labeling, give the disabled better access to the digital space, and insert digital overlays in other TTIP chapters, from services to small–and medium-sized enterprises (SMEs).
- **Step 3: Create a fully open, nondiscriminatory investment space for ICT infrastructure.** Lifting restrictions and equity caps, particularly on business-to-business (B2B) ICT infrastructure, would enhance competition and innovation in the digital marketplace.
- **Step 4: Update the 2011 US-EU Trade Principles for ICT Services and integrate them into TTIP.** The 2011 EU-US Trade Principles for ICT Services have provided common norms that inform trade engagement with third countries, and should be updated.

Rethinking the Building Blocks of US-European ICT Regulatory Cooperation

A thriving digital economy requires an interoperable system of rules that minimizes fragmentation, allows innovation to thrive, and encourages cross-border, multi-stakeholder collaboration. There is a real need to integrate stakeholders, especially US and European startups and SMEs, into discussions about transatlantic digital policy, to ensure that policy outcomes succeed in promoting new business growth and job creation.

- **Step 5: Increase the use of review and consultation clauses in digital rules.** Increasing use of these clauses, on both sides of the Atlantic, would help ensure that openness and flexibility are hardwired into ICT regulation.
- **Step 6: Focus on joint US-EU impact assessments for proposed regulations and standards.** Joint impact assessments increase information sharing and foster a joint-assessment culture in the regulatory process. Joint impact assessments would also increase information sharing, foster a shared assessment culture, and incorporate new actors into the regulatory process—particularly stakeholders like startups, SMEs, and civil society from the other side of the Atlantic.
- **Step 7: Bolster efforts to increase tech literacy in the legislative branch.** The United States and EU should work with industry, academia, and civil society to enhance digital expertise in Congress and the European Parliament (EP).
- **Step 8: Increase cooperation with state and local regulators on the other side of the Atlantic, and highlight local best practices.** Policymakers on both sides of the Atlantic should look for opportunities to expand regulatory partnerships and build coalitions beyond Washington and Brussels.

Building a Cradle of Digital Innovation

Creating the space in which innovation can flourish is the cornerstone of the digital economy. While most responsibility for incubating the right innovation conditions lies in the domestic arena, there are steps the Atlantic partners can take together to unleash new innovation and set the pace for other digital economies.

- **Step 9: Support a startup culture by promoting laws that open up access to finance, and create one-stop shops that cater to new companies looking to expand in the EU.** The EU and its member states can draw lessons from each other and the United States in terms of increasing the accessibility of private-sector finance and other measures to enable startups.
- **Step 10: Ensure nascent net-neutrality regulations minimize fragmentation between the United States and Europe.** The US Federal Communications Commission (FCC) and EU have taken recent steps to develop rules to ensure an open Internet. As these new rules are implemented, coordination is required to minimize fragmentation and arbitrage while at the same time, encouraging ISP infrastructure investment.
- **Step 11: Use investment funds and spectrum allocation to encourage early adoption of frontier technology and foster the industrial Internet.** The United States and EU must enhance the use of public investment and spectrum choices to catalyze industrial policy based on cloud computing, big-data analytics, and the Internet of Things.
- **Step 12: Launch joint reviews of major future policy issues, such as the labor-market effects of the Internet of Things and the sharing economy, and the potential impact of crypto-currencies on the transatlantic market.** The United States and EU should launch a joint assessment of the economic impact of these tech-driven economic phenomena on the labor market, and examine strategies that balance innovation and labor-market resilience.
- **Step 13: Expand transatlantic antitrust dialogue to address questions about the digital economy and**

US and European regulatory approaches. US and EU competition authorities should complement their deep operational cooperation with greater dialogue on the approach to the digital sector.

Reinforcing Transatlantic Data Protection and Privacy

US-European differences on data protection stem from a fundamental philosophical divergence on the interpretation of privacy rights in law. The breakthrough US-EU Privacy Shield Agreement shows both sides' commitment to a resilient, interoperable transatlantic data environment. The task of maintaining it will require the United States and EU to step up cooperation. This is particularly true as vulnerabilities to cyberattacks proliferate, and the threat of terrorist attacks and online recruiting by ISIS becomes more acute.

- **Step 14: Play an active role in the revision of the Council of Europe's Convention 108.** As the Council of Europe updates its 1981 Convention 108, the United States should play an active role in its revisions, with the intention of eventually ratifying it.
- **Step 15: Expand the discussion on thresholds and legal distinctions for personal data for the era of big data and the Internet of Things.** As the United States and EU deal with an exponential explosion in data, they should define different classes of data and the conditions separating industrial and personal data, as well as addressing questions around data ownership.
- **Step 16: Explore discrete sectorial confidence-building measures (CBMs) centered around users' access to their data, user privacy and user security.** The United States has a broad array of sector-specific laws on data protection that could act as useful nodes for transatlantic cooperation. Many of these laws create potential bridges for new, discrete US-EU data-protection cooperation.
- **Step 17: Integrate cybersecurity more fully into transatlantic discussions on privacy policy.** The nexus between privacy and data protection is currently underserved in transatlantic policymaking. The policy narrative around security and privacy often pits the two against each other—or avoids the information-technology (IT) security aspect altogether—when, in fact, they are mutually reinforcing. Transatlantic policymakers must work to correct these imbalances and elevate the cybersecurity dimension into policy discussions on privacy.

Leading in Global Internet Governance

The United States and Europe have been working to realize two objectives on the global stage: defending the existing multi-stakeholder system of Internet governance, and unleashing the Internet's social and economic potential for middle- and low-income countries.

- **Step 18: Reinforce the multi-stakeholder model to Internet governance, both globally and at home.** As new ideological challenges like "digital sovereignty" arise, the United States and EU should work with global civil society to renew an Internet governance framework based on a multi-stakeholder process and include Internet governance priorities in their own national strategies.
- **Step 19: Elevate Internet connectivity in the transatlantic development agenda.** The United States and EU should ensure Internet infrastructure-development projects receive priority alongside the construction of other infrastructure projects, such as roads, dams, and hospitals.
- **Step 20: Complete the Internet Assigned Numbers Authority (IANA) transition, tied to enhanced multi-stakeholder accountability in the Internet Corporation for Assigned Names and Numbers (ICANN):** Guaranteeing a transparent, multi-stakeholder, accountable system of Internet governance must be a geopolitical priority. Inaction could lead some actors to break away from the current system and strengthen the hands of states like Russia and China, which want a more state-centric system and have the potential to Balkanize the Internet.

A Transatlantic Digital Marketplace: Opportunity and Challenge

As the global economy stands at the edge of a great digital revolution, the United States and the European Union have a historic opportunity—perhaps their last—to be leaders in building the digital marketplace of the future. Together, they can give a new burst of energy to a global Internet economy centered on thriving digital commerce, innovation, creativity, online security, and citizens' rights.

This report is a call to action. The United States and EU must quickly seize this opportunity to create a real transatlantic digital single market, stretching from Silicon Valley to Tallinn. Such a market would: accelerate economic growth in the wake of the financial and eurozone crises; promote innovations like social media, cloud computing, mobile applications, robotics, and the Internet of Things; and enhance shared privacy and cybersecurity protections. This will not be easy. Digital issues have recently been among the most contentious in the transatlantic arena. Now is the time to create a new pattern, bringing business, government, citizens, and other stakeholders together in a way that aims to reduce transatlantic friction, while creating more opportunity for the free flow of digital goods and services.

The stakes could not be higher. Cloud computing, cross-border supply chains, inventory and shipping management, the Internet of Things, the rise of peer-to-peer services, and the sharing economy are reshaping business models and means of production, while giving rise to a new class of SME, the "Micro-Multinational."[1]

Globally, a new wave of consumers and producers are coming online in middle- and low-income countries. By 2020, the number of online devices is estimated to double to nearly 25 billion—3.5 networked devices for every person on the planet.[2] Cyberattacks are becoming more prevalent, more sophisticated, and—in an era of networked cars, medical devices, and appliances—increasingly capable of causing significant, and potentially physical, harm. New powers like China and Russia, which do not always share a commitment to openness and online freedom, are seeking to promote a very different kind of digital environment. In addition, the Internet's dark potential as a breeding ground for terrorist recruitment and operations has been underscored by attacks in Paris and San Bernardino.

Against this backdrop, transatlantic cooperation is more important today than ever before. If the United States and the EU do not get it right, there will be significant costs. The digital economy has become a key—perhaps the key—driver of US and European economic growth. Consider this: in 2013, the information and communication technology (ICT) sector was responsible for 22 percent of all jobs created in the Organization for Economic Cooperation and Development (OECD).[3] While last year the United States produced twenty-two "unicorns"—that is, tech startups reaching $1 billion—the EU is increasingly becoming a noteworthy "land of unicorns" as well, producing eleven over the same period.[4] In 2012, the EU had a $168 billion surplus in digital services, compared to $151 billion for the United

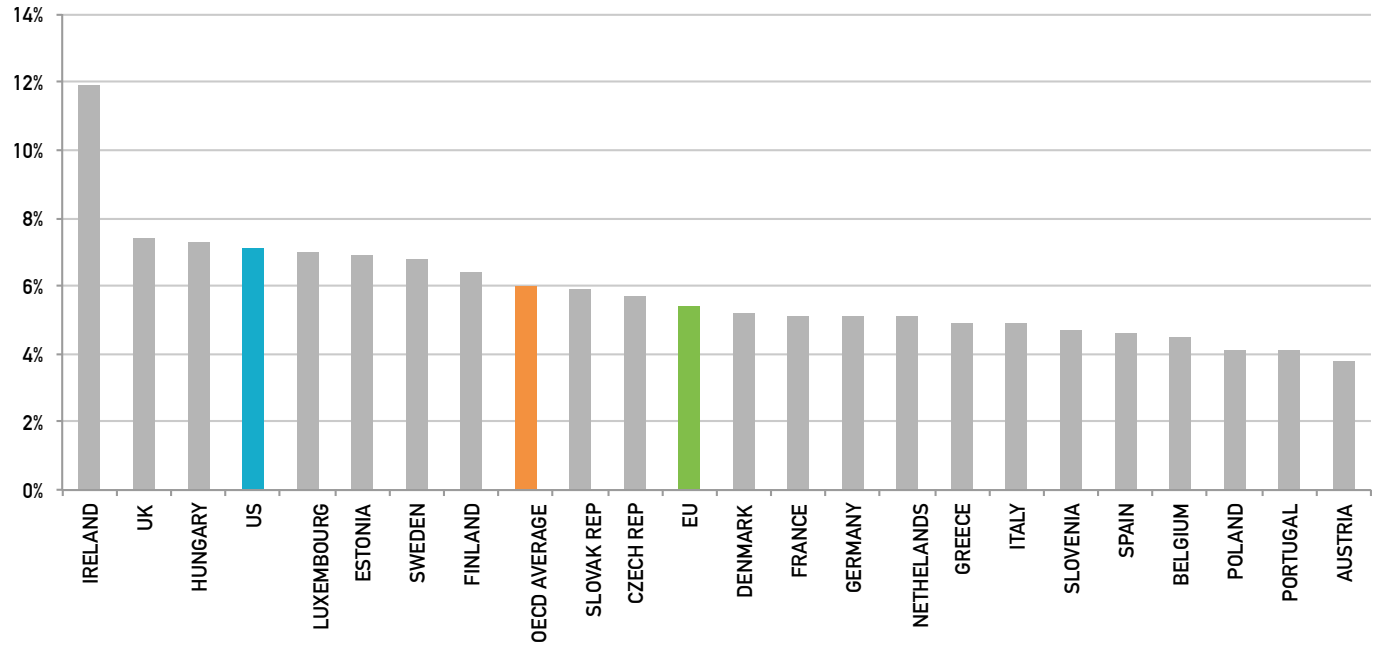
1 James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela Hung Byers, "Big Data: The Next Frontier for Innovation, Competition, and Productivity," *McKinsey Global Institute*, June 2011, http://www.mckinsey.com/business-functions/business-technology/our-insights/big-data-the-next-frontier-for-innovation; Hal R. Varian, "Technology Levels the Business Playing Field," *New York Times*, August 25, 2005, http://www.nytimes.com/2005/08/25/business/technology-levels-the-business-playing-field.html?_r=0 ; Ann Mettler and Anthony D. Williams. "The Rise of the Micro-Multinational: How Freelancers and Technology-Savvy Start-ups are Driving Growth, Jobs and Innovation," *Lisbon Council Policy Brief*, vol. 5, no. 3, 2011, http://www.eurada.org/files/SME%20support/LISBON_COUNCIL_Rise_of_the_Micro-Multinational%5B1%5D.pdf.

2 Ron Davies, "The Internet of Things: Opportunities and Challenges," *European Parliamentary Research Service*, May 2015, http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf.

3 Organization for Economic Cooperation and Development, *OECD Digital Economy Outlook 2015*, (Paris: OECD, 2015), p. 42, http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-digital-economy-outlook-2015_9789264232440-en#page1.

4 "The Rise of Europe's Unicorns," *European*, September 9, 2014, *http://www.the-european.eu/story-8416/rise-europes-unicorns.html*; CB Insights, "The Unicorn List: Current Private Companies Valued at $1B and Above," *https://www.cbinsights.com/research-unicorn-companies*.

ICT Sector Share of GDP (2011)



Source: World Bank, Digital Dividends.
**Data collected for 2011*

States.[5] In 2013, 42 percent of all apps were US-made; 22 percent were made in Europe, often by SMEs.[6] Commercial and research activity currently accounts for 40 percent of transatlantic data flows and is expected to generate the majority of data-flow growth in the future, particularly as the Internet of Things becomes a reality in daily life.[7]

The United States is the largest market for many European digital services, and vice versa. The European Commission estimated that the digital economy could generate as many as 825,000 ICT jobs in the EU by 2020, a number roughly the size of the entire Estonian labor force.[8] Digital transformation is changing industries like finance, tourism, audiovisual technology, and retail—generating more than 75 percent of tech-driven economic value in the global economy.[9] American tech companies are important European employers. In short, the EU and United States are both beneficiaries of the digital revolution.

Last year, the EU launched a high-profile effort to complete its single market in digital services. The European Commission's May 2015 Digital Single Market (DSM) strategy aims to assemble Europe's fractured commercial landscape into a unitary space for consumers, businesses, startups, civil society, and regulators.[10] The DSM centers around three interlocking planks seeking to promote access, increase fairness and innovation, and encourage economic growth. The EU is also completing a new General Data Protection Regulation (GDPR) that will upgrade the 1995 directive by providing greater certainty of protection standards and enforcement throughout the EU-28 and codifying new

5 Catherine A. Novelli, "Growing the Trans-Atlantic Digital Economy," speech delivered at the Lisbon Council, June 2, 2015, http://www.state.go/e/rls/rmk/243086.htm.
6 Stuart Lauchlan, "Europe's Big Chance in the Global Apps Market," *Diginomica*, September 11, 2013, http://diginomica.com/2013/09/11/europes-big-chance-global-apps-market/.
7 Joshua Paul Meltzer, "A New Digital Trade Agenda," (Geneva: E15 Expert Group on the Digital Economy, 2015), http://e15initiative.org/publications/a-new-digital-trade-agenda/.
8 World Bank, "Labor Force Data," 2015.
9 Matthieu Pélissié du Rausas, James Manyika, Eric Hazan, Jacques Bughin, Michael Chui, and Rémi Said, "Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity," *McKinsey Global Institute,* May 2011, http://www.mckinsey.com/industries/high-tech/our-insights/internet-matters.
10 European Commission, *Digital Single Market: Bringing Down Barriers to Unlock Online Opportunities*, http://ec.europa.eu/priorities/digital-single-market_en.

Hotspot Atlantic : A Mapping of Every Device Connected to the Internet

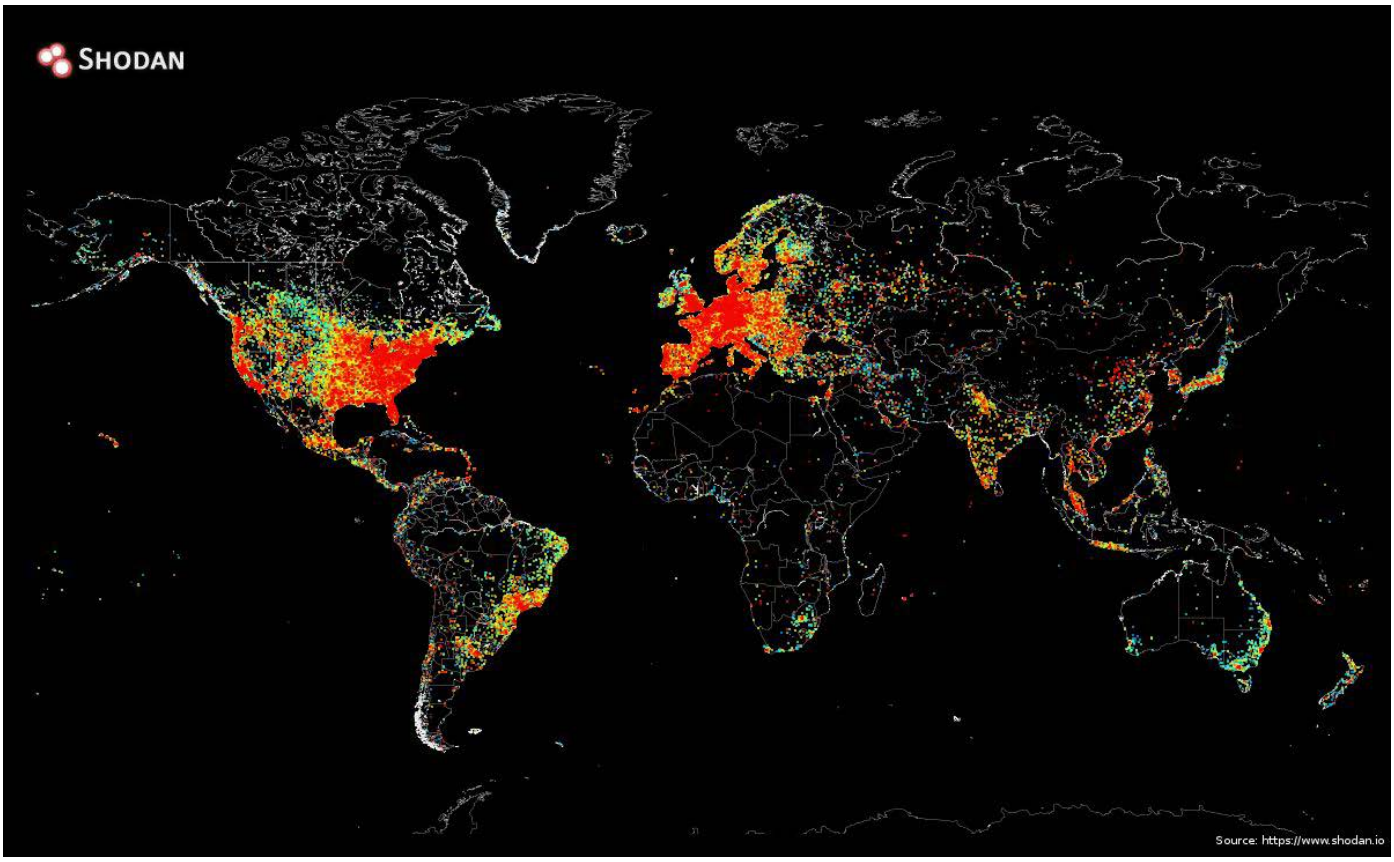


Photo credit: SHODAN.

data-protection norms at levels consistent with new technology.[11]

At the same time, US and European policymakers together seek to formulate a body of interoperable laws, principles, and codes of conduct that preserve the twin principles of openness and integration. This includes negotiating the Transatlantic Trade and Investment Partnership (TTIP), a major free-trade agreement (FTA) with ambitious aspirations in e-commerce, transatlantic data flows, and digital services. It also means: working on a plurilateral Trade in Services Agreement (TiSA); completing the so-called "Umbrella Agreement," a data-protection framework intended to enable enhanced data sharing in law enforcement; and putting a new Privacy Shield framework agreement in force. Congress' unanimous passage of the Judicial Redress Act is just one example of the broad political support behind these efforts.

The bottom line is that these two big ideas—the EU's DSM and the notion of a transatlantic digital marketplace—will not work in isolation from one another. For the DSM to succeed, it needs an ambitious digital trade environment. For TTIP to succeed, it must allow the United States to plug into a European digital marketplace unencumbered by internal and external barriers to digital commerce. The DSM and TTIP are mutually reinforcing. Only when both are realized can the United States and EU achieve a truly transatlantic digital single market that allows startups, SMEs, innovation, and civil society to flourish.

These efforts are taking place against a politically charged backdrop. Edward Snowden's 2013 revelations opened deep rifts over the processing, storing, and managing of personal data. Polling shows that the Snowden episode reinforced an idea in Europe that Americans—the US government and companies alike—are cavalier in their treatment of European personal data. For example, Germans overwhelmingly prefer

11 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, January 25, 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

European data-protection standards to US standards (85 percent to 3 percent).[12] While the Obama administration and Congress have made headway in efforts to refine, limit, and place new checks on mass surveillance by intelligence agencies, many Europeans believe those efforts do not go far enough. The October 2015 decision by the Court of Justice of the European Union (CJEU) in the *Schrems* case, striking down the Safe Harbor framework was welcomed by many Europeans.[13] A Second Circuit US Court of Appeals ruling allowing the US government to access Microsoft servers in Ireland, without Irish government permission, could further irritate the relationship.[14]

Moreover, many Europeans believe the EU tech sector is at a comparative disadvantage to its US equivalent. The European Commission highlights the dominance of US-based online services when making the case for the EU's DSM. The top two attributes that Europeans ascribe to US tech companies are "successful" (38 percent) and "too powerful" (37 percent).[15] In turn, many Americans are suspicious that the EU is using technocratic means to break down Silicon Valley's perceived competitive advantage over Europe's tech sector.

On the whole, the transatlantic digital economy continues to work well, but mutual suspicion and thin trust are political realities hampering the potential benefits of deeper joint action. The reality is simple: more than any other major economies, the United States and EU have a shared stake in building a global digital marketplace based on openness, dynamism, and innovation, and which guarantees wide access while protecting consumers' rights, security, the public interest, and democracy.

This report is not a comprehensive analysis of transatlantic digital policy, its development, or its deficiencies. Nor does this report provide more than a tertiary examination of US-European cooperation in national security, intelligence, cybersecurity, and law enforcement, beyond their impact on the transatlantic digital market. These areas, taken together, are worthy of future exploration—especially in a world where ISIS recruitment, porous borders, and the proliferation of networked communications and everyday objects vulnerable to attack have created new urgency for coordinated action.

Rather, this report draws on the broad expertise of task force members to propose **twenty steps toward building a transatlantic digital single market by 2020.** Given the current political climate, the best path forward will be paved by a mix of big steps and some small, technical steps—institutionalized dialogues, confidence-building measures, and joint-review mechanisms—that bridge political and philosophical differences, and build on common principles. Future generations of Americans and Europeans will be digital natives. Today's leaders have a responsibility to create the setting for tomorrow's digital prosperity, and to promote security and privacy for a world where digitalization permeates everything, data is moving faster, and borders are less relevant. This report identifies operational recommendations that the United States and EU can take to build trust, bond the transatlantic marketplace, and preserve the Internet as a public good and a global commercial commons.

Achieving these aims will not be easy. It will require sustained high-level engagement and cooperation between the United States and EU. The transatlantic digital economy—along with its impact on society and citizens—must be a top priority in transatlantic interactions over the next five years, or this opportunity may be lost.

Step 1: Launch a high-level US-EU Digital Council to provide oversight of the transatlantic digital relationship in a way that binds the political with the practical. A US-EU Digital Council will help catalyze political leaders and provide a focus for public and stakeholder engagement. It could also marshal resources and coordinate efforts across governments, and provide a platform for high-level discussion of regulatory outcomes and best practices. It could also provide early warning of regulatory divergence.

The revival of the Information Society Dialogue has been a positive first step.[16] But, given the hive of activity on digital policy, it is time to take the digital dialogue to the

12 Pew Research Center in Association with the Bertelsmann Foundation, *Support in Principle for a US-EU Trade Pact: But Some Americans and Germans Wary of TTIP Details*, (Washington, DC: Pew Research Center, 2014), http://www.pewglobal.org/2014/04/09/support-in-principle-for-u-s-eu-trade-pact/.

13 Court of Justice of the European Union, press release, *The Court of Justice Declares that the Commission's US Safe Harbor Decision is Invalid*, October 6, 2015, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf. It should be noted that the Schrems decision was only partially based on bulk data collection, and the ruling even cites flawed reporting on surveillance programs.

14 Karlin Lillington, "Data Case has Huge Implications for Personal Privacy," *Irish Times*, January 14, 2016, http://www.irishtimes.com/business/technology/data-case-has-huge-implications-for-personal-privacy-1.2495493.

15 Brunswick Group, *Europe & the Internet: It's Complicated*, September 28, 2015, https://www.brunswickgroup.com/publications/surveys/european-views-of-us-tech-companies/.

16 Daniel Sepulveda, "The 2015 US-EU Information Society Dialogue," *Dipnote: US Department of State Official Blog*, April 22, 2015, https://blogs.state.gov/stories/2015/04/22/2015-us-eu-information-society-dialogue.

next level. A Digital Council—housed in the White House and at senior levels in the European Commission—would elevate the Information Society Dialogue and give transatlantic coordination the political weight capable of breaking down bureaucratic silos. It would help connect the dots between political and economic objectives, and guide operational coordination of regulation at a more technical level. It could proactively shape US and European policies in the digital space, including on net-neutrality policy, data protection, the Internet of Things, broadband development, open data flows, encryption, cybersecurity, and Internet freedom. No one is more aware than policymakers of the need for new crosscutting mechanisms to tackle these issues head-on.[17]

The US-EU Energy Council offers a good model for this type of mechanism. Established in 2009, the Energy Council has been highly effective at using practical cooperation to bridge strategic priorities. For instance, at the height of Russia's 2014 aggression in Ukraine, the Energy Council allowed the United States to plug into Europe's regional energy-security conversations, and encourage the building of new gas interconnectors and LNG-import terminals in the Baltics, as well as reverse-flow capacity for gas pipelines in Poland, Hungary, and Slovakia. Through the Energy Council, the United States has generally been able to support the EU on its path toward an effective energy union.

Creation of such a council will more clearly define ownership of the transatlantic digital relationship, rather than leaving some areas of digital policymaking isolated or siloed. Digital Council meetings could also serve as an action-forcing instrument that assists the European Commission to coordinate and encourage consensus among member states on sensitive digital issues.

The Digital Council should also build in broader consultative roles for other stakeholders, such as representatives of European national governments, state and local governments, civil society, academics, think tanks, and the private sector, particularly startups. By creating an open and collaborative environment, the Digital Council will best reflect the multi-stakeholder model that both the United States and EU champion at home and globally.

17 Julie Brill, "Transatlantic Privacy After *Schrems*: Time for An Honest Conversation," speech delivered at the Amsterdam Privacy Conference, October 23, 2015, https://www.ftc.gov/system/files/documents/public_statements/836443/151023amsterdamprivacy1.pdf.

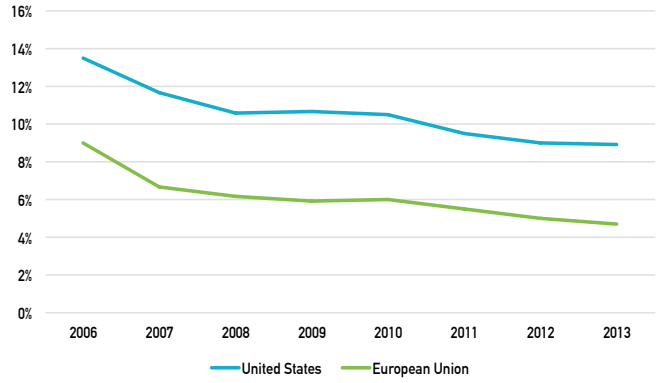
Redefining the Rules of Digital Trade

Digital trade is slated for a significant global overhaul as the Transatlantic Trade and Investment Partnership (TTIP), plurilateral Trade in Services Agreement (TiSA), and Trans-Pacific Partnership (TPP) recast international rules for ICT regulation, e-commerce, and cross-border data flows for the twenty-first century.

The United States and EU are well positioned to use the new trade order to extend their leadership in the €12 trillion global e-commerce market.[18] Digitally enabled service exports continue to power economic growth, reaching $356.1 billion in the United States in 2011. US digital trade has played a role in the creation of up to 2.4 million jobs.[19] The United States and EU remain world champions for digital services like cloud computing, and financial service and accounting applications, with the North American market valued at $33 billion and the European market valued at $38 billion in 2011. The value of web hosting and co-location were $23 billion in the United States and $8.6 billion in the EU. Not only are companies adopting digital products and services, but digitalization is becoming an integral part of most companies' organizational integrity.

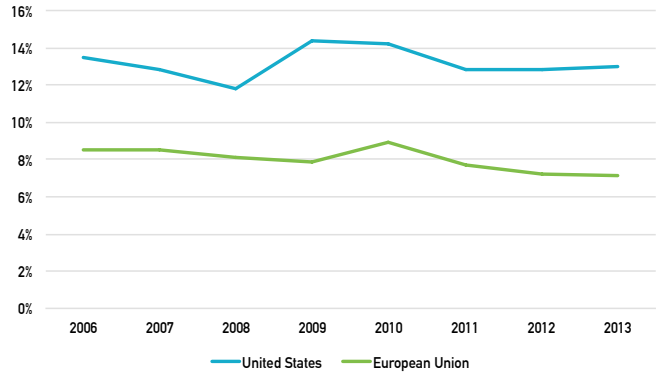
Increasingly, executive decisions, administrative oversight, supply chain management, and personnel management require global data flows. The International Trade Commission estimates economic gains of up to 0.3 percent—a number that some have called understated—simply as a result of lower barriers to data flows.[20]

ICT Share of Total Goods Exports



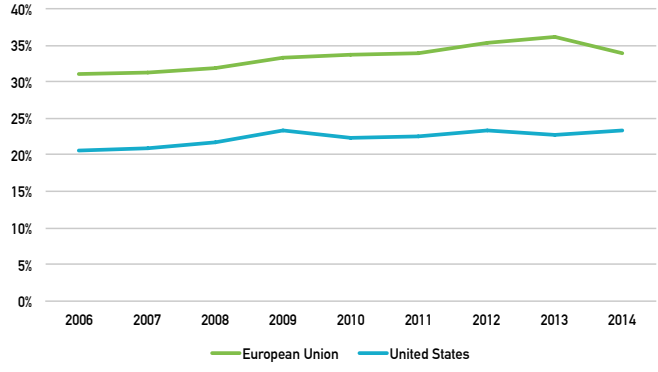
Source: World Bank.

ICT Share of Total Goods Imports:



Source: World Bank.

ICT Share of Service Exports:



Source: World Bank.

18 European Commission, *Trade for All: Towards a More Responsible Trade and Investment Policy* (Luxembourg: European Commission, 2015), p. 12, http://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153846.pdf.

19 Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries," *Information Technology and Innovation Foundation (ITIF),* February 2015, p. 11, http://www2.itif.org/2015-cross-border-data-flows.pdf.

20 Robert D. Atkinson, "Internet Data Flows: Promoting Digital Trade in the 21st Century," testimony delivered November 3, 2015, before the House Judiciary Committee, http://www2.itif.org/2015-atkinson-international-data-flows.pdf.

Mega-FTA negotiations are taking place against the backdrop of rising digital protectionism, both globally and in the transatlantic space. Non-tariff and technical barriers to trade can take different forms. Data-localization requirements and data-privacy laws are among the most prevalent, but there are also source-code-disclosure requirements, procurement and investment restrictions, and discriminatory treatment of service providers. Unlike sectors like agriculture, chemicals, automotive, and audiovisual, the Internet sector is a relative neophyte to trade policy. On the whole, the sector continues to lack the trade-negotiation literacy and expertise needed to respond to the dynamics of ongoing negotiations. National privacy laws are not necessarily trade barriers, per se. European and American rules can be seen as approaching privacy differently, while remaining consistent with trade obligations. The central challenge is to ensure interoperability between the two systems, through mechanisms like the Privacy Shield that allow companies to transfer data across the Atlantic, while complying with national privacy laws.

At least seventeen advanced industrial economies—including several in Europe—have passed or are considering laws with data-localization requirements. European companies have cited concerns about past use of the USA PATRIOT Act and potential National Security Agency (NSA) access to European personal data to justify limiting US cloud providers, in terms of gaining public contracts and market presence. Government officials in Germany and France have discussed the idea of national clouds. Informal pressure due to concerns about US surveillance has led companies like Shell to repatriate data storage from the United States to Europe. Microsoft attempted to dispel European mistrust of US data handling by creating a trustee relationship with Deutsche Telekom, with data centers in Germany that give customers the option of storing their data in the EU rather than in the United States.[21] However, the "Fort Knox" approach to storage can make data more vulnerable. At times, the best way protect the integrity, confidentiality, and security of data is to store it diffusely.[22]

Although restrictions on data flows and forced data localization can create some low-value jobs in brick-and-mortar data facilities, data analysis and usage beyond national borders results in more consumer savings, smarter and safer products, and even yield information that can lead to better policies. This data can be used to analyze soil usage and crop yield, examine climate patterns, determine demographic and migratory flows, and improve medical research and energy consumption.

Moreover, restrictive policies raise costs significantly for consumers of these services—making procurement more expensive, imposing new costs on startups that weigh down competitiveness, and hitting individual users. Additionally, they sever important linkages to global research networks, as well as supply and logistics chains that are increasingly the lifeblood for transatlantic business.[23] Data localization is particularly costly for small players and startups, who are disadvantaged by the barriers to scale that larger, more established players can more easily shoulder.

The United States and EU share similar objectives for the role TTIP and TiSA should play in reaffirming open cross-border data flows and combatting data protectionism. The 2015 Trade Promotion Authority, authorizing the US administration to negotiate trade agreements on Congress' behalf, emphasizes open data flows, limits on forced localization, and an extension of the World Trade Organization (WTO) moratorium on electronic-transmissions duties.[24] The European Commission's "Trade for All" communication, which includes digital trade as an area of negotiation for the first time, provides a full-throated endorsement of regulatory and standard-setting cooperation and efforts to combat "unjustified data localization and data storage requirements."[25]

The EU has taken data privacy off the table for TTIP. That said, both sides envision an ambitious and comprehensive e-commerce chapter that will codify market access for ICT and digital services, address data flows and data-infrastructure localization issues, and draw attention to everything in digital commerce, including spam, contract liability, and e-signatures.

Combined with a new Privacy Shield Agreement and pending multilateral arrangements in the OECD and the Council of Europe, the United States and EU can

21 Friedrich Geiger, "Microsoft Offers EU Customers Option to Store Data in Germany," *Wall Street Journal*, November 11, 2015, http://www.wsj.com/articles/microsoft-tightens-eu-clients-data-protection-1447247197.

22 Forced data localization and flow restrictions not only run counter to the spirit of the World Trade Organization principles of openness and greater regulatory coherence; they arguably violate the General Agreement on Trade in Services (GATS), which clearly restricts forced localization and other barriers to an open market in digital services.

23 Robert D. Atkinson and Ben Miller, "Digital Drag: Ranking 125 Nations by Taxes and Tariffs on ICT Goods and Services," *Information Technology and Innovation Foundation (ITIF)*, October 2014, pp. 24-25, http://www2.itif.org/2014-ict-taxes-tariffs.pdf.

24 US House of Representatives, "Bipartisan Congressional Trade Priorities and Accountability Act of 2015," April 2015, https://www.congress.gov/bill/114th-congress/senate-bill/995/text.

25 European Commission, *Trade for All*, p. 12.

reinforce open transatlantic data flows through respect for consumer rights and domestic laws. The EU's privacy and data-protection laws will continue to apply to European citizens and within European territory. In the United States, a more sector-based approach will continue. The key is guaranteeing mechanisms that protect the interoperability of the two systems, allowing data flows from Europe to the United States, and vice versa. Those interoperability mechanisms—such as the Privacy Shield Agreement, Binding Corporate Rules (BCR), model contracts, and consent—must provide assurances that the data being transferred is subject to the laws in the jurisdiction from which the data is transferred. Mechanisms should also be cost-effective, in order to take full advantage of the digital economy's potential.

The transatlantic trade negotiations will also be affected by the conclusion of the Trans-Pacific Partnership between the United States and eleven Pacific Rim states. TPP applies to 40 percent of global economic activity, and its e-commerce chapter offers a starting point for several measures regarding data flows and e-commerce that could be reinforced in transatlantic and global contexts. Like the parties to TPP, transatlantic partners are committed to maintaining a no-customs zone for the provision of digital services and equal, nondiscriminatory treatment of digital products and services. This should guarantee, for example, that European gaming apps and US cloud-computing application providers enjoy the same treatment on the other side of the Atlantic that they would receive at home. Moreover, given that more than half of global services trade is reliant on open data flows, the United States and EU should work together on TiSA to address market conditions, confront forced localization, and maintain open data flows in telecommunications, financial services, and e-commerce.[26]

But TTIP can go further, particularly given its regulatory cooperation and standard-setting dimension. Transatlantic negotiators have emphasized that TTIP will represent a new kind of "living agreement," moving from traditional tariff issues to tackle new barriers that impede services, regulatory coherence, and ICT. The last is one of nine sectors that trade negotiators have identified for enhanced cooperation in TTIP's regulatory chapter.[27]

Step 2: Use TTIP negotiations to reduce digital barriers and underscore the importance of digitization in transatlantic and global trade. The United States and EU should use TTIP negotiations to create an open, interoperable digital marketplace, limiting data localization and other measures that bring protectionism into digital trade. In particular, the United States and EU should use trade talks to bring the best elements from the TPP e-commerce chapter into TTIP, in order to create more seamless digital commerce. TPP offers lessons on digital trade for TTIP. These include key measures to: protect e-signatures; authenticate electronic transmissions; make commercial legal documents available for exchange; reaffirm the WTO commitment that digital transmissions should not be subject to tariffs or customs; ban source-code disclosure requirements as a condition for market access; strengthen consumer protections against spam, fraud, and deceptive messaging; and elevate the importance of cybersecurity cooperation between signatory Computer Emergency Readiness Teams (CERTs).[28] TPP also makes the crucial assertion that participating in a country's digital marketplace should not require building or using brick-and-mortar data centers in the country. TPP's ban on forced localization—with limited exemptions subject to fierce scrutiny—should become the gold standard in the Atlantic space as well, and in TTIP, these prohibitions should apply to all sectors, including financial services.[29]

The United States and EU should also work to align e-labeling and e-accessibility requirements for digital consumer products and services, particularly in the Internet of Things. As the market undergoes a massive proliferation of networked devices, providing required information in a standardized manner across product lines will increase transparency and ease the way consumers interact with the products they use. TTIP could include areas in which a great deal of effort has already been made—particularly in increasing accessibility of ICT for the disabled and creating interoperable e-labeling standards. This could streamline labeling requirements and, at the same time, make

26 Stephen Ezell, "Safeguarding Digital Trade is Vital to Ensuring a Thriving Global Innovation Economy," *Bridges,* December 2014, http://ostaustria.org/bridges-magazine/volume-39-may-2014/item/8177-safeguarding-digital-trade-is-vital-to-ensuring-a-thriving-global-innovation-economy.

27 European Commission, *Report of the Eleventh Round of Negotiations for the Transatlantic Trade and Investment Partnership*, October 2015, p. 14, http://trade.ec.europa.eu/doclib/docs/2015/november/tradoc_153935.pdf.

28 Office of the US Trade Representative, *TPP Full Text*, November 5, 2015, https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text.

29 It should be noted that TPP is not perfect. It lacks fair-use provisions, allowing limited use of copyright materials, which has lubricated online innovation, discussion and debate, and creative activity. These provisions could be addressed in TTIP.

product instructions on items such as medical devices, appliances, and televisions more user friendly and competitive. The United States and EU can also work within TTIP to establish common requirements and benchmarks that will provide the disabled with better access to digital technology and online applications.

In TTIP, digital overlays could also be created in chapters apart from e-commerce, to ensure the full benefits of an open digital economy. ICT and e-commerce are both specific sectors of trade, as well as enablers of trade that allow other sectors to thrive. TTIP chapters on financial services, SMEs, procurement, agriculture, intellectual property rights (IPR), and investment must have provisions that broaden digital adoption. These could include: assistance to SMEs to access e-commerce tools and enable transatlantic data flows; explicit mandates for regulators to share information and best practices, and to work with the private sector on self-regulation; and open, nondiscriminatory public-sector procurement with limited carve-outs and exemptions. Crucially, TTIP should reinforce prohibitions on data-housing requirements in TPP and extend them to all sectors.

Finally, the United States should provide a first-in-line guarantee that any extension of new privacy protections to foreign nationals will also apply to Europeans. The United States could provide a side guarantee as part of the TTIP negotiations—or in another forum—that the EU-28 will be at the front of the line for all extensions of privacy protections to foreign nationals. The United States provided a similar side commitment to select TPP signatories, such as Australia.

Step 3: Create a fully open, nondiscriminatory investment space for ICT infrastructure: The United States and EU state in the 2011 joint ICT principles that "governments should allow full foreign participation in their ICT services sectors, through establishment or other means."[30] Yet, barriers to full, nondiscriminatory participation in the US telecommunications sector continue to exist. Restrictions and equity caps on purchases of cable, broadband, and telecom companies in the United States restrict the flow of investment capital in these networks. Lifting these restrictions would provide added competition in the market landscape, incentivize new investment, and make it a more robust network.

Step 4: Update the 2011 US-EU ICT Principles and integrate them into TTIP as an annex. The 2011 EU-US principles for ICT services provide meaningful lessons about how the United States, the EU, and EU member states can create a "song sheet" of common norms that inform their trade engagement with third countries. The transatlantic partners should update these principles to account for emerging issues—addressing encryption, emphasizing the economic benefits of open data, creating standard language on cooperation on the Internet of Things, and establishing principles for rights to industrial data as digitized industry and global supply chains internationalize networked manufacturing.

30 European Commission, *European Union-United States Trade Principles for Information and Communication Technology Services*, April 4, 2011, http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc_147780.pdf.

Building a New Framework for US-European ICT Regulatory Cooperation

A thriving digital economy requires an interoperable system of rules that minimizes fragmentation, allows innovation to thrive, and encourages cross-border collaboration between multiple stakeholders. Without attention to the transatlantic dimension of these rules, the United States, the EU, and the EU member states risk drifting apart. With the world's largest markets and most sophisticated regulatory systems, the United States and EU can set global regulations and standards on everything from cars to chemicals. On the whole, this capacity has acted as a global public good, benefiting international commerce. US and EU regulators—often acting alone—have been first movers in setting ICT regulations and standards that best reflect the technical standards already represented in industry, and create positive outcomes for consumer safety, data security, performance, and interoperability.

Both the United States and the EU want greater regulatory convergence and coordinated standard setting in the digital space. But the size, sophistication, and power of the US and EU regulatory systems create challenges to transatlantic cooperation. US and EU regulators have specifically defined mandates, as well as different processes for testing and approving regulations, and must respond to entrenched domestic interests. These conditions make cooperation between regulators difficult, even when the logic for regulatory alignment is overwhelming.

The history of transatlantic regulatory cooperation has been mixed, at best. Efforts under the 1995 New Transatlantic Agenda—the first major push toward regulatory alignment under a series of formal mutual recognition agreements (MRAs)—were limited.[31] The United States and EU have been able to deliver some tangible results through later mechanisms, like the US-EU High Level Regulatory Cooperation Forum and the Transatlantic Economic Council (TEC). The two sides made progress in areas of standardization, such as efforts for battery standards in electric vehicles and e-health, and flexible recognition schemes for each other's certifications in discretely defined areas—including cargo security, generic pharmaceuticals, and organic foods.[32] But traditionally, progress has been cumbersome, labor intensive, and slow.

In this context, ICT rule-making poses a unique set of challenges. Innovation often outpaces rule-making, and that trend will accelerate with the growth of smart cities, networked manufacturing, self-driving cars, 3D printing, robotics, and artificial intelligence. While the world's Internet users today are people, tomorrow's users will be devices—automatically shifting and transferring data to monitor city and home electricity usage, prevent traffic accidents, optimize inventory for companies, and combat urban pollution. The rapid pace of digital development can leave regulators behind.

Tech rule-making is also multifaceted. It touches on a thick knot of interconnecting threads in the transatlantic digital-policy discourse—standardization, taxation, privacy, copyright, financing, infrastructure, criminal law, the evolving cyber threat landscape, national security, and competition. Drawing boundaries between these regulatory areas prevents the development of a seamless regulatory fabric.

In this environment, transatlantic rule-makers should think in terms of a "digital Hippocratic Oath." Their first principle must be to do no harm. This means that regulators must have the humility to recognize that, in many cases, the marketplace can solve problems better and faster than regulation, including most challenges facing the evolution of one global data network. This report offers three broad principles:

- **Outcome-oriented, rather than technology- or company-specific, regulations and standards:** Regulations and standards work best when they are

31 *European External Action Service,* "The New Transatlantic Agenda," December 1995.

32 US Department of State, *Transatlantic Economic Council*, http://www.state.gov/p/eur/rt/eu/tec/

goal-oriented, rather than specific to a technology or company. Once an industry sets down a precise, technological path, it can be extremely difficult to adjust. This is true for everything from letter arrangement on keyboards to electrical wattage in houses.

- **Co-regulation and regulation by design:** Rule-making must be an ongoing, robust, and equal collaboration among technology developers, users, and policymakers. To encourage a multi-stakeholder process including startups, civil society, and users for developing and enforcing standards, regulators can provide positive incentives like convening platforms, "quality seal" systems, and public financing, as well as negative incentives like the prospect of top-down regulatory intervention.[33]
- **Use of soft law:** Codes of conduct, principles, norms, and guidelines provide the most fruitful space for cooperation. Self-regulation, voluntary compliance, and certification with codes of conduct—rather than prescriptive laws—often are better equipped to address the needed speed, flexibility, and expertise of rule-making, and often yield the best results for citizens. Reputational incentives also play an important role. E-commerce "trustmark" badges, for instance, give companies an accessible way to show they have implemented consumer-protection and security measures.[34]

One example that incorporates these principles was the work of the National Institute of Standards and Technology (NIST) in developing the 2014 cybersecurity framework.[35] The exercise drew upon existing best practices, guidelines, and standards to create a voluntary framework for companies—including startups and SMEs—to evaluate their cybersecurity posture and develop a roadmap for improving it, as a way to reduce cybersecurity risk to critical infrastructure. The NIST drew from its top internal experts, but also crowdsourced standards from industry, encouraged partners outside the United States to choose these standards, and developed a body of hard and soft law that was flexible and user friendly.

To build on these three principles and improve transatlantic collaboration in ICT regulation and standards, the United States and EU should take several steps.

Step 5: Increase the use of review and consultation clauses in digital regulation, to encourage greater flexibility and interoperability. Given the rate of change in digital technology, lawmakers must make sure that rules are flexible and allow breathing room for innovation. The United States and EU should push for review and consultation clauses in ICT laws and regulations, which should be made standard on both sides of the Atlantic. Review clauses—which would require regular reexamination of ICT regulations—would compel regulators to think about whether the rule is effective, up-to-date, and consistent with the global regulatory landscape. Consultation clauses—required at the point of review—would write into law the necessity of examining and discussing regulation with international counterparts, while still respecting the democratic process and preserving the regulators' legitimate right to make rules in the public interest. Both of these clauses would help enshrine openness and flexibility in ICT regulation.

Step 6: Focus on joint US-EU impact assessments for proposed regulations and standards. The United States and EU should also develop joint impact assessments for proposed regulations and standards. Rather than focusing primarily on the alignment of rules, the United States and EU should channel more energy into joint impact assessments when regulators on both sides determine that rules will have a substantial impact on the transatlantic digital economy. By conducting impact assessments together, US and European regulators will have a better understanding of potential consequences of policy choices on the social, economic, and innovative environments. Joint impact assessments would also increase information sharing, provide a common lexicon of potential effects, foster a joint-assessment culture, and incorporate new actors into the regulatory process—particularly stakeholders like startups, SMEs, and civil society from the other side of the Atlantic. Joint impact assessments should not only draw on econometric analysis of a regulation's potential impact, but also on real-world implications, including clear assessments of possible effects on particular innovations, business models, companies, and citizens.

Step 7: Bolster efforts to increase tech literacy in the legislative branch. All too often, legislators have been the missing pieces in transatlantic regulatory cooperation. Tech literacy among legislators is low on both sides of the Atlantic, and legislation sometimes

33 Gerald Spindler and Christian Thorun, *Key Points of a Digital Regulator Policy*, (Berlin: Institut für Verbraucherpolitik, 2015), https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/dae-library/cornerstones_of_a_digital_regulatory_policy_-_executive_summary.pdf.
34 Ecommerce Europe, "Trustmark," http://www.ecommerce-europe.eu/trustmark.
35 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

GSM and the Early Mobile Phone Industry: A Case Study in Creating Global Standards

The spread of Global System for Mobile Communication (GSM) protocols for mobile phones in the 1990s is one example of how leadership and smart promotion can lead to a global ICT standard. In that case, the European Telecommunications Standards Institute (ETSI) benefited from the sophistication of Europe's early adopters, market size, and standard quality.[1] GSM adoption has rendered a large number of mobile phones interoperable. For customers using GSM, this interoperability has helped break carrier control, and allowed users to switch their SIM cards seamlessly between devices. Today, GSM is the default global standard, with a market share above 90 percent of the world's 3.6 billion cell phone users.[2] US policymakers opted not to mandate a single protocol at the time, preferring to allow a market-based standard to evolve in order to spur competition and innovation. It cannot be denied that Europe's decision to mandate a single transmission protocol was instrumental in catalyzing the nascent mobile marketplace.

1 European Telecommunications Standards Institute, *Cellular History.*
2 GSMA Associations, *The Mobile Economy 2015*, (London: GSMA, 2015), http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf.

lacks engineering, entrepreneurial, cybersecurity, and startup perspectives. The United States and EU should work with industry, academia, and civil society to create digital boot camps in Congress and the European Parliament (EP), to create greater expertise among legislators and their staffs on vanguard technologies, their potential applications, and the effects of regulation on tech development.

Both the United States and EU should also examine and promote efforts to embed tech fellows—including engineers and startup entrepreneurs—in congressional and EP committee staffs and personal offices. Tech fellows working on ICT legislation build on the "regulation by design" ethos by having tech-savvy individuals—often the object of the regulation—actively involved in the drafting of laws. Increasing the availability of digital boot camps and tech fellows will help break down barriers between Silicon Valley, London's Tech City, and Berlin on one hand, and Capitol Hill and Brussels on the other. This can also create a better understanding of cyber threat landscapes for frontier technology like the Internet of Things.

Congress and the European Parliament should also consider tasking the Congressional Research Service (CRS) and European Parliament Research Service (EPRS) with producing joint background papers on digital issues and legislation. Such joint papers will help ensure that the perspectives and concerns of the other side of the Atlantic are taken into account when elected officials are considering new legislation.

Step 8: Increase cooperation with state and local regulators on the other side of the Atlantic and highlight local best practices. Transatlantic cooperation on digital policy often focuses on the federal level in the United States, and the European level in the EU. This is appropriate, as the federal and European levels are the most influential hubs of regulatory decision-making. That said, the regulatory environment is multidimensional. Action at the state and municipal levels can also be useful in transatlantic partnerships. For instance, big-data solution centers established by local governments in Berlin and Dresden could provide lessons for US cities looking to promote usage of municipal open data in industrial and research fields.[36] Policymakers on both sides of the Atlantic should look for opportunities to expand regulatory partnerships and build coalitions beyond Washington and Brussels.

36 *OECD Digital Economy Outlook 2015*, p. 24.

Building a Cradle of Digital Innovation

The EU's Innovation Czar, Robert Madelin, recently said, "the most important thing 'Europe' creates is not the law but the space." The same is true across the Atlantic. Creating the space in which innovation can flourish is the cornerstone of the digital economy, but this space is mainly nurtured in the realm of domestic policy, largely cordoned off despite extraterritorial pressures from outside partners. In this context, the United States and EU must design an innovation landscape that encourages integration and avoids fragmentation. A continent isolated from global innovation and economies of scale is, by definition, limiting its technological, economic, and security potential.

Policy choices related to Internet infrastructure development, investment climate, conditions for startups, competition, and copyright law involve complex considerations. They touch on a host of vital domestic issues including: economic competitiveness; consumer protection; legal tradition; tradeoffs between incumbent and startup industries; education and skills availability; democracy and fundamental rights; and even quirks of history. That said, there is room for coordinated action. The United States and EU achieve the best outcomes when they can minimize fragmentation, smooth out divisions in the digital marketplace, and share policy lessons and best practices.

Startups

Key to digital innovation—and to economic growth overall—is establishing an environment in which entrepreneurs and startup companies can thrive. A review of the EU and US experiences shows that four principal public policy conditions are needed for startups to flourish: ease of market access; rules that encourage innovation; availability of startup capital; and a hiring environment that enables diversity, including through visa availability for high-tech workers.[37] That said, the United States enjoys certain natural advantages compared to other OECD economies, including the EU:

- **Market size:** The US market size makes scalability easier. Once a startup is a consequential player in the American market of 320 million consumers, it is well positioned to expand into other markets. While the EU's market is theoretically larger—if fragmentation were fully eliminated—European differences in language, culture, and online behavior remain.
- **Access to finance:** The United States has a mature culture in terms of venture capital (VC), angel investment, and crowdfunding, with almost six times more capital ($29.7 billion) than the EU, and three times as many investment rounds. Moreover, the amount of VC as a percentage of European GDP decreased steadily during the financial and eurozone crises.[38] European VC totaled $5.7 billion in 2012, with 1,074 investment rounds.
- **Complex support networks:** Complex innovation ecosystems in urban clusters, like Boston or Silicon Valley, often have state-of-the-art research universities at their core. Universities help attract and retain global talent at each stage of professional development: 52.4 percent of Silicon Valley-based startups are either founded or cofounded by non-US citizens.[39] Europe has started to follow suit with tech hubs, campuses, and accelerators, like Tech City in London, 42 in Paris, and the Factory in Berlin. The world's largest digital business incubator, La Halle Freyssinet, will open its doors to more than one thousand Paris startups in 2017.[40]
- **Higher risk tolerance:** The US tech sector's competitiveness has gained most attention from

37 In Germany, for instance, 22 percent of startup employees are not German citizens.

38 Arjun Kharpal, "Can Europe Compete with US Tech Startups?" CNBC, January 1, 2014, http://www.cnbc.com/2014/01/01/can-europe-compete-with-us-tech-startups.html.

39 Alan Gleeson, "Why Europe Lags the US in Technology Startups," *TechCrunch*, September 17, 2010, http://techcrunch.com/2010/09/17/guest-post-why-europe-lags-the-u-s-in-technology-startups/.

40 Le Halle Freyssinet, *1000 Start-Ups*, http://1000startups.fr/?lang=en.

stories of major successes, such as Google and Facebook, but the "graveyard of failures" has played an important role in creating industry champions. The higher tolerance for both entrepreneurial and capital risk remains a significant differentiation between the United States and Europe.

The EU's tech startup landscape is comparatively less developed, in part due to the factors above. However, European startups are showing leadership in fields like mobile gaming and "fintech," including apps, trading algorithms, and crypto-currencies that are transforming the financial system. Governments have devoted more resources to startup incubation, with some good results. France, for instance, has committed €200 million to a new hub intended to accommodate one thousand new startups. New pools of private capital have emerged in Europe, especially in London, Berlin, and Helsinki. While the United States accounted for 60 percent of global crowdfunding, the EU reached 35 percent in 2012, and that total is growing.[41] One side effect of high youth unemployment in cities like Madrid and Lisbon is a growing tolerance of risk among young entrepreneurs, giving rise to new pockets of dynamism. This changing environment is creating new European "unicorns" like the French ride-sharing company BlaBlaCar, and the German food-service app Delivery Hero.

But as the EU's startup community grows, it is confronting a policy environment that sometimes favors more heavily regulated incumbent industries. Several recent policies, including recent decisions on the EU's net-neutrality rules, have made clear the power of politically savvy, incumbent industries.[42] As a result, the startup community is now beginning to advocate in Brussels and other European capitals.

Internet Infrastructure

The United States and EU have developed distinct market structures, each working in some ways as a laboratory of policy choices. Nowhere is this more clearly demonstrated than in the regulation of Internet service provider (ISP) infrastructure. Demand on fixed and mobile broadband networks is growing at different rates across the OECD—but, in both cases, it is growing.[43] Additionally, governments are looking into greater deployment of fiber and spectrum resources to increase complementarity, optimize efficiency, and widen access to underserved populations.

The United States has created a multilevel market landscape that enjoys a high degree of both market consolidation and competition. The duopoly between cable and telecom companies, which have shifted their investment focus primarily to wireless, has forced ISPs to contend with competition across these modes of access. At the same time, sector consolidation has led to economies of scale, accelerating the deployment of high-speed Internet. While costs remain significantly higher for US consumers than EU consumers, due in part to market consolidation, US policymakers have worked to make high-speed Internet more accessible. In the 2009 stimulus package, the Obama administration included grants for broadband-infrastructure development and rules contingent on inclusion, increased access, and net-neutrality principles.[44] The FCC's 2010 National Broadband Plan envisions the release of 500 megahertz (MHz) of new spectrum for wireless broadband by 2020, with incentives to extend affordable broadband access to under-resourced communities.

Greater profitability also allows for greater flexibility in regulatory changes to broaden access, encourage innovation, and lead to changes in consumer behavior. The early availability and adoption of fiber, Long-Term Evolution (4G LTE), and other broadband infrastructure, for example, has led to increased availability of online video services such as Netflix and Hulu.[45]

The EU is a different story. The European marketplace is more fractured. On average, each member state—from Germany to Denmark—has at least four network operators. Consolidation is closely monitored.[46] Costs for EU consumers are lower than in the United States. The debate continues over the effect of market fragmentation in Europe. Although new market consolidation is beginning to take place in the European mobile market, the European telecommunications sector has not demonstrated equal levels of investment in next-generation infrastructure. Capital investment in Europe has lagged behind that in the United States, although new infrastructure-investment streams—up to $100

41 *OECD Digital Economy Outlook 2015*, p. 60.
42 The startup lobbies mushroomed in 2015. Among new Brussels-based advocacy groups are Allied For Startups' Brussels office, the European Tech Alliance, and the European Competitive Telecommunications Association (ECTA).
43 Demand on fixed networks has grown 3.7 percent, and on mobile networks at 14.2 percent. *OECD Digital Economy Outlook 2015*, p. 17.
44 Stephanie Condon, "Stimulus Bill Includes $7.2 Billion for Broadband," *CNET*, February 17, 2009, http://www.cnet.com/news/stimulus-bill-includes-7-2-billion-for-broadband./
45 According to one account, up to 35 percent of all Internet traffic by size can be attributed to video streaming via Netflix. Todd Spangler, "Netflix Video Puts Even More Strain on the Internet," *Variety*, May 14, 2013, http://variety.com/2013/digital/news/netflix-puts-even-more-strain-on-the-internet-1200480561/.
46 Ruth Bender and Shayndi Raice, "European Telecom Companies Race to Merge," *Wall Street Journal*, June 1, 2015, http://www.wsj.com/articles/european-telecom-companies-race-to-merge-1433160138.

An Angry Bird's Eye View of Mobile App Gaming

The global gaming industry reached $76 billion in 2015, and is expected to grow to $86 billion this year. While Japan, South Korea, and the United States remain major players in online and console gaming, European developers, most founded since 2009, hold a commanding position in the smartphone gaming landscape.

Two the so-called "three kings" of mobile gaming are European: King Games (Ireland), the largest developer of Facebook games and producer of Candy Crush Saga, with $2.26 billion in revenue in 2014; and Supercell (Finland), the Clash of Clans creator and current industry leader. Some of the sector's other European titans include Gameloft (France), Minecraft creator Mojang (Sweden), Kiloo (Denmark), Ustwo (UK), online game hub Aeria (Germany), and Rovio Entertainment (Finland), creator of Angry Birds, the most downloaded game series in history with more than three billion downloads. Even as European gaming companies have become acquisition targets for gaming companies outside of Europe, mostly from Japan, Europe remains the center of gravity for the mobile gaming industry.

billion since 2011—have begun to flow from content and application providers.[47]

Despite differences in ISP market structure, the United States and EU have both recently enacted policies to promote the concept of net neutrality—Internet infrastructure access based on the premise of nondiscrimination. Both sides of the Atlantic have converged around the principle, with targeted carve-outs around the management of online traffic. There are important differences, and US companies operating in Europe may face a different environment than at home, as will European companies operating in the United States. The outcome of these debates demonstrates the challenges of regulatory coordination across the Atlantic, and the flexibility required to operate in this space.

In the United States, the March 2015 FCC order established rules for what is and is not allowed in network management, on both fixed and mobile broadband networks. It prohibits blocking, throttling, paid prioritization, and discriminatory management of network traffic. The FCC also ruled that it has the authority to adjudicate matters involving ISP interconnection practices. [48]

In the EU, establishing net neutrality was part of the 2013 Connected Continent program. The approach reflects an inclination to tread lightly at the EU level, leaving national regulators to interpret definitions and exemptions. As such, the EU remains an uneven patchwork when it comes to net neutrality, reflecting many member states' national regulatory predispositions.

After months of debate and revision, the EU seems to have somewhat narrowed the gap between the EU and FCC interpretations of the extent to which network management can be permitted. However, important differences between US and EU approaches to net management remain and, in the United States, the rules are pending appeal in the court system.[49] Moreover, the drive by Europe's telecoms for specialized services that would allow for discriminatory prioritization of bits and bytes has led to broader exemptions in Europe's draft approach than in the US regulatory structure.

47 David Abecassis and Andrew Kloeden, "Content and Application Providers are Major Investors in the Networks that Make up the Internet," *Analysys Mason Quarterly*, October 13, 2014, http://www.analysysmason.com/About-Us/News/Newsletter/Internet-infrastructure-investment-Oct2014/.

48 Andrea Renda and Christopher Yoo, "Telecommunications and Internet Services: The Digital Side of the TTIP," *Center for Transatlantic Relations*, 2015, p. 8-9, https://www.ceps.eu/publications/telecommunications-and-internet-services-digital-side-ttip.; White House, *Net Neutrality: President Obama's Plan for a Free and Open Internet*, 2014, https://www.whitehouse.gov/net-neutrality.

49 Net neutrality will be tied up in the legal system for the next five to ten years, which will lead to diminished broadband investment.

Online Platforms

The European debate on online platforms remains highly dynamic, vigorous, and sometimes combative. The EU's DSM strategy states that the European Commission will undertake a "comprehensive assessment on the role of platforms." Some in Brussels, and in member states, have called on the EU to examine platforms as a public utility. Others, including some regulators and members of the European Parliament, have expressed interest in expanding the principle of neutrality to account for the way platforms—specifically search engines—govern traffic. The EU has demonstrated a willingness to address the issue of discriminatory search practices as a component of its competition investigation into Google.[50] The DSM, in its discussion of platforms, builds on member-state policy discussions concerning the role of online intermediaries in changing traditional modes of organization, fostering innovation, use of content generated by others, and making it more difficult for new market entrants to become players.

This debate has exposed a number of new divisions and evolving alliances: between intermediaries and content producers; between incumbent players and new entrants; between the United States and EU; and between different tech companies. The fault lines are not clean, but are concentrated largely in two policy domains. The first concerns the degree to which competition law is equipped to examine and address accusations of potential monopolistic behavior and market abuse by the Internet's largest players. The second involves the liability of online intermediaries disseminating content, and the use of illegal content.

In the competition space, online services and business models are raising new questions about the potential for monopolistic behavior and market abuse. Some observers believe that online platform services benefit from self-perpetuating network effects. Greater usage leads to better data and increased confidence in the service, which reinforces—by design—the propensity for future use. This can lead to questions about whether data monopolies exist and—to the extent that they do—can lead to anticompetitive behavior. If these concepts can be dealt with through the instruments of antitrust law, then platform-specific rules on market abuse should, in theory, not be necessary.

EU competition authorities differ from their US colleagues in their expectations for large companies with consequential positions in the European market. For instance, EU authorities focus primarily on a static concept of market dominance, and give less weight to the market dynamism in the online space that regularly wipes out companies in previously market-dominant positions. Dominant social networks, such as Friendster in 2003 and Myspace in 2007, have given way to Facebook, which, in turn, is yielding market share to Instagram and Snapchat. Search-engine companies that thrived fifteen years ago are limited players today. The Federal Trade Commission unanimously agreed that there was no need to take action, and that assertions about potential consumer and competitor harm were unfounded.[51]

As for copyright issues focused on responsibility for third-party content, both sides of the Atlantic recognize liability limitations for ISPs and platforms as an essential legal precondition for the Internet to develop into a flourishing marketplace. In the United States, broad immunity was granted to intermediaries under Section 230 of the 1996 Communications Decency Act, shielding platforms from legal exposure as a result of user behavior. The Digital Millennium Copyright Act (DMCA) builds on this by reaffirming the liability protections for intermediaries, paired with a clear notice-and-takedown regime for when intermediaries are notified by rights holders. The EU's 2000 e-Commerce Directive followed a roughly similar legal philosophy. This body of law limits the obligations for intermediaries to monitor and filter user activity, limiting the administrative burden, upholding user privacy, and allowing an open and vibrant online environment to thrive.

Under pressure from publishers and some EU member states, the commission's DSM is revisiting some of these previous assumptions—opening up the discussion on the possibility of implementing a "duty of care" for Internet intermediaries. The "duty of care" provision could effectively eliminate the liability carve-outs that intermediaries currently enjoy. New calls have also come from some national governments to enlist intermediaries in enforcing laws on hate speech, speech to incite violence, and terrorist communications.

The willingness to review liability protections granted to guard intermediaries from user behavior has raised alarm bells in some corners, both in Europe and in the transatlantic space. It would place immense burdens on ISPs and platforms to monitor content passing over their networks, and could discourage new platform startups unable to overcome costly administrative hurdles. Removing those protections could also lead to a chilling effect on speech—on the part of users, worried that

50 Renda and Yoo, "Telecommunications and Internet Services," p. 13.

51 Dennis Schaal, "Priceline.com CEO on the Death of Search Engine Optimization," *Skift*, October 20, 2015, http://skift.com/2015/10/20/priceline-com-ceo-on-the-death-of-search-engine-optimization-rip/.

legitimate speech activity might violate copyright laws; and on the part of intermediaries, who would likely more zealously police and take down possibly even lawful content, in order not to run afoul of their responsibilities. It could dry up new seed funding for startups, as investors weigh legal risks involving consistent monitoring of content, and the costs associated with each slipup.[52]

Moreover, making platforms and ISPs liable for content could open a Pandora's box for the global Internet, imbuing ISPs with a troubling degree of power by placing them in the position to screen all content—and opening them up for abuse by authoritarian regimes interested in cracking down on free speech, democratic debate, and civil society. As the debates surrounding the US Stop Online Piracy Act (SOPA) and PROTECT IP Act (PIPA) and the EU Anti-Counterfeiting Trade Agreement (ACTA) demonstrate, the political climate on both sides of the Atlantic has little tolerance for deputizing ISPs and platforms to police copyright violations. That said, both the United States and EU have strong creative sectors—publishers, artists, musicians, and filmmakers—whose output should be protected, and whose rights over content they produced have been codified in both international and domestic law. US and European lawmakers must ensure a proper balance that continues to promote innovation and incentivizes new artists, writers, and journalists by protecting their work.

Most responsibility for incubating the right conditions for innovation lies in efforts undertaken domestically. But the Atlantic partners should compare experiences and best practices on these policies. In a few areas, they might find possibilities for joint efforts aimed at unleashing innovation and setting the standards for other digital economies.

Step 9: Support a startup culture by promoting laws that open up access to finance and creating one-stop shops that cater to new companies looking to expand. The United States has six times the level of the EU's startup VC. US venture capitalists are private individuals rather than banks, which tend to be more risk averse and require collateral, which most digital startups do not have. Moreover, serious regulatory gaps exist in the ability to pursue equity crowdfunding in the areas of liability, fraud, taxation, registration, and reporting.[53] The EU and its member states can draw lessons from each other, and the United States, on increasing the accessibility of private-sector finance. The Jumpstart Our Business Startups (JOBS) Act offers one model, as it eases securities regulations for SMEs and startups by increasing the number of shareholders required before a company must register with and report to the US Securities and Exchange Commission (SEC). This then creates exemptions from investor accreditation, making equity crowdfunding easier.[54] Other models have been implemented in Poland and the United Kingdom, which have updated capital-market regulations and made it easier for startups to raise capital outside of traditional banks. At the EU level, completing the proposed Capital Markets Union (CMU) could reduce national barriers to investment and financing, making a wider pool of funds available for European startups.

Startups can also benefit from the creation of one-stop shops and other adaptable regulatory regimes that allow access to the entire EU market with simple, straightforward value-added tax (VAT) requirements, corporate registration, and licensing. For example, Estonia has an uncomplicated e-residency portal that allows individuals to: establish an Estonian company online; digitally sign, encrypt, and transmit documents; conduct banking; and declare taxes.[55] It is a great portal for startups within Europe, as well as those aiming to enter or expand in the EU market.[56] The European Commission is considering similar proposals that would simplify the registration of one-person, one-euro companies through a proposed directive that would allow member states to create *societas unius personae* (SUPs), thus harmonizing the main requirements for setting up shop in an EU member state. The US startup community should share its experiences with the EU and member states as they set up the SUP regime.[57]

52 Daniel O'Connor, "The Digital Single Market and a Duty of Care: Preserving the Transatlantic Legal Foundation of a Thriving Internet," *Disruptive Competition Project*, July 9, 2015, http://www.project-disco.org/competition/070915-the-digital-single-market-and-a-duty-of-care-preserving-the-transatlantic-legal-framework-for-a-thriving-internet/#.VszcYvkrLcs.

53 Garry A. Gabison, *Understanding Crowdfunding and its Regulations*, (Seville, Spain: European Commission, 2015), p. 21-22, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC92482/lbna26992enn.pdf.

54 Amir Mizroch, "Europe's 2015 Tech Startup Landscape," *Wall Street Journal*, February 18, 2015, http://www.wsj.com/articles/europes-2015-tech-startup-landscape-1424300739.

55 "Estonian e-Residency," *e-Estonia*, https://e-estonia.com/e-residents/about/.

56 Robin Wauters, "15 European Startup Associations Unite to Urge Commission to Put Innovators at Heart of Digital Single Market Strategy," *Tech.eu*, May 4, 2015, http://tech.eu/news/european-startup-associations-digital-single-market-letter/.

57 European Commission, press release, "Proposal for a Directive on Single-Member Private Limited Liability Companies—Frequently Asked Questions," April 9, 2014, http://europa.eu/rapid/press-release_MEMO-14-274_en.htm.

Step 10: Ensure that nascent net-neutrality regulations minimize fragmentation between the United States and Europe. The legal ambiguities and uneven timing of the litigation process on net-neutrality regulations could lead to coordination difficulties in the transatlantic space. That said, this regulatory frontier also offers an opportunity as rules on both sides are established and settled over time. For example, both the FCC and EU should provide space for implementation of the rules in a way that best achieves their intended outcome, and avoids cutting off potential future innovations. US-EU coordination on both governing practices and outcomes could do much to minimize fragmentation and arbitrage.[58] The EU is already working to head off market fragmentation across Europe as it creates its implementation guidelines. Efforts should be extended informally, but institutionally, across the Atlantic.

Step 11: Use investment funds and spectrum allocation as instruments that encourage early adoption of frontier technology and foster the industrial Internet. Both the United States and the EU, along with EU member states, can enhance the use of public investment and spectrum choices to catalyze industrial policy based on cloud computing, big-data analytics, and the Internet of Things. EU research and development (R&D) mandates have been established in the Horizon 2020's Seventh Framework Program (FP7), DG CNECT, and the EU's broad goals for economic competitiveness.[59] The United States should also use its massive R&D weight—for example, in the procurement and hiring arms of the Department of Defense—to help drive an ICT industrial policy based on the Internet of Things.[60]

Step 12: Launch joint reviews of major future policy issues, like the labor-market effects of the Internet of Things and the sharing economy, and the potential impact of crypto-currencies on the transatlantic market. Just as manufacturing has given way to the service industry as the base for transatlantic employment, the Internet of Things and the sharing economy will also lead to immense restructuring of the labor market. Already, Internet-enabled driving and hotel services, pet sitting, and lending—along with car, bike, and apparel sharing—are altering industrial-era labor models, with implications for wages, retirement, worker protections, and on-the-job liability. The Internet of Things is further compounding labor-market transformation. For instance, self-driving cars will reduce the number of truck and delivery driving jobs, which were the most common type of job in twenty-nine of the fifty US states in 2014.[61] Networked devices will displace low-skilled, service-sector jobs in other sectors on both sides of the Atlantic as well. The United States and EU should launch a joint assessment of the economic impact of these twin developments on the labor market, and examine strategies that balance innovation and labor-market resilience.

They should also examine—perhaps in a future Digital Council—the potential impact of crypto-currencies and smart contracts on the transatlantic financial market. Crypto-currencies and block-chain technology are primed to have the same transformative impact on financial services that Uber and Lyft have had on the car service and taxi industry, and that Airbnb has had on the hotel industry. Both sides of the Atlantic will see new models for transforming lending, credit, payments, and mortgages. The Federal Reserve, the European Central Bank (ECB), private banks, and financial institutions have long had a dialogue on regulatory approaches to block-chain technology and other crypto-currency arrangements. US and EU policymakers—as well as civil society, academia, and other stakeholders—should expand that dialogue into a more comprehensive review of the impact of such "fintech" on the transatlantic financial system.

Step 13: Expand transatlantic antitrust dialogue to address questions about the digital economy and US and EU regulatory approaches. Antitrust authorities at the Justice Department and Directorate General for Competition (DG COMP) have one of the most sophisticated and deep relationships of any transatlantic government agencies. Transatlantic trust, information sharing, and support for intervening against market abuse is a model for other regulators. The two sides should complement their operational cooperation with greater dialogue on the approach to be taken with the digital sector, where market definitions are less clear and competitive pressures more diverse, incumbency is limited, and market dynamism is unprecedented. Establishing a common understanding of if and when it might be appropriate to intervene in the digital market will greatly enhance the predictability, certainty, and dynamism of the transatlantic digital marketplace.

58 Renda and Yoo, "Telecommunications and Internet Services," p. 11.
59 This includes effectively Europeanized German industrial policy—Industrie 4.0—as it relates to creating an ecosystem of cloud computing, automated command and control, deployment of sensors, and robotics.
60 US Department of Defense, *Fact Sheet: Building the First Link to the Force of the Future*, November 18, 2015, http://www.defense.gov/Portals/1/features/2015/0315_force-of-the-future/documents/FotF_Fact_Sheet_-_FINAL_11.18.pdf.

61 Quoctrung Bui, "Map: The Most Common* Job In Every State," *NPR*, February 5, 2015, http://www.npr.org/sections/money/2015/02/05/382664837/map-the-most-common-job-in-every-state.

Reinforcing Transatlantic Data Protection and Privacy

The Internet economy and open data flows are predicated, more than anything, on digital trust. Discussions on data protection and privacy are perhaps the most charged in the transatlantic digital discourse. Commercial policy and the desire to protect personal data—from identity theft, organized crime, and nefarious states—intermingle with: concerns about NSA surveillance; the European perception, accurate or not, that American tech business models render personal data a commodity; and the counter perception that European data laws are a disguised form of digital protectionism. In reality, US-European differences on data protection stem from a fundamental philosophical divergence on the legal interpretation of privacy rights.

In the United States, the right to privacy stems from the Fourth Amendment's protection of individuals, their "houses, papers and effects against unreasonable searches and seizures."[62] Privacy, itself, is not explicitly enumerated in the US Constitution. Its interpretation in US law has developed through judicial cases and legislation addressing issues related to government searches. In commercial contexts, privacy has developed in the realm of cooperative regulation and company-based standards and terms of service, and across a patchwork of federal laws in discrete areas like health (HIPAA), finance (FATCA), and minors (COPPA), company-based standards and terms of service, and cooperative regulation.

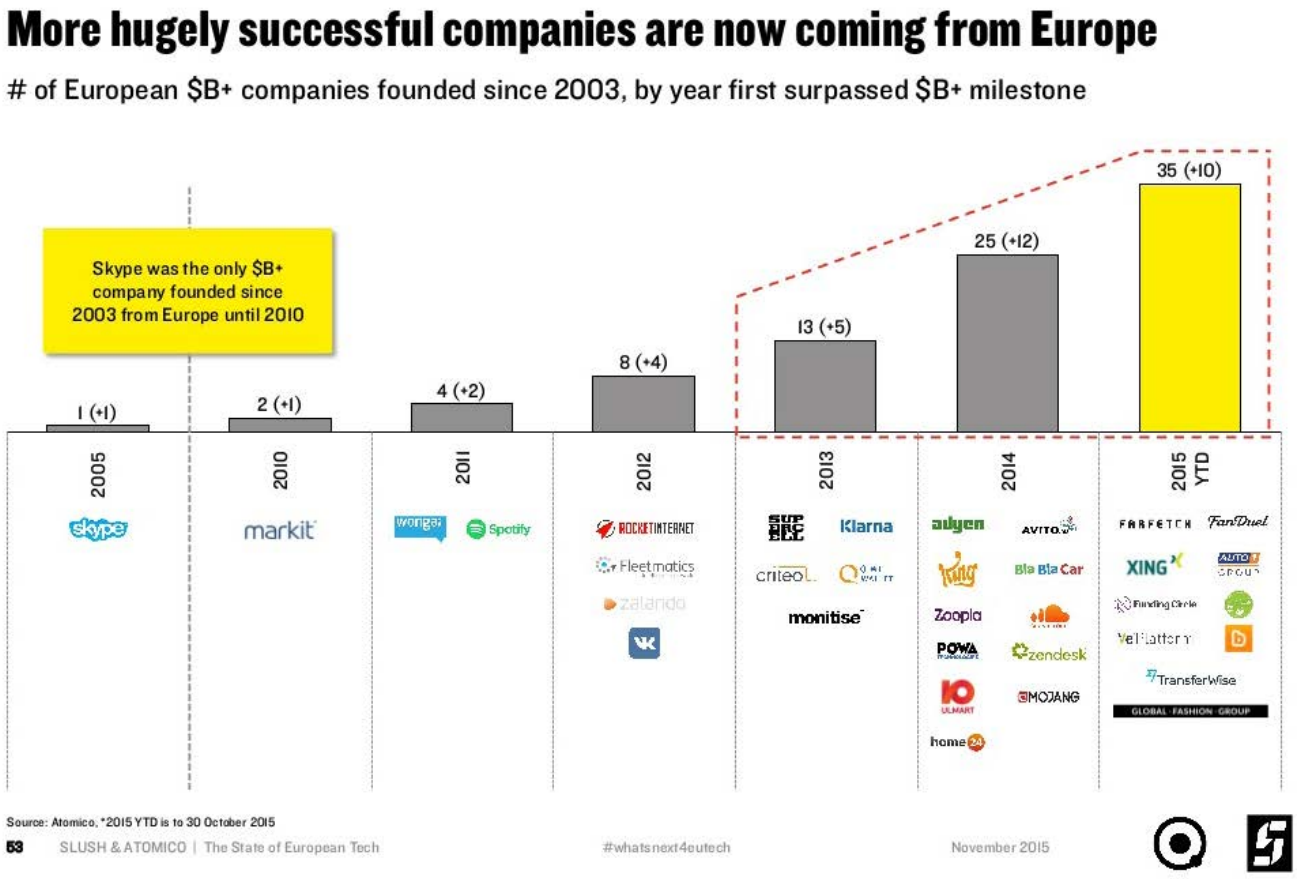
The EU Charter of Fundamental Rights enshrines a dignity-based conception of two separate rights—to privacy and to the protection of personal data.[63] This dignity-based model of data privacy and protection arises from the German legal tradition of *Informationelle Selbstbestimmung,* which establishes a form of personal control over an individual's data use at every step in one's digital life. In effect, personal data becomes almost like a "digital appendage."

Differences between the two sides extend beyond legal philosophy. While US laws cover discrete patches, like health, with court rulings gradually building out other protections, the EU's legal instruments for enforcing these protections—the 1995 Data Protection Directive, the 2002 e-Privacy Directive, and the General Data Protection Regulation (GDPR)—establish high-standard, blanket protections for personal data, cutting broadly across all swaths of daily digital life. This understanding of privacy applies to the use, processing, control, and transfer of data for commercial purposes by companies. It also applies to the activities of governments, international organizations, and other public actors, although there are exemptions related to security, law enforcement, and economic welfare.

The US-EU data-protection and privacy relationship has essentially been focused on creating interoperable bridges between these two entrenched philosophical traditions. These sometimes-prickly negotiations have cut across a range of policy areas where law enforcement, national security, and free transatlantic commerce collide—including terrorist financing (2010 Terrorist Finance Tracking Agreement), passenger travel (2012 Passenger Name Records Agreement), and, most recently, a broad, turnkey agreement on data sharing between law enforcement (2015 Data Protection and Privacy Agreement). The US-EU information-sharing architecture has focused on ways to keep the treatment of personal data proportional, retention limited, and transparency and recourse avenues ample for citizens on both sides of the Atlantic.

In the commercial space, the 2000 Safe Harbor agreement—along with other EU-sanctioned instruments, like binding corporate rules and model clauses—served as the primary portal through which US companies participate in the transatlantic data economy. The Snowden revelations left a digital sword of Damocles hanging over US-European exchanges of personal

62 Renda and Yoo, "Telecommunications and Internet Services," p. 21.
63 European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*, April 2014, https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf.



Source: SLUSH and ATOMICO, The State of European Tech.

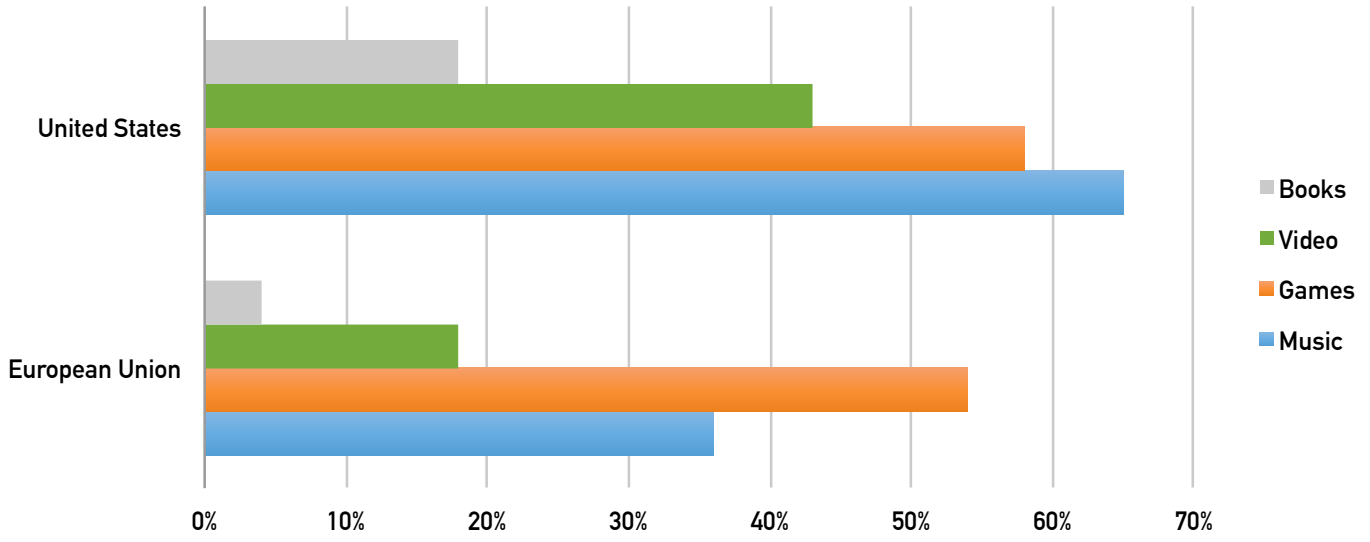
data. Following the 2013 Snowden revelations, the European Commission released a series of thirteen recommendations aimed at enhancing assurances in the data-flow corridor. These included greater transparency for self-certified companies and access to dispute-resolution mechanisms for European consumers. In February 2016, Congress passed the Judicial Redress Act, providing European citizens with new access to the US judicial system to address claims of abuse to their personal data.

The October 2015 *Schrems* decision in the EU Court of Justice (CJEU) invalidated Safe Harbor, asserting that protections offered by US companies to Europeans' personal data were not "essentially equivalent" to those under the EU's Data Protection Directive. The decision also granted national data-protection agencies greater authority to exercise oversight. This came despite efforts by Congress and the administration to pare bulk data collection, introduce new checks and requirements on the need for data collection, add new forms of judicial recourse and transparency, and expand the rights of foreign nationals.

The landmark US-EU Privacy Shield Agreement, agreed to in February 2016, addresses the most acute issues that the CJEU raised in its October ruling. It establishes tougher, binding commitments for companies, enforceable by the Federal Trade Commission (FTC) and monitored by the US Department of Commerce. The agreement creates new checks, proportionality requirements, and safeguards that limit dragnet data collection for national security. It also mandates a host of new redress possibilities for European citizens, including through US companies, European data protection authorities (DPAs) with the Commerce Department and the FTC, and a new State Department ombudsman slated to field Europeans' requests related to national security.

Still, several questions remain. For instance, even with newly written guarantees limiting their scope, data-collection and surveillance activities by the intelligence community—including the NSA—will continue. Oversight of this collection by the State Department ombudsman will necessarily be limited. Second, under Safe Harbor, companies certified their own compliance. While cases have been brought by the FTC against at least

Digital Shares of Content Markets (2013)



Source: OECD, OECD Digital Economy Outlook 2015.

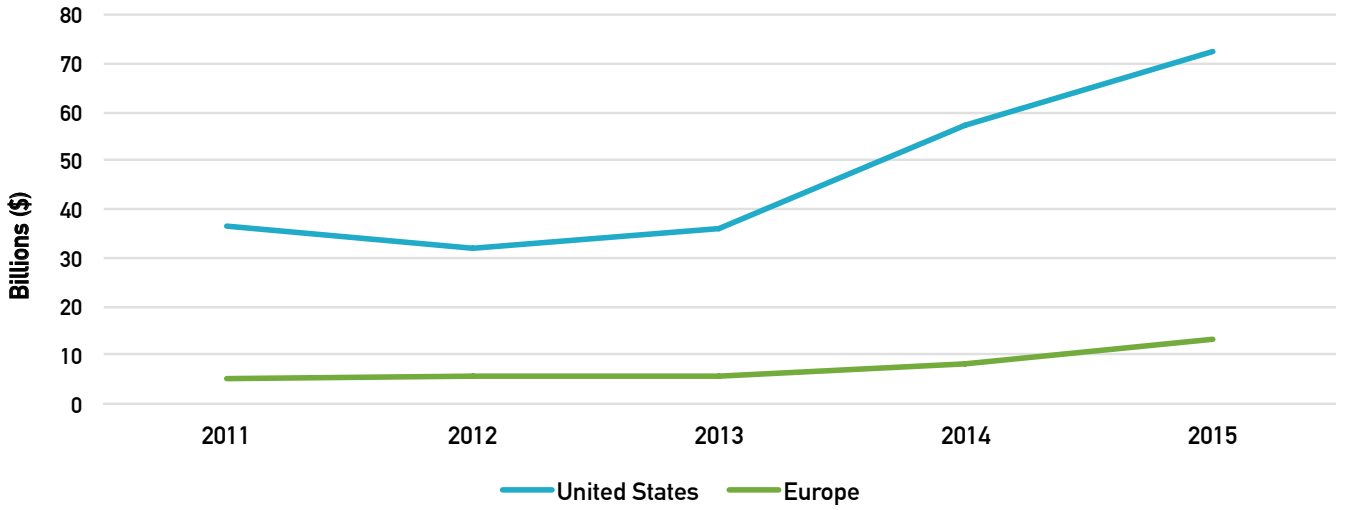
ten companies, the perception in Europe remains that voluntary compliance with Safe Harbor provisions was not vigorously enforced. Even with a more muscular enforcement framework, the fact remains that US agencies will be responsible for enforcement that could raise doubt about the independence and DPA involvement in how compliance is monitored, enforced, and prosecuted. New legal action questioning the European Commission's decision to grant adequacy through the Privacy Shield is inevitable.

At the same time, the EU's massive overhaul of its domestic data-protection law has implications for the transatlantic digital relationship. The GDPR—the most amended piece of legislation in EU history—has given rise to some of the most raucous domestic and transatlantic challenges. GDPR provisions include: stringent bookkeeping requirements for companies to demonstrate that they are in compliance with GDPR; breach notification within seventy-two hours; openness to the possibility of individual EU member states requiring companies to assign in-house data-protection officers; and a codification of the "right to be forgotten," introduced as an implicit right in a 2010 CJEU ruling. The consequence for noncompliance could be enormous—up to 4 percent of a company's annual global turnover.

The GDPR places heavy responsibility on intermediaries as the gatekeepers of data. For example, they will determine whether takedown is appropriate under right to be forgotten requests, often with insufficient direction from regulators. Thus, the incentive is to err on the side of takedown, yet the effect could be a significant degradation of the flow of information. GDPR also waters down the one-stop shop for data regulation, by opening up companies to multiple interpretations of data-protection regulations while they operate in multiple jurisdictions. Moreover, it pays limited attention to frontier data areas, like artificial intelligence and the Internet of Things, which could render the GDPR brittle, and quickly out-of-date. At the same time, the GDPR's regulations could be a significant burden for nascent sectors, startups, and technologies. The GDPR does not change the principle that European personal data must remain within EU territory—unless the recipient country's legal protections are deemed "adequate" by the European Commission, or where legal safeguards are sufficiently high to ensure protection of personal data. The CJEU ruling has injected new uncertainty about the conditions under which adequacy can be conferred on the United States or any third-country jurisdiction.

The constraints on cross-border data-flow disruption could be particularly damaging. A 2013 study by the European Center for International Political Economy (ECIPE) found that in a doomsday scenario—a full break in the transatlantic digital services and cross-border data flows, including the elimination of Safe Harbor, binding

Total Amount of Venture Capital ($ billions)



Source: OECD, OECD Digital Economy Outlook 2015.

corporate rules, and model contract clauses—would cost EU GDP between 0.8 and 1.3 percent.[64]

At the same time, Europe is reexamining whether its intelligence-collection and intelligence-sharing regimes work in the wake of the January 2015 Charlie Hebdo attack and November 2015 ISIS-affiliated attacks in Paris. New counterterrorism and intelligence policies cannot be considered apart from the EU's internal data-protection policy or the adequacy expectations the EU and its member states have for allies and economic partners. Creating inconsistencies between member states' national-security and intelligence laws and EU-level digital market rights and regulations will rip deep fissures in the fabric of the European, and global, digital economy. The EU and its member states must work to reconcile these contradictions, in order to preserve their place at the cutting edge of the digital marketplace.

The task of creating a resilient, interoperable transatlantic data environment—with protections and privacy guarantees that are consistent with the GDPR and the Privacy Shield Agreement—will require the United States and EU to step up cooperation. This will mean finding a way forward in a very complex environment, as the threat of terrorist attacks and online recruiting by ISIS become more acute.

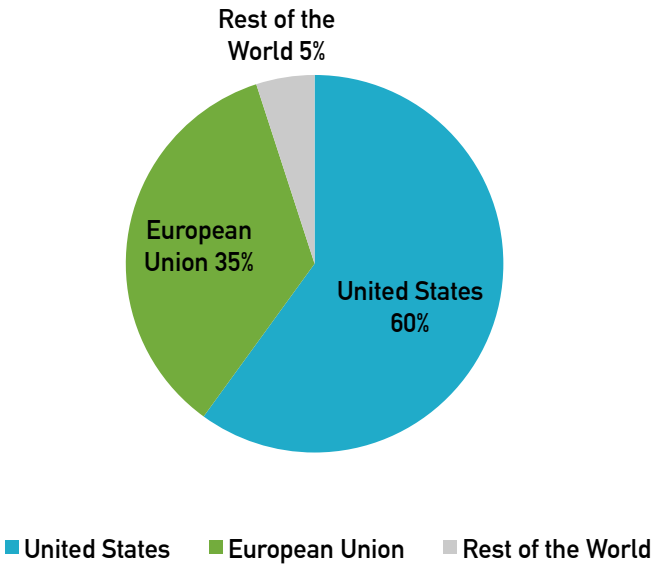
Step 14: Play an active role in revision of the Council of Europe's Convention 108. The 1981 Convention 108 for the "Protection of Individuals with regard to Automatic Processing of Personal Data" was the first legally binding instrument guaranteeing an individual right to personal-data protection, and setting baseline standards for data protection. The Convention was deliberately designed to allow non-European states to become signatories (currently only Uruguay has done so). The United States—along with other like-minded countries, including Canada and Australia—has been a party to negotiations related to the convention and its implementation since the beginning. As the Council of Europe is currently looking to update that convention, the United States should play an active role in its revisions, with the intention of eventually ratifying it. There is precedent for this. The US Senate ratified the Budapest Convention (185) on Cybercrime by unanimous consent in 2006.[65] Ratification of a legally binding convention would take immense political will, given the current congressional climate, but the United States should have that as its eventual goal.

Step 15: Expand the discussion on thresholds and legal distinctions for personal data for the era of the Internet of Things and big data. Definitions related to "data subjects" and "personal data" will be central for determining the treatment of data under the GDPR and the Privacy Shield. As big-data analytics and the Internet

64 Matthias Bauer, Fredrik Erixon, Michal Krol, Hosuk Lee-Makiyama, and Bert Verschelde, *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce* (Brussels: European Centre for International Political Economy (ECIPE), March 2013), https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

65 All members of the Council of Europe, except Turkey, have signed and ratified Convention 108, the most recent being Russia in September 2013 and San Marino in September 2015.

Share of Global Crowdfunding (2013)



Source: OECD, OECD Digital Economy Outlook 2015.

of Things—self-driving cars, networked appliances, sensors monitoring households—become more commonplace, the volume of data collected can make it easier to identify individuals, even if personal data is absent from singular data points. Similar to pieces in a jigsaw puzzle, personal identities emerge from the overlay of multiple datasets. This opens up a host of new questions about the thresholds at which a data cluster goes from being non-personal to personal, as well as the ownership of data and the benefits for society as a whole from the nonproprietary use of big data.[66]

US and EU companies will both use networked devices, manage commercial supply chains, and benefit from the analysis of billions of data points to improve citizens' lives. Thus, the United States and EU should exchange information on definitions of different classes of data, the conditions under which the line between industrial and personal data is crossed, the proper means for de-identifying data, and what that means for data treatment. Such an approach could assist in improving US-EU interoperability regimes without necessarily harmonizing rules in this space.

Step 16: Explore discrete sectoral confidence-building measures (CBMs) centered around users access to personal data, user privacy, and user security. The United States has a broad array of sector-specific laws on data protection that could act as useful nodes for transatlantic cooperation. Many of these laws create potential bridges for discrete US-EU data-protection cooperation. E-health, for example, is ripe for new work together.[67] The United States and EU could expand their e-health memorandum of understanding (MoU) roadmap to include interoperable e-health records that allow patients eased access, portability, high breach-security requirements, and control over their health data.[68] The Blue Button model—launched as part of the US "My Data Initiative" to give US patients greater access and control of their personal medical records—could serve as the basis for interoperable, portable policies in the transatlantic space. European states—for example, Germany, Austria, and Italy—have already worked on similar measures to deploy e-medical histories, electronic prescriptions, and doctors' appointment planning, with added emphasis on interoperability and potential data-security risks.[69] Other transatlantic efforts could focus on energy data—working with the National Institute of Standards and Technology (NIST) to refine and internationalize smart metering data records like the "Green Button" initiative, an effort to provide households with better access to energy-consumption data.[70] Others could focus on the protection of minors, discussing ways to limit monetization of children's data, and aligning right to be forgotten laws and best practices for minors.[71]

Step 17: Integrate cybersecurity more fully into transatlantic discussions on privacy policy. The nexus between privacy and data protection is currently underserved in transatlantic policymaking. The policy narrative around security and privacy often pits the two against each other—or avoids the IT-security aspect altogether—when, in fact, they are mutually reinforcing.

66 The EU's free flow of data initiative is looking to guarantee that legal and technical obstacles to data flows—for reasons other than personal data protection—do not encumber data movement across borders. This is particularly true in cloud computing, where limitations on portability, certification, and ownership hamper cloud adoption and prevent the market from knitting itself together. European Commission, *A Digital Single Market Strategy for Europe,* May 6, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192.

67 In 2017, Europe is predicted to have the largest market for mobile health apps ($6.7 billion), followed by East Asia ($6.8 billion) and North America ($6.5 billion). Doctors, hospitals, and researchers are already pioneering new life-saving uses and analysis of data. In 2012, apps to track health indicators, such as exercise and caloric intake, reached 69 percent of American smartphone users.

68 European Commission, *Transatlantic Cooperation Surrounding Health Related Information and Communication Technologies*, October 17, 2010, https://ec.europa.eu/digital-agenda/en/news/transatlantic-cooperation-surrounding-health-related-information-and-communication-technology.

69 *OECD Digital Economy Outlook 2015*, p. 32.

70 Two California utilities—Pacific Gas and Electric and San Diego Gas and Electric—rolled out Green Button models for household consumers in 2012.

71 For instance, California's Senate Bill 568 is one example of a baseline version of the right to be forgotten, for minors' posts on social media like Facebook.

Cultural differences in business management between the United States and EU persist.[72] For instance, data privacy officers (DPOs) are more likely to be integrated into boardroom-level decision-making in many European companies than are information technology security officers (ITSOs), those meant to protect systems from cyberattacks and manage breaches when they occur. Legal requirements for DPOs, built into the GDPR at the European level and the national level in states like Germany, perpetuate and harden these imbalances.

Transatlantic policymakers must work to correct these imbalances and elevate the cybersecurity dimension into policy discussions on privacy. Global Internet policy would benefit from a deeper dive into how to best integrate cybersecurity into policy on the fundamental rights of a digitized economy. One initial area worthy of transatlantic exploration is cyber hygiene standards, where small, diffuse steps could prevent low-level attacks and better protect personal data.[73]

72 This is partially a cultural phenomenon. Many of the most high-profile breaches by cyber criminals and nefarious states have happened against US-based entities, including Home Depot (January 2014), Staples (December 2014), CareFirst Blue Cross Blue Shield (May 2015), UCLA Health Care (July 2015), and the Office of Personnel Management (April 2015).

73 Hannah Kuchler, "Security Execs Call on Companies to Improve 'Cyber Hygiene,'" *Financial Times,* April 26, 2015, http://www.ft.com/intl/cms/s/0/8468cfda-e9e3-11e4-a687-00144feab7de.html#axzz427JkGj5l; Sophia Antipolis, "ETSI to Develop European Standards for Cybersecurity," *ETSI*, March 28, 2014, https://www.etsi.org/news-events/news/769-2014-03-etsi-to-develop-european-standards-for-cybersecurity.

Leading in Global Internet Governance

The United States and Europe have been working to realize two mutually reinforcing objectives on the global stage: defending and enhancing a multi-stakeholder system of Internet governance so that decision-making remains with a consortium of stakeholders and not under control of governments; and unleashing the Internet's social and economic potential—and through it, joint ownership of Internet governance—for middle- and low-income countries and their citizens.

Even as global Internet traffic is growing at 20 percent annually, 60 percent of the global population remains offline, with Internet penetration as low as 5 percent in some of the poorest countries. [74] The Internet's economic dividends remain unevenly distributed. Countries—often from middle- and low-income economies positioned to benefit most from an open Internet—have questioned whether the bottom-up stakeholder approach biases the system of governance and allows the United States to exert undue influence over the future of the Internet. National security, law enforcement, freedom of expression, and other concerns have led some governments to push for more national-level control over the Internet's strategic functions.

Russia and China have sought to use this sentiment to redirect Internet governance toward a top-down, state-centric approach. Notably, this approach emerged at the 2012 World Conference on International Telecommunications (WCIT) in Dubai, an intergovernmental summit run by the International Telecommunications Union (ITU) that outlined a new body of international telecommunications regulations.[75] The ITU recommendations galvanized the United States, EU, and a majority of regulators, companies, and civil-society organizations that recognized the potential for abuse. They recognized that some actors might be tempted to assert repressive control, roll back free expression and commerce, extract rents, or fuel corruption.[76]

Since the 2012 summit in Dubai, key swing states in the global South have changed their outlook on Internet governance as their populations have become more digitally dependent, and as governments have begun to see the practical benefits of involving nongovernmental stakeholders in the digital policymaking process. Brazil has taken an active role in this regard, hosting the stakeholder-driven 2014 NETMundial and 2015 Internet Governance Forum (IGF) conferences, and engaging in debates similar to those in the transatlantic space over surveillance, data localization, democratic Internet governance, and startups.[77] India has followed suit, supporting this model and embarking on an ambitious and collaborative domestic agenda for Internet development.

Finally, in 2015, the UN-based review of the outcomes of the World Summit on the Information Society (WSIS) process confirmed these trends toward support for a multi-stakeholder model of governance that incorporates all actors, while making Internet access and connectivity key priorities. In renewing the mandate of the IGF—a multi-stakeholder forum for discussing global Internet policy—the UN General Assembly, as part of the WSIS review, reaffirmed these values.

In 2016, transatlantic leadership will be required to tackle the challenge set by the UN at the WSIS review. In a key step, the United States is slated to relinquish its oversight over the Internet Assigned Numbers Authority (IANA)

74 *OECD Digital Economy Outlook 2015*, p. 46; McKinsey Global Institute, *Offline and Falling Behind: Barriers to Internet Adoption*, October 2014, p. 2, http://www.mckinsey.com/industries/high-tech/our-insights/offline-and-falling-behind-barriers-to-internet-adoption.

75 International Telecommunication Union, *Final Acts: World Conference on International Telecommunication*, December 14, 2012, http://www.itu.int/en/wcit-12/documents/final-acts-wcit-12.pdf.

76 Emily Taylor, *ICANN: Bridging the Trust Gap* (Waterloo, Canada: Centre for International Governance Innovation and Chatham House, 2015) no. 9, pp. 3-4, https://www.cigionline.org/sites/default/files/gcig_paper_no9.pdf.

77 Melody Patry, "Internet Governance: Brazil Taking the Lead in International Debates," *Xindex*, June 16, 2014, https://www.indexoncensorship.org/2014/06/internet-governance-brazil-taking-lead-international-debates.

China's Digital Dilemma

Even as the UN's December 2015 World Summit on the Information Society (WSIS) meeting wrapped up with an inclusive, multi-stakeholder vision for the next ten years of Internet governance, China held its own state-centric counterpoint—the World Internet Conference (WIC).[1] WIC had all the trappings of China's contradictory approach to Internet policy, one of tight control at home while taking advantage of the Internet's global openness.

As digital activity booms, China ranked dead last out of sixty-five countries in a 2015 report about freedom on the Internet.[2] This double standard was even on display at the WIC conference itself, where Chinese attendees remained locked behind the "Great Firewall," as foreign participants were given special access to an uncensored Internet so they could post messages on Twitter and Facebook, post to YouTube, and use Google.

China's Internet companies are bumping headfirst into a regime determined to increase state control, suppress dissent, and police opinion online. China's "Great Firewall" is eroding Internet speed, negatively affecting 86 percent of surveyed businesses. Government regulators have been inconsistent in their approach to regulation involving car-hailing apps, e-commerce in counterfeit goods, and online credit cards.

With 641 million Internet users—19 percent of all users globally—China is too important to ignore. But in bringing it into the global digital economy and Internet governance, both China and its partners are confronted with a dilemma: how to socialize China into an open, free Internet, without allowing that Internet to be co-opted to lend legitimacy to China's system of double standards.

1 President Xi confirmed China's intention to tighten censorship and Orwellian assertions about the need to "purify the Internet," all while echoing the rhetoric of a "multilateral, democratic, and transparent" Internet.
2 Freedom House, *Freedom on the Net 2015,* https://freedomhouse.org/report/freedom-net/freedom-net-2015.

to a global multi-stakeholder stewardship community. The transition process recognizes management of the Internet's core functions—the domain name system (DNS) root zone, numbering, and Internet protocol parameters—as a global public good that should not be under the exclusive control of any government or group of governments. The Internet's legitimacy, interoperability, and continued openness are best reinforced through broadly based, multi-stakeholder control.[78] The US Department of Commerce's National Telecommunications and Information Administration (NTIA) currently manages the contract with the Internet Corporation for Assigned Names and Numbers (ICANN) to perform the IANA functions. NTIA has articulated four conditions for the transition: preserving the multi-stakeholder—rather than intergovernmental and state-centric—system of governance; protecting the Internet DNS; maintaining Internet performance that meets the needs of all global users; and guaranteeing the Internet's first principles, such as openness.[79] The IANA Stewardship Transition Coordination Group (ICG), responsible for managing the process, has generally received high marks from governments, business, and civil society for its transparency and inclusiveness.[80]

For such a model to work, increasing international trust in ICANN is also key. Civil society, businesses, and governments in the United States, EU, and elsewhere have taken great care to guarantee that power

78 IANA has approved and registered 1,034 top-level domains, including: country-code top-level domains (TLDs) like .uk, .eu, and .de; generic TLDs (gTLDs) like .com and .org; and new ones from the post-2012 reform, like .lawyer and .haus.

79 National Telecommunications and Information Administration, press release, *NTIA Announces Intent to Transition Key Internet Domain Name Functions*, March 14, 2014, https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.
80 Kathryn Brown, "We're Almost There… IANA Stewardship Transition," *Internet Society*, October 20, 2015, https://www.internetsociety.org/blog/public-policy/2015/10/were-almost-there-iana-stewardship-transition.

Internet Policy in Putin's Russia

In the wake of the 2011 Arab Spring, 2011-12 Russian winter protests, and June 2013 Snowden revelations, the Russian government has increased government control over the Internet and its users. The 2012 Russian Internet Restriction Bill instituted a blacklist for illegal content—child pornography, extremist and drug-related material, information on suicide, and information prohibited by the courts—administered by *Roskomnadzor*, the state telecommunications and IT regulator.[1] In 2014, the Russian Association of Internet Users identified a sharp uptick in government-led initiatives limiting Internet freedom, through this and other regulation.[2] In April 2015, *Roskomnadzor* instituted a law severely restricting online memes and parody accounts on the sites *VKontakte* and Twitter.[3] In September 2015, a sweeping requirement under the On Personal Data (OPD) law went into effect. The law requires that all Russian citizens' personal data—from health and government records to online purchases and email exchanges—must be stored inside Russian territory.[4] Analysts have noted that *Rostec* and *Rostelecom*, the state-controlled giants currently building domestic data farms, benefit most from forced localization.[5]

Russia has also stepped up its advocacy of "digital sovereignty" in its dealings with international actors. Russia is a chief proponent of having intergovernmental, treaty-based arrangements like International Telecommunications Union (ITU) play the central role in Internet governance. The state has run exercises to sever the Russian Internet from the global Internet in the event of perceived outside aggression, by creating national operating systems and a national text-messaging service, and repatriating control over the most frequented top-level Russian domains, like .ru and .rf.

1 J.Y., "Lurk No More," *The Economist,* November 16, 2012, http://www.economist.com/blogs/easternapproaches/2012/11/internet-censorship-russia.
2 Gregory Asmolov, *Welcoming the Dragon: The Role of Public Opinion in Russian Internet Regulation* (Philadelphia: Center for Global Communication Studies, 2015), http://www.global.asc.upenn.edu/publications/welcoming-the-dragon-the-role-of-public-opinion-in-russian-internet-regulation/.
3 "Russia's (Non) War on Memes?," *BBC News,* April 16, 2015, http://www.bbc.com/news/blogs-trending-32302645.
4 Shaun Walker, "Russian Data Law Fuels Web Surveillance Fears," *Guardian*, September 1, 2015, http://www.theguardian.com/world/2015/sep/01/russia-internet-privacy-laws-control-web.
5 Jason Verge, "Firms Rethink Russian Data Center Strategy, as Data Sovereignty Law Nears Activation," *Data Center Knowledge,* July 21, 2015, http://www.datacenterknowledge.com/archives/2015/07/21/russian-data-localization-law-spurs-data-center-strategy-changes/.

concentrations are coupled with democratic safeguards that ensure that the ICANN is accountable to the global community after the transition is complete.

In another step toward a more democratic and socially cohesive digital space, the UN's new Sustainable Development Goals (SDGs), for the first time, elevate the role of Internet access and connectivity in global development. The World Bank estimates that every 10 percent increase in Internet penetration correlates with a 1 to 2 percent increase in GDP.[81] Yet, the development community has been conspicuously slow to make Internet infrastructure, connectivity, and access headline development priorities.

This, however, is changing quickly. The UN's updated SDGs mention the ICT's potentially catalytic power in four of its seventeen headline aspirations of the global community. Target 9.c, for instance, aims for Internet access for all citizens of the least-developed countries by 2020. Prominent NGOs and private-sector coalitions have thrown their weight behind this target.[82] Also, the United States, Estonia, and the World Bank launched a

81 Yongsoo Kim, Tim Kelly, and Siddhartha Raja, *Building Broadband: Strategies and Policies for the Developing World* (Washington, DC: World Bank, 2010), p. 4, http://www.infodev.org/articles/building-broadband-strategies-and-policies-developing-world.

82 ONE, *The Connectivity Declaration: Demanding Internet Access for all and Implementation of the Global Goals,* September 26, 2015, http://www.one.org/us/2015/09/26/the-connectivity-declaration-demanding-internet-access-for-all-and-implementation-of-the-global-goals/.

Global Connect initiative that aims to bring 1.5 billion people online by 2020.[83]

The United States, EU, World Bank, and a chorus of other representatives from advanced industrial economies are working to broaden digital access to a larger swath of global consumers, producers, and entrepreneurs. They must marry these efforts with the incorporation of a greater cross section of global stakeholders into a maturing—more permeable, accessible, and diffuse—Internet governance. IANA's transition to the global multi-stakeholder community will be an important diplomatic milestone in this effort.

Across the board, the Internet's architecture requires cooperation between like-minded transatlantic stakeholders, including governments. The United States and the EU should take leading roles.

Step 18: Reinforce the multi-stakeholder model of Internet governance, both globally and at home. For more than a decade, the United States and EU have been champions of an open, bottom-up collaborative approach to Internet governance. The notion of "digital sovereignty" poses a new type of ideological challenge to this model. It is advocated by authoritarian actors such as Russia and China and, increasingly, some leaders within the transatlantic space have also flirted with the idea. The United States and EU should work with global civil society and industry to renew an Internet-governance framework based on the multi-stakeholder process, and make sure that this independent ethos remains at the heart of their domestic rule-making practices. The OECD conference on the Digital Economy in Cancun in June 2016 will also provide a forum for multi-stakeholder discussions.

The United States and EU must also ensure that their national Internet strategies take into account international Internet governance. The EU and its member states have increasingly focused on national strategies. From national-level strategies to the EU's DSM strategy, public-sector ICT policy has moved from a "citizen-centered" to a "citizen-driven" approach, in which the relationship between government, business, and civil society is less prescriptive and more collaborative. While this bottom-up approach is more democratic, it also means governments must work harder to add an international dimension to strategic policy planning. The OECD has pointed out this challenge.[84] The EU and its member states should update national strategies to reflect international and Internet governance priorities, including measures to modernize arrangements such as mutual legal-assistance treaties (MLATs), so that governments can embrace the Internet's open, multi-stakeholder character, without fear of undermining their legitimate concerns about national security and law enforcement.

Step 19: Elevate Internet connectivity in the transatlantic development agenda. The United States and EU, in collaboration with the World Bank and other international financial institutions (IFIs), should ensure Internet infrastructure-development projects are implemented alongside the construction of other infrastructure projects, such as roads, dams, and hospitals. Development agency funding should promote both digital and non-digital infrastructure, and look for opportunities where projects can be mutually reinforcing—like "dig once" projects, in which fiber is laid at the same time as roads are being constructed. The United States and Europe should also: place the crosscutting role of digitization and connectivity at the heart of implementation of the Sustainable Development goals; support partner countries in drafting and implementing national strategies that emphasize domestic digital inclusiveness and global interoperability; identify the best ways to incorporate middle- and low-income countries into the industrial Internet of digital supply chains and the Internet of Things; and push for greater emphasis on ICANN's work to help developing countries build up measures of the Domain Name System Security Extensions (DNSSEC).

Step 20: Complete the IANA transition, tied to enhanced multi-stakeholder accountability in ICANN. The decision to tether ICANN's accountability to the IANA transition has been welcomed by a majority of transatlantic and global Internet watchers, but successful accountability and transparency reform also have a deep geopolitical dimension. Dissatisfaction with the current ICANN model can lead countries like Russia and China to break away from the current structure and form new standards, which would lead to a fragmentation of the Internet.

83 Catherine A. Novelli, "Development in the Digital Age," speech delivered at United Nations General Assembly, September 27, 2015, http://www.state.gov/e/rls/rmk/247375.htm.
84 *OECD Digital Economy Outlook 2015*, p. 34.

A Hamilton Moment for the Transatlantic Digital Market

Alexander Hamilton—the visionary who saw the future of the United States shaped by a shared national financial system—would probably be hailed as the founding "disruptor" today. When others saw the United States as a country of provincial farmers, he saw a country of manufacturers, innovators, and engineers empowered by a unified financial system. When they were loyal to their states, he implored his fellow countrymen to "learn to think continentally."

The digital world is today craving its Hamilton moment, one that will force policymakers to learn to think transatlantically or, better yet, globally. In the coming years, digitalization will: bring the promise of greater prosperity; create new threat vectors, as billions of networked devices create potential vulnerabilities for economic disruption and physical harm; and open up new conundrums for fundamental rights and democracy. How will policymakers and stakeholders respond?

If the United States and Europe—as leaders in the digital economy—can establish a truly transatlantic digital market, they will set the global rules. The twenty steps outlined here offer a roadmap to deepen the transatlantic digital market and recast an open, secure, and democratic global Internet. Taken together, these steps advance the five core objectives that will make an integrated market possible: enhancing digital trade; improving the building blocks of transatlantic digital regulation and standard setting; providing lessons for domestic conditions that foster innovation; restoring trust in transatlantic cooperation on data protection and privacy; and advancing shared US-EU values in global Internet governance.

The reality is simple: more than any other major economies, the United States and the European Union have a shared stake in building a global digital marketplace based on openness, dynamism, and innovation—a marketplace that guarantees wide access while protecting consumers' rights, security, the public interest, and democracy. Will they seize the opportunity? The clock is ticking.

Atlantic Council Board of Directors

CHAIRMAN
*Jon M. Huntsman, Jr.

CHAIRMAN EMERITUS, INTERNATIONAL ADVISORY BOARD
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard Edelman
*C. Boyden Gray
*George Lund
*Virginia A. Mulberger
*W. DeVier Pierson
*John Studzinski

TREASURER
*Brian C. McK. Henderson

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stéphane Abrial
Odeh Aburdene
Peter Ackerman
Timothy D. Adams
John Allen
Michael Andersson
Michael Ansari
Richard L. Armitage
David D. Aufhauser
Elizabeth F. Bagley
Peter Bass
*Rafic Bizri
Dennis Blair
*Thomas L. Blair
Myron Brilliant
Esther Brimmer
*R. Nicholas Burns
William J. Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
John E. Chapoton
Ahmed Charai
Sandra Charles
Melanie Chen
George Chopivsky
Wesley K. Clark
David W. Craig
*Ralph D. Crosby, Jr.
Nelson Cunningham
Ivo H. Daalder
*Paula J. Dobriansky
Christopher J. Dodd
Conrado Dornier
Thomas J. Egan, Jr.
*Stuart E. Eizenstat
Thomas R. Eldridge
Julie Finley
Lawrence P. Fisher, II
Alan H. Fleischmann
*Ronald M. Freeman
Laurie Fulton
Courtney Geduldig
*Robert S. Gelbard
Thomas Glocer
*Sherri W. Goodman
Mikael Hagström
Ian Hague
Amir Handjani
John D. Harris, II
Frank Haun
Michael V. Hayden
Annette Heuser
*Karl Hopkins
Robert Hormats
Miroslav Hornak
*Mary L. Howell
Wolfgang Ischinger
Reuben Jeffery, III
*James L. Jones, Jr.
George A. Joulwan
Lawrence S. Kanarek
Stephen R. Kappes
Maria Pica Karp
Sean Kevelighan
Zalmay M. Khalilzad
Robert M. Kimmitt
Henry A. Kissinger
Franklin D. Kramer
Philip Lader
*Richard L. Lawson
*Jan M. Lodal
Jane Holl Lute
William J. Lynn
Izzat Majeed
Wendy W. Makins
Mian M. Mansha
Gerardo Mato
William E. Mayer
Allan McArtor
Eric D.K. Melby
Franklin C. Miller
James N. Miller
*Judith A. Miller
*Alexander V. Mirtchev
Karl Moor
Michael Morell
Georgette Mosbacher
Steve C. Nicandros
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Hilda Ochoa-Brillembourg
Sean O'Keefe
Ahmet Oren
*Ana Palacio
Carlos Pascual
Thomas R. Pickering
Daniel B. Poneman
Daniel M. Price
Arnold L. Punaro
Robert Rangel
Thomas J. Ridge
Charles O. Rossotti
Stanley O. Roth
Robert Rowland
Harry Sachinis
John P. Schmitz
Brent Scowcroft
Rajiv Shah
Alan J. Spence
James Stavridis
Richard J.A. Steele
*Paula Stern
Robert J. Stevens
John S. Tanner
*Ellen O. Tauscher
Karen Tramontano
Clyde C. Tuggle
Paul Twomey
Melanne Verveer
Enzo Viscusi
Charles F. Wald
Jay Walker
Michael F. Walsh
Mark R. Warner
Maciej Witucki
Neal S. Wolin
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
David C. Acheson
Madeleine K. Albright
James A. Baker, III
Harold Brown
Frank C. Carlucci, III
Robert M. Gates
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
George P. Shultz
John W. Warner
William H. Webster

**Executive Committee Members*

List as of March 28, 2016