B | Center for Technology Innovation at BROOKINGS

OCTOBER 2016

Bridging the internet-cyber gap: Digital policy lessons for the next administration

Cameron F. Kerry*

Cameron F. Kerry is the Ann R. and Andrew H. Tisch Distinguished Visiting Fellow for the Governance Studies' Center for Technology Innovation

INTRODUCTION: FLYING BLIND

When the first leaks from former National Security Agency (NSA) contractor Edward Snowden broke in The Washington Post, I was in my first days as the Acting Secretary at the Department of Commerce. Watching the damage unfold was like watching a car wreck in slow motion. And being in a position of some power but powerless to head off the wreck was an exercise in frustration.

The first story was on the bulk collection of telephone metadata in the U.S.[1] The second broke the next day.[2] This story disclosed the PRISM program, the collection of data from international email traffic transiting the U.S. The story reported (incorrectly in this respect) that the NSA was "tapping directly into the central servers of nine leading U.S. internet companies …," illustrated with a slide showing the logos of each of these companies.

Later that same day President Barack Obama responded to a question at a press availability.[3] In language the White House came to regret, his response was aimed entirely at reassuring a domestic audience that "nobody is listening to your phone calls," and saying that PRISM surveillance of the internet and emails, "does not apply to U.S. citizens and it does not apply to people living in the United States." President Obama also repeated that "it's important to recognize" there are "trade-offs," "some choices," and a "balance" that require "some modest encroachments on privacy."

The effect was to wave a glaring red flag outside the U.S. As Wired later described it in an article feverishly headlined "How the NSA almost killed the Internet:" [4]

* In my other capacity as a lawyer in private practice since 2014, I have advised clients in connection with some issues mentioned in the paper. The paper also refers to entities that are funders of The Brookings Institution, but was not influenced by any such entity.

> *"THE MAJORITY OF APPLE, FACEBOOK, MICROSOFT, AND YAHOO CUSTOMERS ARE NOT CITIZENS OF THE U.S. NOW THOSE CUSTOMERS, AS WELL AS FOREIGN REGULATORY AGENCIES LIKE THOSE IN THE EUROPEAN UNION, WERE BEING LED TO BELIEVE THAT USING U.S.-BASED SERVICES MEANT GIVING THEIR DATA DIRECTLY TO THE NSA."*

As these customers and regulatory agencies reacted, the Commerce Department began to hear a litany of anguished complaints from the companies affected (more than the name brands mentioned by *Wired*).

The initial response to the Snowden stories was freighted with the perception of the leaks entirely as a national security issue that required containment first and foremost. This blinkered vision led to the president's initial remarks, which were tone deaf to privacy concerns, the impact on the affected companies, the impact on international issues—from trade to Europe's privacy debate to internet governance—and the need in that context to affirm American privacy values. Ironically, its defensiveness had the perverse effect of inadequately articulating what American law and political culture do to protect privacy, and particularly the safeguards on the intelligence in the programs at issue.

In the weeks that followed, I ruffled some feathers in the West Wing pushing for a stronger message on privacy while dialing back the emphasis on security, and for discussion of the collateral damage from the leaks and the first response. It wasn't just the Commerce Department that was outside the conversation; the White House offices most attuned to similar concerns, the National Economic Council or the Office of Science & Technology Policy, were not part of the initial response either.

The initial response to the Snowden stories was freighted with the perception of the leaks entirely as a national security issue that required containment first and foremost. This blinkered vision led to the president's initial remarks, which were tone deaf to privacy concerns.

At the time, I was putting final touches on draft legislation codifying the Obama administration's Consumer Privacy Bill of Rights, pushing to finish a project I had led since early in the administration. My instant reaction to the first story was that finishing before I left the government had become impossible because a proposal aimed at privacy rules for business would seem like an effort to change the subject in the face of the predictable outcry about data collection by government.

I had also been leading international engagement on privacy issues and the flow of data across borders. In particular, I had been working to make Europeans aware that the U.S. has laws on privacy that are enforced aggressively by regulators and private litigants, and also has stronger and more comprehensive safeguards against government access to information than most other nations. It was clear that the PRISM would undo this effort by feeding hostility to American technology companies, and turbocharge growing movements to restrict flows of information, break up global networks, and bring the internet under control of intergovernmental organizations.

Well before the Snowden leaks, during the first Obama term, I convened what was dubbed the "Internet-Cyber Group." The name came from the observation at the group's first meeting by then White House Deputy Chief Technology Officer Danny Weitzner that "this world is divided into those people who call it 'the internet' and those who call it 'cyber.'" The former tend to be more focused on the economic and human potential enabled by information and communications technology

(ICT); the latter come more from the security world and focus on the darker sides of ICT—threats, exploits, bad actors, and applications for warfare. Perceptions of the damage from the Snowden leaks reflected these differing outlooks.

The Internet-Cyber Group was an informal deputies committee spanning policymakers at every agency that touches on the internet and cyberspace (including White House policy councils; the Departments of State, Justice, Defense, Commerce, and Homeland Security; the U.S. Trade Representative, and the Intelligence Community). Rather than meeting in the usual decisional context of the Situation Room, it met over occasional Dutch-treat dinners at various agencies to explore issues at a more strategic or conceptual level.

I saw a need for such discussions because I found myself at deputies committee meetings on a variety of security issues—from cybersecurity to telecommunications supply chain security to cyber operations to "going dark"—having variations of the same discussion with different counterparts. All involved the need to consider effects on innovation, trade and competitiveness, and trust in the internet and its governance. I also thought Commerce and other agencies focused on the latter issues should expand their understanding of threats and other security issues, so that both the internet and the cyber sides would operate from greater common understanding.

Because of the intersection of these issues, I found myself diving far more deeply into surveillance issues than I ever could have anticipated heading to the Department of Commerce. Some people clearly wondered initially why on earth the Commerce Department was involved. Similarly, some people at Commerce were uncomfortable stepping outside of what they perceived as its usual lanes.

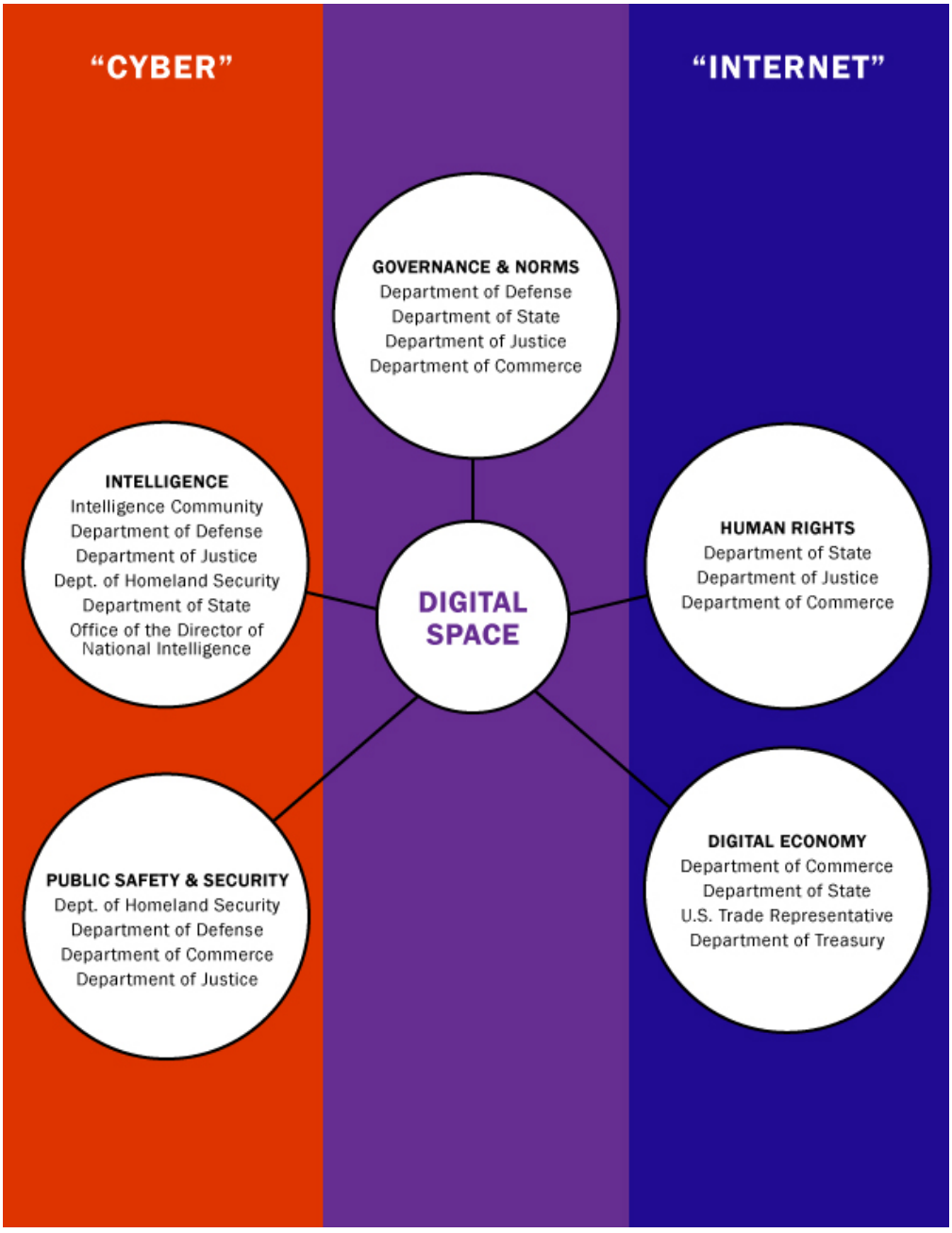
> The "Internet-Cyber Group" name came from the observation at the group's first meeting by then White House Deputy Chief Technology Officer Danny Weitzner that "this world is divided into those people who call it 'the internet' and those who call it 'cyber.'"

An added impetus for the Internet-Cyber Group was the release of the administration's *International Strategy for Cyberspace* in May 2011[5] and the concurrent development of the OECD *Principles for Internet Policy Making.*[6] The *International Strategy* declares the aim of "an open, interoperable, secure and reliable information and communications infrastructure" coupled with "norms of responsible behavior" aimed at the behavior of states and articulates a set of principles to support these aims spanning the economy, security, and human rights. The OECD principles include calls for protecting the global free flow of information and promoting the "open, distributed and interconnected nature of the internet." Carrying out *International Strategy* and advocating the OECD principles clearly warranted discussion that cut across agencies that touch on these areas.

The Internet-Cyber Group helped to broaden awareness of the connections among the issues in this space and break down silos. In particular, it helped develop a shared understanding between Commerce and Homeland Security about a light government touch in cybersecurity focused primarily on public and private sector collaboration. This approach underlaid the 2013 Executive Order 13636 that resulted in the successful NIST Cybersecurity Framework a year later.[7,8] The group also served as a vehicle to discuss diplomatic strategy around internet governance and the implementation of the *International Strategy.*

Figure 1 below illustrates the division between “cyber” and “internet” issues and the principal executive agencies involved. It shows that several agencies have roles on both sides of this division and that the issues surrounding governance fall into both spheres. (It does not reflect White House offices since the White House crosses all the functions).

Figure 1: Schematic of the internet-cyber gap



It was evident from the initial response to the Snowden stories, though, that the shared understanding developed through the Internet-Cyber Group and the integrated outlook of the *International Strategy for Cyberspace* was not

broadly enough shared and internalized. For me, seeing the damage unfold just as I expected seemed like we were starting again from the beginning.

The damage tarnished America's brand and the brands of American companies. The fallout has been felt in increased pressure for national data localization laws requiring that data about individuals within a country be kept in that country, for restrictions on transfers of data from the European Union, and for shifting internet governance away from the loose collection of organizations involved today toward intergovernmental bodies such as the United Nations. These pressures have a variety of motives, but they share a distrust of the internet as an American creation that benefits American companies. This outlook results in barriers to aspects of the internet perceived as reflecting American values such as freedom of speech, disruptive innovation, and the free flow of information.

LEARNING FROM HINDSIGHT

The setting today is different from the summer of 2013 as the Snowden stories unfolded. The Obama administration has learned a lot from the experience, taking a number of steps to restore trust and bolster its policymaking in the digital arena.

It took a concert of voices inside and outside the administration but, by the end of the summer and into the fall, the White House came to appreciate the damage and opened the process to a full spectrum of viewpoints. In August 2013, President Obama announced the appointment of a special review group of trusted former advisers and colleagues from the University of Chicago law school with a broad commission to review signals intelligence gathering.[9] A broad interagency "disclosures" group met over several months to discuss options for changes to intelligence programs and increasing transparency and trust.

During this period, the president, his senior staff, and members of his cabinet spent what the president described as "countless hours" reviewing intelligence collection in the disclosures group on up through a Principals Committee of cabinet members and to the president.[10] In the process, all got an education on privacy, data flows, and internet governance.

The end product of those countless hours produced changes in approach that have helped mitigate the international damage to trust and competitiveness and build support for an open internet. The president's announcement of a package of surveillance reforms in January 2014 included a noteworthy new international norm for foreign intelligence: Presidential Policy Directive 28 (PPD-28) declaring that foreign citizens outside the U.S. should receive protections for privacy and dignity comparable to those of American citizens.[11,12]

For an administration that got to Washington with a tech-savvy campaign enabled by the internet, the Snowden stories were one highly-visible source of discomfiture in 2013. The troubled rollout of the healthcare.gov website was another. These events catalyzed changes in the White House approach to technology and internet issues.

On the technology policy front, the last two years have seen the president intervene publicly with the Federal Communications Commission on net neutrality, making good on a significant campaign tech policy position; the development of a "digital service" to raise the level of tech skills in government agencies; a renewed emphasis on government data as a public good and using data to drive policy. The White House brought a cadre of tech veterans into the Office of Science & Technology Policy, including the first U.S. Chief Data Officer, and

empowered them and others in the same arena. In early 2015, President Obama himself went to the Federal Trade Commission to promote domestic privacy legislation and a cybersecurity "summit" at Stanford. Last March, he showed up at the South by Southwest tech-and-creative-arts festival in Austin.

The technologists in the White House were reinforced by other strong voices close to President Obama. One of the attributes John Podesta brought to his broad role as Counselor to the President was a long and deep background in technology issues, leading him to be tapped to lead a White House policy review on big data that followed the surveillance review.[13] His co-leader in that effort, Secretary of Commerce Penny Pritzker, has strong ties to President Obama and others in the White House; she receives a daily intelligence briefing similar to the president's and has been a trusted voice in issues like built-in access to encrypted communications. So has National Economic Council Director Jeffrey Zients.

All these changes reflect a heightened awareness of technology policy and the digital economy. Today, it is expected that Commerce and other economic agencies will be heard in the discussion of a broad range of issues. As one White House staffer involved describes it, the days are past when a principal at a cabinet meeting could profess not to understand technology; now that would be like admitting not understanding economics. For most of my time in the Obama administration, as the number two or three officer at Commerce, I was the senior official in the government directly involved with international and commercial privacy issues. Now, that senior official is the president, engaging with other heads of state.

The consequences and visibility of issues like data privacy and security, surveillance, and internet policy have grown—and with them the president's own engagement. They have become part of the mainstream of government.

WHAT ARE THE LESSONS?

The question now is, what will the Obama administration leave behind? How much will the collective understanding developed over the course of the current administration survive the senior officials who leave? Or will entropy set in?

This paper looks at what can be done to ensure that the next president and administration act in the digital arena with vision of the entire field. It does so through the lens of my own experience and observations of failures and successes from both inside and outside the administration, filtered by discussions with other participants and stakeholders. With these in mind, the paper seeks to avoid repeating some of the failures of the last seven-plus years and build on successes.

This paper looks at what can be done to ensure that the next president and administration act in the digital arena with vision of the entire field.

From these foundations, the paper draws a series of lessons. The first is the simple but essential premise that a persistent divide between national security issues and economic ones does not reflect today's networked and information-driven world. From this premise, I outline several steps to keep considerations outside "hard" security in sight and avoid replicating the blinkered decision-making seen in the initial Snowden response. These apply the maxim "operations is policy:" how the government goes about making policy and who makes the policy go a long

way toward determining the policy outcome. I then review digital policy challenges ahead for the next administration where these steps can make a difference.

LESSON 1: NATIONAL SECURITY POLICYMAKING NEEDS TO REFLECT THE IMPORTANCE OF ECONOMIC ISSUES IN GENERAL AND THE DIGITAL ECONOMY IN PARTICULAR.

In principle, the notion that national security depends on economic security is widely acknowledged and often stated. In practice, it often has been widely disregarded and poorly integrated into policy.

The principle is expressed firmly in the White House National Security Strategy issued in 2015: President Obama's foreword begins by describing "growing economic strength" that is "the foundation of our national security and a critical source of our influence abroad," and the document identifies "A strong, innovative, and growing U.S. economy in an open international economic system that promotes opportunity and prosperity" as a key national interest.[14] A major building block of this strategy, the Quadrennial Defense Review in 2014, identifies the strength of the American economy as a comparative advantage and the "foundation of U.S. power."[15]

> A persistent divide between national security issues and economic ones does not reflect today's networked and information-driven world.

Increasingly the digital economy is a vital element of this strength. Although digital trade and commerce is notoriously difficult to measure because much of it falls outside conventional goods and services, available measures point to a growing share of the U.S. economy and global economic production.

In an effort to take some measure of this share, the Economics & Statistics Agency of the Commerce Department looked at "digitally-deliverable services" and estimated they accounted for $357 million in exports and $222 billion in services in 2011.[16] The U.S. International Trade Commission valued "digital trade" (products and services delivered via the internet) at between $517 and $711 billion in 2012.[17]

Less conservative measures point to broader contributions. McKinsey Global Institute (MGI) found that ICT contributed five percent of U.S. GDP in 2014, but 10 percent taking into account the benefits to other sectors from applying the technology at declining prices.[18] Accenture models "the digital economy" (measured from "a number of broad 'digital' inputs") at a total value of $5.9 trillion amounting to 33 percent of U.S. GDP in 2016.[19]

While the measures vary, the direction and conclusions do not: the digital economy is "growing quickly" (OECD), existing economic measures do not capture it adequately and, in the United States and around the globe, it is more resilient and faster-growing than the economy as a whole.[20] MGI (2016) reports that even as global flows of trade and finance are flattening, data flows are "soaring," and that "[d]igitization, like electricity, is a general-purpose technology that underpins a huge share of economic activity beyond the sector that supplies it" because it touches so many people and activities.[21]

This trajectory is a function of the explosion of connectivity and velocity of information. Today, some 3.3 billion people in the world have mobile phones and, because of digitization, Cisco estimates that global internet traffic will

triple between 2015 and 2020, and Ericsson projects that some 28 billion devices will be connected to the internet by 2021.[22,23,24] This rapid expansion means the digital economy (by whatever measure) will be an even greater part of future growth. Accenture and MGI each project that effectively harnessing digital infrastructure, skills, and data flows could boost U.S. GDP from $2.2 to $2.8 trillion by 2020.

At the same time, the digital economy presents significant challenges to economic fairness and the future of work. It is a vector contributing to the winner-take-all economy and dislocations of innovation and globalization. MIT's Erik Brynolffson and Andrew McAfee, avowed techno-optimists, are clear-eyed in *The Second Machine Age* that technological progress is accelerating the growing gap in income and mobility and the bounties of competitive success.[25] Without policy intervention, this spread will grow and undermine growth, opportunity, and the social fabric. These challenges will bring the digital economy even more into the mainstream of government policy.

While the measures vary, the direction and conclusions do not: the digital economy is "growing quickly" (OECD), existing economic measures do not capture it adequately and, in the United States and around the globe, it is more resilient and faster-growing than the economy as a whole.

As a consequence, the health and wellness of the digital economy and the systems and technology that support it are vital U.S. interests. The digital arena is an American comparative advantage today, primarily because of our world-leading ICT sector and vibrant innovation that exploits digital technology. America's advantage faces competitive challenges, however. The OECD tracks the digital economy among member countries, and found in 2015 that nearly every member is adopting strategies aimed at improving their digital competitiveness by expanding infrastructure, developing e-government, and directly promoting digital industries. Other countries are intervening more explicitly, with laws requiring local manufacturing in India and data localization in China, Malaysia, and Russia.[26] This growing digital arms race heightens the competitive significance of the U.S. government's role.

Successfully adapting policymaking for the digital age begins with recognizing the increasing significance of technology policy to economic issues along with the inescapable importance of the economy as an element of national security. Economic strength and national security need to be interdependent in policy and not simply on paper. This means that the current expanded and elevated attention to digital economy issues should continue in ways that embed it into the architecture of policymaking in future administrations.

LESSON 2: THE PRESIDENT AND OTHER TOP LEADERS NEED TO CHAMPION AN INTERCONNECTED WORLD.

The time and voice of the president are scarce resources, but there is no substitute for engagement and advocacy by the president and other high-level administration officials. Only the president and vice-president, and to a lesser degree certain cabinet-level officials, can command wholesale audiences internationally, and speak with unquestioned authority for the nation's vital interests. It took President Obama's personal involvement and other high-level help to change the trajectory of damage from the Snowden disclosures. While I was leading engagement with Europeans and others on privacy issues, I worked hard with others in the administration to rebut European perceptions that

America is the Wild West when it comes to privacy and data, with no laws in the area and no concern. I also warned that undoing the Safe Harbor framework that enabled transatlantic data transfers would be very damaging to the U.S.-EU relationship. These messages made some headway on a retail basis, but they were quickly erased once the Snowden stories appeared.

President Obama's January 17, 2014 speech on surveillance and ensuing policy changes resonated more than 100 speeches by the entire sub-cabinet could. He also engaged personally with Presidents Xi Jinping, Dilma Rousseff, and François Hollande and Chancellor Angela Merkel.

In turn, President Obama's involvement was reinforced by Vice-President Biden speaking with EU President Jean-Claude Juncker about the need for a continuing data transfer mechanism. Commerce Secretary Pritzker's took an active role in negotiations for the new Privacy Shield framework and has made the digital economy a signature issue. Secretary of State John Kerry spoke in Korea about why "the United considers an open and secure internet to be a key component of our foreign policy," and personally affirmed a key promise supporting the Privacy Shield.

Now that digital issues are in the mainstream, they will demand continued presidential attention.

Likewise, presidential engagement has had an impact on cyber-espionage. It was a major topic of the "shirtsleeve summit" between Presidents Obama and Xi Jinping at Sunnylands in California in 2013, the most prominent of several Xi-Obama discussions in which the issue was raised (including most recently in bilateral meetings alongside the Hangzhou G-20 meeting).[27] President Obama also sparked bringing the issue to the G-20 to expand the circle of nations engaged.[28] His message was reiterated consistently by an array of U.S. voices at various levels (reciprocating Chinese delivery of consistent talking points up and down the line) and ultimately was reinforced by the federal indictment of five People's Liberation Army members for computer crimes, making good on the warning that there would be consequences if behavior did not change.[29]

In both instances, presidential engagement not only communicated to international counterparts and stakeholders, but also established the agenda and tone within the administration. Now that digital issues are in the mainstream, they will demand continued presidential attention. The next president will need to be conversant in these issues and have a full perspective. Executive Order 13630 makes commercial advocacy to promote exports the job of the whole government, including the president, and the competitive significance of the digital economy means it may call for commercial advocacy from the president.

The bully pulpit of the presidency can promote the benefits of a digital economy through public diplomacy to populations in the rest of world. This is not an always easy sell these days. A sizeable portion of the world views the internet as a Trojan horse for U.S. cultural, political, and economic hegemony and for surveillance by the NSA and American companies. Authoritarian governments view it as a threat to their control. Even in democratic countries, the connectivity of the digital economy presents challenges parallel to those of international trade: many of the same people in Europe who oppose the Transatlantic Trade and Investment Partnership (TTIP) also want to block data transfers to the U.S.

The *International Strategy for Cyberspace* has provided a foundation for this discussion. President Obama's foreword declares that the document is aimed explicitly at "engagement with international partners on the full range of cyber issues," It weaves together technical principles (interoperability, stability, reliable access, and security) with values (freedom, respect for property, privacy, and protection from crime) and governance (multi-stakeholder institutions, and self-defense). The *International Strategy* has provided U.S. agencies with a coherent synthesis of U.S. concerns in the digital arena, and having the president's signature on a document that articulates U.S. principles and values also elevates them.

What is needed is to amplify and persuade. Other governments and their populations need to hear why the values and principles are in their interests and they need to be reassured that the information and communications infrastructure is trustworthy. (Additional action to strengthen U.S. privacy laws to fit the digital economy and expanding data use will reinforce this message).

> The bully pulpit of the presidency can promote the benefits of a digital economy through public diplomacy to populations in the rest of world.

The *International Strategy* makes a general case for the value of the interconnectedness provided by digital communications, not only in the flow of goods and services but in the social and political capital contributed. But the terms "open" and "interoperable" can be technobabble whose meaning or significance is not clear to general audiences regardless of nationality. Audiences around the world need to understand what these mean for their lives and aspirations.

If President Obama (with a boost from John Oliver on HBO's *Last Week Tonight*)[30] can generate excitement about applying Title II of the Communications Act to broadband providers, his successor can surely articulate the benefits of network effects in terms of peoples' interests. The United Nations Sustainable Development Goals adopted a year ago targets as a means to promote infrastructure, industrialization, and innovation to "significantly increase access to information and communications technology and strive to provide universal access the internet in least developed countries by 2020."[31] Despite wariness of technology and the internet, many countries recognize benefits such as access to markets and mobile money through mobile connections and are hungry for connectivity; the State Department's Global Connect program, a public-private partnership to increase connectivity in less developed countries, feeds this hunger.

The values that need emphasizing most are those that promote trust in these networks —security and privacy. These are essential currency in the global digital economy. On network security, President Obama and his administration have been vocal and visible. On privacy, less so. The *International Strategy* focuses on protection from other governments but, in the post-Snowden era, reassurance in relation to the United States and U.S. companies is needed. Even though the U.S. can do more to protect individual data privacy with respect to both, it has far stronger protection than is generally recognized in other countries. This message needs to be affirmed at higher, more visible levels than the agency general counsels, FTC commissioners, and ambassadors who have been the main messengers.

LESSON 3: THE ORGANIZATION OF THE EXECUTIVE BRANCH AROUND DIGITAL ISSUES SHOULD REFLECT THEIR SCOPE AND SIGNIFICANCE.

To maximize the effectiveness of the U.S. government in the digital arena and support and leverage the president, both the Executive Office of the President and executive branch agencies need to reflect the importance of the digital economy and internet policy to U.S. interests. The premise that economic issues are integrated with national security should be reflected better in the decision-making process, and involvement at the top needs to be mirrored in, as well as supported by, the work of executive branch agencies. The White House needs to leverage the capabilities of agencies, and is most effective when it does so rather than acting in isolation or top down.

A. WHITE HOUSE DECISION-MAKING SHOULD REFLECT THE BREADTH OF THE ISSUES INVOLVED.

The National Security Council (NSC) has a rich and well-studied history going back to its establishment by the National Security Act of 1947 to meet the challenges of the Cold War. Through successive presidential directives organizing the NSC in each administration and, well-supported by detailees from agencies, it has evolved a well-established set of procedures and structure: a base of interagency policy committees that feed into a deputies committee where many of the policy issues are resolved, leaving select issues to a cabinet-level principals committee or to the president. This system generally works effectively to ensure that executive decision-making reflects input and coordination from appropriate parts of the government.

Reflecting changing priorities after the Cold War, President Clinton moved to establish similar decision-making structures for economic and domestic policy and technology; in 1993, he issued executive orders establishing the National Economic Council (NEC) and Domestic Policy Council (DPC) and creating a parallel structure within the existing Office of Science & Technology Policy (OSTP), the National Science and Technology Council (NSTC). The Obama administration created the position of Deputy National Security Advisor for International Economics in the NSC, with a dual-hatted relationship to the NEC, to elevate international trade and economic issues and provide economic agencies a window into national security issues. In the second term, Chief of Staff Denis McDonough has encouraged NEC, DPC, and OSTP to replicate the policy development procedures and structures of the NSC.

Despite these efforts to build up policy councils other than the NSC and rebalance decision-making, “hard” security is still dominant over “soft” security or the economy, and the latter lack the same strategic energy and focus. Assistants to the president who lead these other councils have in fact established some processes to parallel those of the NSC, but they lack the resources, accreted experience, and interagency acceptance of their better-established counterpart. Some of this disparity is inevitable: their agency partners do not have budgets as large as those that support the NSC with detailees and policy development, the policy councils do not have the international background and reach of the NSC apparatus, and the conclusion of the Cold War did not end conflict and security threats.

The NSC therefore remains critical to getting digital issues right. Its structure and processes should build on the steps by the Obama administration to ensure a broader point of view. Otherwise, blind spots are likely to recur. As the president’s special review group found, even core national security activities in intelligence collection present risks to foreign relations, trade and commerce, as well as privacy and civil liberties. Such activities warrant greater consideration of these goals, and the process of setting intelligence priorities should include “all departments and

agencies with relevant concerns." PPD-28 adopts this advice by providing that signals intelligence collection must weigh:

> *"OUR RELATIONSHIPS WITH OTHER NATIONS…; OUR COMMERCIAL, ECONOMIC, AND FINANCIAL INTERESTS, INCLUDING A POTENTIAL LOSS OF INTERNATIONAL TRUST IN U.S. FIRMS AND DECREASED WILLINGNESS OF OTHER NATIONS TO PARTICIPATE IN DATA SHARING, PRIVACY, AND REGULATORY REGIMES; THE CREDIBILITY OF OUR COMMITMENT TO AN OPEN, INTEROPERABLE, AND SECURE GLOBAL INTERNET; AND THE PROTECTION OF INTELLIGENCE SOURCES AND METHODS."*

To ensure visibility into such other considerations requires broadening the current interagency process under the NSC.

While the National Security Act names the president and vice-president, the secretary of state, and secretary of defense as statutory members of the NSC[32] and certain other military, security, and law enforcement officials for specific purposes, it also authorizes the president to appoint other cabinet officers. Every administration begins by spelling out how the NSC will operate.

The Obama administration's Presidential Policy Directive 1 (PPD-1) broadens the statutory group by providing that organizations such as the National Economic Council, Treasury, Commerce, and Trade Representative shall participate "when international economic issues are on the agenda."[33] This formulation is too limiting, because economic issues and other issues acknowledged in PPD-28 often are implicated even when they are not explicitly on the agenda, and NSC issues also may have an impact on domestic economic issues. If economic issues are implicated at all, economic agencies should be present—and the presumption should be that these issues are implicated. The effect of such a change would be to switch the default position for NSC participation from economic-agencies-out to economic-agencies-in.

> Both the Executive Office of the President and executive branch agencies need to reflect the importance of the digital economy and internet policy to U.S. interests.

To a great extent, this is where the Obama administration has arrived after the Snowden experience. But that outcome is partly a function of the impact of individuals: as reflected in PPD-28, President Obama has acted to broaden the process, and economic officials like Secretary Pritzker and Treasury Secretary Jack Lew have unusually strong relationships with the president and senior staff at the White House. The current inclusiveness needs to be recognized officially in the next administration's organizing documents so it can be institutionalized and outlast the individuals involved.

The broadening of perspective should extend within the NSC by keeping the position of Deputy National Security Adviser for International Economics, staffed with Senior Directors for each of the major elements of the portfolio, including the digital economy. Institutionalizing this role would reflect the importance of economic issues to national security, and of international economics to the domestic economy and national security. It also brings to these concerns international capability and familiarity with the context of competing bilateral, multilateral, and strategic issues that the NEC, DPC, and OSTP do not have built in. Having a senior member of the National Security Council with an economic and business portfolio that also would provide some insurance the economic and other soft power implications of national security issues have a place at the table and provide a window for other councils and agencies.

Without someone within the NSC itself with this perspective, the decision when "international economic issues are on the agenda" (or implicated, as the case may be) rests in the hands of people who may have blind spots to the soft implications of hard security issues.

The broadening of agency participation should be mirrored in the interagency policy committee structure. Something like the Internet-Cyber Group should institutionalized as a policy committee led by the NSC, Commerce, and State. This would help replicate the education process the current administration went through and institutionalize the cross-cutting communication and broad focus needed to carry out the *International Strategy for Cyberspace*. Updating the *International Strategy* could serve as a vehicle for such an education process and a framework to address specific issues through sub-groups. President Obama's early memorandum directing executive agencies to collaborate[34] established an expectation that encouraged cooperation and the Internet-Cyber Group showed that collaboration can subsist informally. But such collaboration can accomplish more with the official sanction of executive orders and interagency processes to break down digital issue silos further and discipline bad behavior.

"The capacity of other White House policy councils can be enhanced to ensure they are able to present a full range of considerations within the NSC and in all relevant White House decisions."

The capacity of other White House policy councils can be enhanced to ensure they are able to present a full range of considerations within the NSC and in all relevant White House decisions. Executive Order 12835, which establishes the NEC and parallels the orders establishing the other councils, resembles PPD-1 in specifying who should participate, but it does not establish a structure or empower the principals, deputies, and interagency committee process as PPD-1 does for the NSC.[35] A new, more explicit executive order would buttress the legitimacy of the NEC, DPC, and OSTP in these regards.

New executive orders also could spell out specific functions and positions to support these functions. At the outset of the administration, the NEC added its first special assistant to the president with a technology and digital economy portfolio. The growth of this role since its beginnings in what its first occupant has described as "guerilla warfare" reflects how technology policy issues have become mainstream over the course of the Obama administration. This is a portfolio that should endure and move to the level of a deputy assistant to the president.

This NEC portfolio overlaps with some of the functions of OSTP. Consideration could be given to consolidating function to strengthen resources as well avoid duplication or conflict. By and large these overlaps have not been dysfunctional in the Obama administration because of effective coordination between OSTP and NEC. Some technology policy staffers have worn hats in both, and the two councils have collaborated on joint efforts. From the standpoint of outside stakeholders, having these multiple channels into White House discussions can be helpful.

Some of these joint NEC-OSTP efforts provide a template for leveraging the effectiveness of these councils through additional resources. In the last couple of years, OSTP established an interagency Tech Policy Task Force focused on bringing technologists into policy discussions to flesh out technology issues; NEC and also NSC participated. The current OSTP inquiry on issues raised by artificial intelligence is co-sponsored by the NEC. Similarly, the policy development I led on consumer privacy was through the vehicle of a chartered subcommittee of the National Science and Technology Council that I co-chaired from 2009-2012. Both OSTP and NEC participated in this subcommittee. The White House blessing through both the charter and staff participation conferred legitimacy on Commerce's

interagency leadership, leveraging the White House by deputizing our department. It operated as a hybrid of cabinet government and White-House-driven policymaking.

A similar interagency group with a broader policy charter should carry forward. It could combine with the updated version of the Internet-Cyber Group suggested above for the NSC, or operate in parallel so long as a Venn diagram of the two spheres has substantial overlap.

B. EVERY AGENCY NEEDS TO BE PART OF THE DIGITAL AGENDA.

Today, there is scarcely any agency that has not stepped up its activity in the digital arena. Although some have no involvement in digital policy as such, all are involved in some way in using digital technology to improve processes or putting data to use for the agency or the public.

The White House helped to jumpstart this activity with the Presidential Innovation Fellows program patterned on the White House Fellowships and similar fellowship programs and with the "U.S. Digital Service," both aimed at bringing the experience and outlook of startup businesses into the federal government.[36,37] Their work has focused on the outputs of government such as data and services: Veterans Administration services, data on policing for "data-driven justice," and consulting for multiple agencies through the General Services Administration.

This renewed push for innovation on e-government and data mining can benefit every agency, helping to find ways through the maze of procurement and personnel rules to bring technical knowhow and imagination. Raising the level of technical proficiency is likely to increase understanding of the implications of policy choices in the digital arena.

I see the Department of Commerce, my former agency, as the agency that has integrated digital issues into its work most fully (at least in its policy work if not in its internal technology). While I take some credit for this, it is a natural outgrowth not only of Commerce's broad mandate for domestic and foreign commerce, but its components' involvement in so many aspects of the digital economy and technology. Among other things:

- The National Telecommunications and Information Administration (NTIA) is by statute the president's advisor on telecommunications and information policy and in the forefront of global debate on internet governance.
- The National Institute of Standards & Technology (NIST) has played a key role in cybersecurity, working with the private sector to develop the NIST Cybersecurity Framework as well as federal agency information security standards.
- The International Trade Administration has administered the U.S.-EU Safe Harbor Framework, and negotiated its replacement in the wake of Safe Harbor's invalidation by the Court of Justice of the European Union.
- The Patent & Trademark Office (PTO) issues patents that enable commercialization of new technologies and, through the Secretary of Commerce, advises the president on intellectual property issues.
- The Economics & Statistics Administration issues many key economic statistics and reports and with other Commerce agencies (mainly the Census Bureau and the National Oceanic & Atmospheric Administration) accounts for 40 percent of all the data put out publicly by the U.S. government.

Commerce is unusual in that, because of its disparate mixture of functions and agencies, its components often can have differing interests on digital policy issues. On legislation to block internet piracy sites (the Stop Online Piracy and Protect Intellectual Acts, remembered as SOPA-PIPA), for example, NTIA and NIST were focused on the impact on the internet and network security while the priority of the PTO was on intellectual property protection. The Bureau

of Industry & Security at Commerce administers export controls, including controls on encryption technology that other components promote. Thus, Commerce is not simply about woolly internet stuff; it also was at the front end of dealing with concerns about Huawei and ways to respond to cyber-espionage.

Early in the first Obama term, we pulled all these bureaus together into an Internet Policy Task Force, led by the secretary's office and embraced by the White House as a vehicle for developing policy in this area.[38] This role was boosted by a strong ethic of collaboration and a principle that the Commerce Department would speak with one voice rather than present different positions from different components. In the SOPA-PIPA context, for example, the PTO, NIST, and NTIA synthesized positions in a way that foreshadowed the eventual outcome from the White House.

In the second term, Secretary Pritzker has embraced the digital agenda energetically, identifying the digital economy as a top strategic priority. Commerce stepped up economic studies on the subject and established a high-profile Digital Economy Board of Advisors. The department initiated the training of the Foreign Commercial Service to be "digital attachés" placed in key posts (ASEAN, Brazil, China, the EU, and Japan). Secretary Pritzker appointed the federal government's first Chief Data Officer to build on the Commerce's role as a data agency and took a personal hand in negotiations of a new Privacy Shield transatlantic data transfer framework and elevating concerns about barriers to the flow to data and technology.

To underscore this strategic priority and align the work of Commerce's various bureaus, Secretary Pritzker brought in Alan Davidson, respected as the former head of the New America Open Technology Institute and Google's Washington office, as senior adviser for the digital economy, reporting directly to the deputy secretary and heading an agency-wide Digital Economy Leadership Team. The next secretary should keep the position and fill it with an equally strong appointment.

The other agency with a cross-cutting role in digital affairs is the Department of State, which touches on every aspect of these issues, from national security to the digital economy and internet governance to human rights. As at Commerce, these various roles can result in differing interests within the agency.

- State deals with national security issues through its Under Secretaries of Political Affairs; Arms Control and International Security; and Civilian Security, Democracy, and Human Rights; and the Bureau of Intelligence and Research is part of the Intelligence Community.
- The Bureau of Democracy, Human Rights, and Labor deals with promoting internet freedom and human rights online, including grants to support technologies that help activists and journalists in authoritarian countries avoid government surveillance.
- The Bureau for Economics, Energy, and Environment, deals generally with digital economy issues, and its deputy assistant secretary and coordinator for international communications and information policy, who has ambassadorial rank, leads diplomacy on communications and information policy, including representing the United States on communications and internet issues in international bodies such as the International Telecommunications Union.
- The Under Secretary for economics, energy and environment is also delegated the authority under PPD-28 to coordinate "diplomatic and foreign policy efforts related to information technology issues" and act as a point of contact for foreign governments on intelligence collection issues, and designated under the Privacy Shield framework as the "ombudsperson" to receive complaints from individuals in the EU about U.S. surveillance.

To help harmonize these diverse and sometimes conflicting portfolios, State in 2011 established the position of coordinator for cyber issues, which reports directly to the secretary of state and is charged with advancing U.S. interests outlined in the *International Strategy for Cyberspace.* A major focus has been international engagement

on issues of cybersecurity, cyber operations, and intellectual property protection (including the task of leading a dialogue with China that, when it takes place, takes up the issue of hacking and commercial espionage). Dialogues with Germany, India, Japan, and Korea have broadened to incorporate issues such as Internet governance and data localization, with involvement from other State Department offices and other U.S. government departments (including Commerce). An essential aspect of this coordinator position is its direct line to the secretary and a portfolio spanning the department to provide visibility into State's disparate digital roles. This should continue in the next administration.

The concentration of force at State is within the Political Affairs Bureau, which oversees the overseas missions and regional and country desks that form the backbone of the State Department's operations. To build greater awareness of digital issues into this workforce, State has instituted a "Digital Economy Officer" program. This role is assigned to 139 economic officers at posts abroad, and they are being trained to include U.S. interests on digital issues as part of their job descriptions. State also has "cyber officers" in missions, who work together with the digital economy officers as part of country teams on digital issues.

Commerce and State are not alone in dealing with digital issues. As digital technology introduces new business models across sectors, other agencies face issues with important implications for the future economy.

State and Commerce between them have a large share of the day-to-day work of persuading other countries of the value of "open and interoperable" communications networks. The two agencies worked closely together in the NSTC subcommittee on commercial privacy I co-chaired, the charter of which encompassed coordinating international engagement on privacy. When the U.S. government had concerns with EU legislation on privacy, that subcommittee successfully cleared a paper over a short span of time; briefed U.S. mission officials on the issues, a precursor to digital attachés and digital economy officers; and set up a system for them to report back to U.S. Mission to the EU in Brussels—a virtual "war room." The coordinating authority of PPD-28 and the added troops on the ground in missions overseas can systematize and expand that kind of ad-hoc campaign. Similar close collaboration between State and Commerce will be important to the success of the digital economy officer, cyber officer, and digital attaché initiatives and the digital diplomacy they contemplate.

Commerce and State are not alone in dealing with digital issues, however. As digital technology introduces new business models across sectors, other agencies face issues with important implications for the future economy. The Treasury Department is examining the issues presented by virtual currencies such as Bitcoin, and their implications for management of currency and regulation such as currency transaction reporting and "know-your-customer." The Department of Transportation is dealing with drones and autonomous vehicles.

Major elements of *International Strategy for Cyberspace* fall on the "hard" security agencies—the Departments of Defense, Justice, and Homeland Security. Along with State's international lawyers, they deal with the safety, norms of responsible behavior, and network protection components of the *International Strategy*. These issues need not play out in isolation from the "soft" issues, however, and require a broad view of the web of issues in the digital space.

I saw an example of the role security agencies can play in these when Central Command brought me to discuss principles of internet openness and governance with Middle Eastern defense partners; my Defense counterpart

provided robust support of these principles and explained that, with strong encryption, much of DoD's systems ride on the public internet. The State-led cyber dialogues help to show that these principles are compatible with strong cybersecurity. Interventions like these with audiences outside natural constituencies for internet freedom and openness show that hard security agencies can be invaluable force multipliers for the softer aspects on the *International Strategy*. Likewise, economic agencies have a role in amplifying and reinforcing U.S. interests on cybersecurity and norms of behavior.

As agencies prepare their priorities in the next administration and their next set of strategic plans, they will need to consider the role of technology and their role in the *International Strategy for Cyberspace* and successor plans. To address these needs, many policy planning shops need someone conversant in these issues, and many agencies could emulate the White House and Federal Trade Commission in bringing aboard a chief-technologist on high-level staff. Similarly, many could adopt the Commerce precedent of appointing a chief data officer to enhance the use of data that they generate as public goods and management tools, and perhaps also the appointment at State as well as Commerce of a senior digital affairs advisor.

LESSON 4: OPEN THE ARCHITECTURE OF DECISION-MAKING AFFECTING THE DIGITAL ECONOMY AND ECOLOGY OF THE INTERNET.

In ways different from most issues, the issues that come up in the digital arena require broad input. Because they involve complex systems that change at a rapid pace, they require technological expertise. And in an environment where interconnection and interoperability are important features, cooperation and collaboration are indispensable.

Moreover, when it comes to setting standards for technology, both established executive branch policy under OMB Circular A-119[39] and statutory law[40] articulate a strong policy preference to address technical issues with voluntary consensus standards. In the internet space, the *International Strategy* calls for advancing openness and innovation "through outreach to appropriate multi-stakeholder institutions and organizations," and specifically endorses multi-stakeholder governance of the internet as appropriate to an architecture "which is decentralized, cooperative, and layered." Policymaking in this arena needs to live up to these descriptions, and a multi-stakeholder approach has shown to work as a model.

One reason the Commerce Department has been effective on digital issues is that its business, science, and technology portfolio demands engagement with business, civil society, academia, and technologists. In addition, because of NIST's role in working with the private sector and standards-developing organizations in developing such standards and NTIA's role in working with internet governance, such interaction is part of the culture at Commerce.

For many other agencies, this interactive approach does not come as easily. For example, as a general matter the Justice Department has clients and adversaries, not stakeholders. When I convened businesses to meet with the Justice Department and Securities and Exchange Commission to discuss issues of compliance with the Federal Corrupt Practices Act, one prosecutor told me it was eye-opening, especially since "we're in the business of prosecuting, not talking to people we might prosecute." The perspective helped inform new Justice Department and Securities and Exchange Commission guidelines clarifying enforcement of laws against bribery of foreign officials.[41]

Perhaps because of the networked nature of the subject matter, arms of the White House involved in technology issues (including a succession of cyber coordinators in the NSC) also have been more engaged outside the government.

Issues such as encryption and surveillance also have stepped up discussion between outside stakeholders and agencies such as the Justice Department, FBI, and NSA.

Interactivity comes even less naturally for many national security agencies whose activities require secrecy. Because of this secrecy and the time required to declassify materials like Foreign Intelligence Surveillance Court decisions and procedures for approval of data queries by NSA analysts, the response to the Snowden leaks was handicapped by delay. Interviewed as he was preparing to leave his job nine months later, former NSA Deputy Director Chris Inglis said "I think going forward what I would change is that we need to continue to move in the direction of having greater transparency about the nature of the NSA, what its authorities are, how those authorities are brought to bear."[42]

In an environment where interconnection and interoperability are important features, cooperation and collaboration are indispensable.

This reflects a tectonic cultural shift in the intelligence community. In the wake of the Snowden leaks, a great deal has been done by the intelligence community, presidential review board, and Privacy and Civil Liberties Oversight Board to make information public, and officials have been engaged with a variety of people and groups outside the normal community for these agencies. The result has been that the intelligence community has explained itself much better and also understands public concerns better.

Indeed, secrecy can make people suspect the worst. When a draft Department of Defense "Strategy for Cyberspace" contained many redactions for classified material in its public version, I "non-concurred" within the deputies committee out of concern that the extent of redactions could lead to unnecessary paranoia. With backing from the White House, the eventual outcome was a more transparent document that proved to be noncontroversial.

The controversy over SOPA-PIPA bills making their ways through Congress in 2011, provides a useful lesson in the acute sensibilities of the online world as well as the value of digital technology in opening government decision-making. This legislation to block pirate websites, backed by producers of content such as films and music affected by piracy and a coalition of business, labor, and law enforcement interests, easily passed the House. The tech industry and internet community vocally opposed it, fearing the legislation would erode the principle of protecting from liability "intermediaries" that route internet traffic but do not control content; they saw the blocking of content as something that could "break the internet."

Early on, reflecting its use of online tools in the 2008 campaign, the Obama administration committed to respond to online petitions with 100,000 signers.[43] Once such a "We the People" petition against SOPA-PIPA met this threshold, the administration had to respond. The petition coincided with an interagency process on the legislation within the Obama administration. This process raised significant concerns about the constitutionality of the legislation and its impact on network security, and led to discussions of less restrictive approaches. Even so, without the petition the perceived politics of the issue might have tipped toward supporting the legislation.

Because the petition changed the political calculus, the administration was able to publish a blog post opposing SOPA-PIPA not long before coordinated action in the internet community shut down Wikipedia, darkened Google's landing page, affected many other websites for a day in January 2012, and unleashed thousands of emails and calls to Congress.[44] This storm of protest killed the legislation altogether and provided policymakers on both ends

of Pennsylvania Avenue with a memorable demonstration of the power of the "netroots," the community of internet activists.

As this instance shows, one byproduct of increased adoption of digital technology in government can be to expand ways of getting and distilling public input. Although the Federal Advisory Committee Act, Paperwork Reduction Act, Federal Records Act, and democratic transparency impose some constraints on how such input is gathered, there are ample ways to expand outreach. It took some time early in the administration to figure out how government use of tools such as Twitter and online comments fit laws and regulations written for an analog and paper environment, but creative thinking found ways.

LESSON 5: PERSONNEL IS POLICY.

The right people in the right places make a great difference. That is evident in the record of the past seven years: key achievements are a reflection of the people involved more than of the process.

As recounted above, much of the change in response to the Snowden leaks came about because of President Obama's own instincts. He can be a technophile who gets genuinely excited about geeky things. His background as a constitutional law professor was reflected in what he described as "a healthy skepticism toward our surveillance programs after I became president," and early in the Snowden conflagration he expressed a desire for a "national conversation" on privacy and security.[45] He had an inclination to conduct this conversation himself through a series of town meetings and seminars, and the appointment of a review board made up of people he knew and trusted was a substitute for doing it himself.

The Commerce Department's broad involvement in the digital economy came about initially because a group of like-minded people at the sub-cabinet and staff levels saw linkages among a set of emerging issues and were supported by Secretary Gary Locke in making these issues a priority for the agency. Similarly, the development of the *International Strategy for Cyberspace* was led by staffers with the peripheral vision to see the implications beyond the cyber domain, including internet governance, trade, and liberty.

The Commerce role expanded later because of Secretary Pritzker's view of the digital economy and investment of her own considerable energy and political clout to give the agency more weight. The critical mass of experienced information technologists at OSTP over the past three years is another example where having the right people in the right places has an impact.

By process of evolution the next administration may have a higher proportion of appointees conversant with technology and digital economy issues. The increased impact and visibility of digital issues and generational change are likely to increase the pool of candidates who are digital natives or digitally fluent.

Even so, it will be important to be sure that, in the aggregate, cabinet-level appointees and senior staff are at least as conversant with these issues as the Obama administration has become through difficult experience. Literacy in this area encompasses (among other things) a basic understanding of the architecture and ecology of the internet, the mechanisms of cybersecurity threats, and the role of information and communications technology in the economy the future. It may not mean knowing how to code, but should incorporate an understanding of how code works. It also requires relationships with the community of experts and advocates on these issues at home and abroad.

> It will be important to be sure that, in the aggregate, cabinet-level appointees and senior staff are at least as conversant with these issues as the Obama administration has become through difficult experience.

The appendix below shows high-level positions in the 2012 "Plum Book" in which these attributes will be as important as a basic understanding of economics or the Constitution in key cabinet agencies. Some three dozen marked with an asterisk are positions engaged enough in aspects of digital affairs that such attributes are essential to the job. In addition, the appendix also shows numerous less-specialized positions where some facility in these is essential. It does not include less senior positions where knowledge will be needed to support positions listed, nor does it include the numerous chief information officer, chief information security officer, or chief technology officer positions needed to address the technical infrastructure of government. Likewise, it leaves out career positions and independent agencies such the Federal Communications Commission and Federal Trade Commission, and the CIA and the FBI that can have a significant impact in these areas.

Similar capabilities are needed not only in key political and policy positions, but across a wide array of political and career jobs. As the exit of baby boomers continues to spike federal retirements, there is an opportunity to remake the federal workforce, including its digital capabilities. Agencies need to adopt the model of the Presidential Innovation Fellows and the Digital Service of bringing in technical savvy to take on government projects as startups.

Filling these positions with digitally-literate women and men can come from a wide range of sectors. The recent wave of technologists in the White House drew heavily from the private sector, but numerous significant contributors have come from civil society (including several at Commerce and the White House from the Center for Democracy and Technology), and from think tanks and academia. Agencies also can apply the model of the Commerce and State digital attachés and digital economy officers with specific training for existing personnel to improve policy as well as use of technology.

PUTTING THE LESSONS TO WORK

The next presidential administration will need to pick up the unfinished business of the Obama administration and be in a position to deal with a series of global challenges on digital issues. To do so effectively will require focus and organization from the get-go that weaves together the strategic, economic, and political strands of policy in cyberspace, internet affairs, and information technology.

The U.S. has faced some strong headwinds as result of the Snowden leaks. The reaction to the stories went beyond anger at surveillance to heightened distrust of internet technology, the companies involved, and the model of internet governance developed and promoted by the U.S. In reaction to a perception that the U.S. government "runs" the internet, allies such as France and Germany were bruiting about ideas of a "European internet" that would keep data of EU citizens on EU territory.[46] Channeling her own anger at having been a target of NSA surveillance according to reports from the Snowden documents, former Brazilian President Dilma Rousseff announced a plan to convene Brazil's own global internet governance conference.[47] Colored by unrebutted allegations based on the Snowden stories, the Court of Justice of the European Union invalidated the Safe Harbor framework that had been the principal basis for transfers of data from the EU to the U.S.[48]

The turbulence has subsided appreciably. Europeans abide by their exceptionalism as to privacy, but the data localization fever appears to have broken and EU trade negotiators recognize their own offensive interests in preventing data localization by trading partners around the world.

With support from European allies, the United States has achieved diplomatic successes that showed increased appreciation among democratic allies of the value of internet openness, interconnection, and nongovernmental control. Brazil's Netmundial conference in early 2014 rejected proposals to bring internet governance under multilateral governmental control and instead produced an endorsement of multi-stakeholder governance. Of the 89 nations that in 2012 endorsed expanding the role of the intergovernmental International Telecommunications Union over the internet, 30 have endorsed a plan for multi-stakeholder supervision of functions of the Internet Corporation for Assigned Names and Numbers (ICANN).[49] The new government of Prime Minister Narendra Modi in India—a pivotal player in the internet governance debate—joined Brazil in switching from the multilateral to the multi-stakeholder side. The completion of the ICANN transition can help to solidify and broaden this support.

> The next presidential administration will need to pick up the unfinished business of the Obama administration and be in a position to deal with a series of global challenges on digital issues. To do so effectively will require focus and organization from the get-go.

A less charged atmosphere in Europe enabled U.S. negotiators to reach agreement on a new Privacy Shield framework for transatlantic data transfers to take the place of Safe Harbor.[50] This outcome required the collaboration of a number of agencies, and benefited from increases in transparency concerning intelligence collection, the passage of the USA FREEDOM Act limiting bulk surveillance, and passage of the Redress Act extending federal Privacy Act protection to citizens of foreign countries that provide reciprocal remedies.[51] These developments enabled President Obama, in signing the Redress Act and marking the Privacy Shield, to deliver the message that "we take our privacy seriously," adding pointedly, "We enforce our privacy laws, unlike a number of other countries."[52]

There remain tensions and uncertainties around the Privacy Shield and other transatlantic data transfer mechanisms. These almost certainly will face legal challenges, and the Privacy Shield must undergo annual reviews by the European Commission and skeptical member state privacy and data protection regulators. The continuity of transatlantic data transfers will need additional high-level attention, not only for diplomacy with the European Union and member states, but also for advocacy to affect European public opinion. Meanwhile a different data transfer model under the Cross-Border Privacy Rules of the Asia-Pacific Economic Conference needs wider adoption by member countries on the other side of the Pacific.

In some other parts of the world, struggles over the flow of information and technology and the rules that govern them are intensifying. In particular, China has escalated its control of the internet. Although Lu Wei, until recently head of China's Cyberspace Administration, uses the term "multi-stakeholder," only one stakeholder counts, and Beijing has ratcheted up its blocking of content offensive to the government and its generation of web content that reflects the government doctrine. As the technologies of blocking and surveillance become more accessible, other authoritarian and non-Western governments are following the Chinese model of "digital sovereignty," including in

Russia, Malaysia, and the Middle East.[53] These trends threaten to turn the global internet into a set of national or regional internets.

With support from European allies, the United States has achieved diplomatic successes that showed increased appreciation among democratic allies of the value of internet openness, interconnection, and nongovernmental control.

The *International Strategy for Cyberspace* articulates a countervailing model. It calls for collaboration rather than prescription—with the private sector, with civil society, with multi-stakeholder organizations involved in internet governance. In particular, the *International Strategy* calls for the United States, in order to advance its approach, "to engage the international community in frank and urgent dialogue, to build consensus around principles of responsible behavior in cyberspace and the actions necessary … to build a system of cyberspace stability." There is a need for added frankness and urgency.

The passage of the Redress Act and the USA FREEDOM Act as well as several cybersecurity bills in 2014 and 2015 indicates that this a rare area where there is significant bipartisan consensus. Indeed, the Fiscal 2016 Appropriations Act in effect endorsed the *International Strategy for Cyberspace*, calling on the State Department to report on its implementation, and the Digital Global Access Policy Act of 2016 (or "Digital GAP Act")[54] introduced this summer by the bipartisan leadership of the House Foreign Relations Committee and reported out by that committee would set digital diplomacy goals that resemble the *International Strategy*.[55] Its key focus is expanding access to digital communications around the globe, in effect codifying State's Global Connect program as national policy.

As the U.S. engages in international dialogue on issues in digital space, it is not just authoritarian governments that assert sovereign authority in ways that generate pressures to openness, interoperability, and the flow of information. Brazilian criminal courts suspended the service of WhatsApp in Brazil in an effort to get access to the content of messages sent via that app.[56] French privacy regulators seek to apply the EU's "right to be forgotten" not only to Google's European domains (google.fr, etc.) but also to google.com (the domain Google uses in the U.S.).[57] The U.S. itself obtained a warrant for data of an Irish citizen that Microsoft stores at a data center in Ireland[58] (In both Brazil and the U.S., appellate courts found that the actions reached too far. Google is appealing the French ruling to France's highest court, and Congress or the Supreme Court may act in response to the Microsoft warrant case).

Tensions between interests in territorial sovereignty on one hand and international trade and communications on the other are nothing new. They have existed for as long as nation-states have engaged in trade and other relations with one another. What is new is that, in a world in which bits move instantaneously almost anywhere and everywhere, nearly every nation has some claim to jurisdiction and some ability to project into another's territory. This exponentially multiplies the possible jurisdictions and threats. And applying rules from the physical world in virtual space can be challenging because the analogies can be unclear, especially if the technology is unfamiliar.

Even so, the United States and likeminded countries have made some headway in developing international norms in this space.

In the area of law enforcement access to data, the U.S. and U.K. have worked with stakeholders to shape a tentative agreement that may provide a template for updated mutual legal assistance treaties. More streamlined processes for these agreements will relieve some of the pressures for data localization and built-in access to communications.

Paving the way to applying principles of kinetic warfare to cyberspace, the U.S. has obtained multilateral declarations from the G-20, United Group of Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, and NATO that international law applies to state conduct in cyberspace. On the parallel path of "Track Two" diplomacy, experts from the U.S. and allies have developed the Tallinn 2.0 Manual on the International Law Applicable to Cyber Warfare to address the difficult question when a cyber-attack crosses a line that justifies self-defense.[59]

With regard to surveillance, the U.S. has initiated a shift in the previous norm for foreign intelligence surveillance. For centuries, regardless of whatever limits nation-states may impose on collecting intelligence involving their own citizens and within their own borders, spying elsewhere in the world has been considered fair game. This is the paradigm embodied in the Foreign Intelligence Surveillance Act since it was first adopted in the wake of the last big wave of disclosures in the 1970s about FBI and CIA domestic spying. That paradigm changed in January 2014 with the declaration in Presidential Policy Directive 28, that "all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information." This unilateral initiative sets a bar for other democratic countries.

> In a world in which bits move instantaneously almost anywhere and everywhere, nearly every nation has some claim to jurisdiction and some ability to project into another's territory.

Just as other countries are taking a systematic look at their digital strategies, the scope of intelligence collection is under debate outside the U.S. In the EU, a requirement that personal data transferred to the United States receive a level of protection from surveillance that is essentially equivalent to that under EU law has forced a look inward to consider just what this level of protection is. Not only do numerous EU member states have surveillance laws and programs that permit bulk collection of data with fewer democratic safeguards than in the U.S., but none applies its safeguards for people inside its borders to those outside.

As a result, even as objections to surveillance confront what needs to be done about the wave of ISIS-inspired attacks in the west, EU countries are having their own debate about national security powers, and the Court of Justice of the European Union and the European Court of Human Rights are considering what safeguards are required by basic laws on fundamental rights. Germany (one of the countries that employs bulk surveillance) is considering adopting something resembling the PPD-28 norm with legislation that would extend its domestic safeguards to people in other EU countries. The European debate about data that travels to the U.S. has also raised questions about what the level of protection is for data that travels to other EU trading partners, including Russia and China; and the European Commission intends to review its findings concerning countries other than the U.S.

The U.S. also has made headway in developing a norm for cyber-espionage for commercial purposes. This recurring topic was at the top of the agenda for President Obama's "shirtsleeve summit" with President Xi Jinping. Then, China made a sharp departure from its usual position of denying that commercial espionage takes place, and pledged

that it will not engage in such espionage. That progress provided the opening to widen the pledge by making it an action item for G-7 and G-20 discussions. Now Germany is seeking the same sort of understanding. It appears from reports on cyber threats that these discussions (coupled with calling out People's Liberation Army hackers with indictments) may be having an effect on China's behavior.

With cyber threats from non-state actors such as ISIS to more conventional criminals burgeoning in volume and sophistication, nation-states have important interests in common, and the progress on cyber-espionage offers promise for progress on these interests. This field provides an opportunity for the U.S. because of its lead in dealing with cybersecurity: it has greater capabilities and has had laws and policies in place for some time to address cybersecurity. In turn, its response to cyber threats relies heavily on public-private cooperation—the NIST Cybersecurity Framework, the use of Information Sharing and Analysis Centers and Information Sharing Operations Center, and other information-sharing. In exporting U.S. cybersecurity capabilities, there is an opportunity to promote the U.S. model of collaboration and governance in digital space. Cybersecurity exchanges with other countries have taken this opportunity. This avenue of promotion should continue and broaden.

In the economic arena, the Trans-Pacific Partnership includes in its e-commerce chapter a general agreement not to interfere with the free flow of information and a specific agreement not to require data localization; a similar provision is in leaked drafts of the Transatlantic Trade and Investment Partnership Agreement and the Trade in Service Agreement. These gains may be collateral damage of the growing political skepticism of trade agreements. In internet governance, OECD members endorsed *Principles for Internet Policy Making*, and the post-Snowden progress on Internet governance indicates that members are willing to live up to them in the main. In addition to broad advocacy in contexts like multilateral organizations and trade agreements, data localization measures and other technical barriers will require focused advocacy as they crop up.

CONCLUSION

It took 30 years to arrive at a treaty on the Law of the Sea (which the United States observes but has not ratified). Similarly, it will take decades to arrive at some global understanding on a global digital commons that is effectively open, interoperable, secure, and reliable.

Getting there will take global engagement, leadership, and cooperation from the United States and a systematic and coordinated broad effort across the government—in the military and security arena, in cybersecurity cooperation, in trade rules, in technical and operational governance. The next administration will have to take the baton in this arena forcefully throughout the executive branch. To succeed without repeating lapses of the past, this effort must reflect the openness and interoperability that is so central to U.S. policy in a digital world.

APPENDIX: THE DIGITAL POLICY "PLUM BOOK"

AGENCY	SUB-AGENCY	POSITIONS	COMMENTS
EXECUTIVE OFFICE OF THE PRESIDENT	National Security Council	Assistant to the President (A/P) for Homeland Security and Counter-terrorism	
		*A/P & Deputy National Security Adviser for International Economics	
		*Senior Director and Cyber Coordinator	
	National Economic Council	Deputy Assistant to the President & Deputy Director	
	Office of Science and Technology policy	*A/P & Chief Technology Officer	
		*Associate Director for Technology	
	U.S. Trade Representative (USTR)	Deputy Trade Representative	At least one deputy has been involved in data flow issues, which need involvement of several career Assistant USTRs
	Office of Management & Budget	*Intellectual Property Enforcement Coordinator	
		Associate Director for Economic Policy	
		Associate Director for General Government Programs	
	Council of Economic Advisers	Member	Consider an econometrician familiar with new methods of measurement

AGENCY	SUB-AGENCY	POSITIONS	COMMENTS
DEPARTMENT OF COMMERCE	Office of the Secretary	Secretary of Commerce	*At least one or more of these top five positions is mission-critical
		Deputy Secretary	
		General Counsel	
		Chief of Staff or Deputy Chief of Staff	
		*Director of Policy and Strategic Planning	
		*Senior Adviser for the Digital Economy	
	Economics & Statistics Administration	Under Secretary for Economic Affairs, Deputy Under Secretary, Chief Economist, and Deputy Chief Economist	At least one of these should understand the issues of measurement in the digital economy
	International Trade Administration	Assistant Secretary for Industry and analysis	
		*Deputy Assistant Secretary of for Services, Industry and Analysis	
	National Telecommunications & Information Administration	*Assistant Secretary and Administrator	
		*Deputy Assistant Secretary	
		*Chief of Staff	
		*Associate Administrator for Policy Analysis and Development	
	National Institute of Standards & Technology	*Under Secretary	
	Patent & Trademark Office	Under Secretary and Director	*At least one of these is mission critical
		Deputy Under Secretary	
		Chief of Staff	
		Administrator for Policy & External Affairs	

AGENCY	SUB-AGENCY	POSITIONS	COMMENTS
DEPARTMENT OF DEFENSE	Office of Secretary	Secretary	Defense is a key player and staff in the Secretary's and Deputy Secretary's office have supported this role.
		Deputy	
		*Under Secretary for Policy	Supported by appropriate deputies and assistant secretaries.
		Under Secretary for Acquisition, Technology & Logistics	Has a major impact on the marketplace for technology.
		*Director, Defense Advanced Research Projects Agency	Developed the internet (need I say more?)

AGENCY	SUB-AGENCY	POSITIONS	COMMENTS
DEPARTMENT OF EDUCATION	Office of Secretary	Assistant Secretary for Planning, Evaluation & Policy	An important role in education data

AGENCY	SUB-AGENCY	POSITIONS	COMMENTS
DEPARTMENT OF ENERGY		Under Secretary for Science	
		Assistant Secretary for Policy & International Affairs	

AGENCY	SUB-AGENCY	POSITIONS	COMMENTS
DEPARTMENT OF HEALTH & HUMAN SERVICES	Office of Civil Rights	*Director	A key role on health data

AGENCY	SUB-AGENCY	POSITIONS	COMMENTS
DEPARTMENT OF HOMELAND SECURITY	Office of Secretary	Secretary	DHS role in cybersecurity makes it a key player. Some combination of senior positions need to be conversant
		Deputy Secretary	
		Assistant Secretary for Policy	
		*Chief Privacy Officer	
		*Deputy Chief Privacy Officer	
	National Protection and Programs Directorate	Under Secretary	*At least one of these first three positions is mission-critical and needs to be well-supported by staff
		Deputy Under Secretary	
		Counselor to the Deputy Under Secretary	
		*Deputy Under Secretary, Cybersecurity	
		*Assistant Secretary for Cybersecurity & Telecommunications	

AGENCY	SUB-AGENCY	POSITIONS	COMMENTS
DEPARTMENT OF JUSTICE	Office of Attorney General	Attorney General	
		*Deputy Attorney General	Supported by Associate Deputy AGs. This office is where issues of law enforcement and civil liberties meet.
		*Chief Privacy & Civil Liberties Officer	
	Office of Legal Policy	*Assistant Attorney General	This office has handled the interface with "soft" security and economic issues
	Antitrust Division	Assistant Attorney General	*at least one or more of these positions is mission-critical. The Antitrust Competition Policy and Networks & Technology Enforcement divisions have a significant impact on innovation markets.
		Principal Deputy Assistant Attorney General	
		Senior Counsel (Competition Policy)	
	Criminal Division	*Assistant Attorney General or Deputy Assistants	The Computer Crimes & Intellectual Property Section of this division significantly affects activity in digital space. Oversight of this role requires a nuanced understanding of the impact of this enforcement.
	National Security Division	*Assistant Attorney General	

AGENCY	SUB-AGENCY	POSITIONS	COMMENTS
DEPARTMENT OF STATE	Office of Secretary	Secretary	One of these top three officials should be well-versed.
		Deputy Secretary	
		Counselor	
		*Cyber Coordinator	
	Office of Foreign Policy Planning	Director of Foreign Policy Planning	Office of Foreign Policy Planning needs specialized capability on digital issues.
		Principal Deputy Director of Policy Planning.	
	Bureau of Public Diplomacy & Public Affairs	Under Secretary for Public Diplomacy	
	Bureau of Civilian Security, Democracy & Human Rights	Under Secretary	*One or more of these officials is mission-critical because of internet freedom issues and their connection to the bureau's mission.
		Assistant Secretary for Democracy Human Rights & Labor	
	Bureau of Political Affairs	Representative to the United Nations	Various UN bodies (committees and special rapporteurs are involved) and the UN General Assembly is a forum for discussion of multilateral internet governance.
		*Representative to the Organization for Economic Cooperation and Development (OECD)	The OECD is a key international player on digital issues.
		*Representative to the European Union	Essential to transatlantic data transfer issues and US digital commerce in Europe
		Chief of Mission, China	These are particularly countries where issues affecting digital technology can be problematic
		Chief of Mission, France	
		Chief of Mission, Germany	
	Bureau for Economic Growth, Energy & the Environment	*Under Secretary	Currently delegated authority under PPD-28 and designated as "Ombudsperson" for EU complaints about US intelligence collection

AGENCY	SUB-AGENCY	POSITIONS	COMMENTS
DEPARTMENT OF STATE	Bureau for Economic Growth, Energy & the Environment	Assistant Secretary for Economic & Business Affairs	
		*Deputy Assistant Secretary for International Communications & Information Policy and U.S. Coordinator	

AGENCY	SUB-AGENCY	POSITIONS	COMMENTS
DEPARTMENT OF TREASURY	Office of Secretary	Secretary	Treasury is the key player on the development of virtual currency/ means of exchange as well as international networks for trusted information exchange (SWIFT etc.)
		*Deputy Secretary	Oversees the Committee on Foreign Investment in the U.S.
	Bureau of International Affairs	Under Secretary	
	Bureau of Terrorism & Financial Intelligence	Under Secretary	See comment above on the Office of Secretary. This bureau oversees financial crimes enforcement.

*Indicates positions where broad understanding of digital issues is mission-critical.

Source: United States. Congress. Government Printing Office. *United States Government Policy and Supporting Positions (Plum Book).* Washington: Government Printing Office, *2012. 1 Dec. 2012. Web.*
[60]

ENDNOTES

"Note: I am grateful for the research and editing assistance of Jack Karsten and Maximilian Fiege of The Brookings Institution, and to colleagues, former colleagues, family, and others whose ideas and comments have helped to inform and improve this paper. Errors or misconceptions that remain are mine."

1 "NSA Slides Explain the PRISM Data-collection Program." The Washington Post, 6 June 2013. Web.

2 Gellman, Barton, and Laura Poitras. "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program." *The Washington Post*. 7 June 2013. Web.

3 The White House. Office of the Press Secretary. *Statement by the President.* June 2013. Web.

4 Levy, Steven. "How the NSA Almost Killed the Internet." *Wired* 1 July 2014. Print.

5 United States of America. The White House. Office of the President. *International Strategy for Cyberspace*. 16 May 2011. Web.

6 OECD. *Principles for Internet Policy Making*. 2014. Print.

7 Exec. Order No. 13636, 3 C.F.R. (2013). Print.

8 United States of America. Department of Commerce. National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. 12 Feb. 2014. Web.

9 The White House. Office of the Press Secretary. *Statement by the Press Secretary on the Review Group on Intelligence and Communications Technology*. N.p., 27 Aug. 2013. Web.

10 "Review of U.S. Signals Intelligence." President Obama Speaks on U.S. Intelligence Programs. Speech.

11 McCarthy, Tom. "Obama Announces New Limits on NSA Surveillance Programs." *The Guardian* 17 Jan. 2014. Print.

12 Presidential Policy Directive 28, 3 C.F.R. (2014).

13 *Big Data: Seizing Opportunities, Preserving Values*. Rep. Executive Office of the President, May 2014. Web.

14 The White House. *National Security Strategy*. Feb. 2015. Web.

15 Department of Defense. *Quadrennial Defense Review*. Rep. 4 Mar. 2014. Web.

16 Economics and Statistics Administration. *Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services*. Rep. Department of Commerce, 27 Jan. 2014. Web.

17 U.S. International Trade Commission. *Digital Trade in the U.S. and Global Economies, Part 2*. Aug. 2014. Web.

18 Manyika, James, Sree Ramaswamy, Somesh Khanna, et al. *Digital America: A Tale of the Haves and Have-mores*. Rep. McKinsey Global Institute, Dec. 2015. Web.

19 Accenture. *Digital Disruption: The Growth Multiplier*. Jan. 2016. Web.

20 *OECD Digital Economy Outlook 2015*. Organization for Economic Development, 2015. Print.

21 Manyika, James, Susan Lund, Jacques Bughin, et al. *Digital Globalization: The New Era of Global Flows*. Rep. McKinsey Global Institute, Feb. 2016. Web.

22 Ritzer, George. *Globalization: The Essentials*. Oxford: Wiley-Blackwell, 2011. Print.

23 *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper*. Rep. Cisco, 1 Feb. 2016. Web.

24 Cerwall, Patrick, Jonsson, Peter, et al. *Ericsson Mobility Report: On the Pulse of the Networked Society*. Rep. Ericsson,

Nov. 2015. Web.

25 Brynjolfsson, Erik, and Andrew McAfee. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. January 2014. Print.

26 Ezell, Stephen. "Forced Localization Policies Threaten Global Trade in Innovative Industries." Bridges 38 (2013) Print. Innovation Matters.

27 Orlik, Tom. "An Insider's Guide to 'Shirt-Sleeves Summit'." *The Wall Street Journal* 7 June 2013. Print.

28 Williams, Katie Bo. "G20 Nations Reach Anti-Hacking Pledge." *The Hill* 17 Nov. 2015. Print.

29 Department of Justice. Office of Public Affairs. *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*. May 2014. Print.

30 McDonald, Soraya Nadia. "John Oliver's Net Neutrality Rant May Have Caused FCC Site Crash." *The Washington Post* 4 June 2014. Web.

31 The General Assembly. *Transforming Our World: The 2030 Agenda for Sustainable Development*. Resolution. The United Nations, 21 Oct. 2015. Web.

32 Office of the Historian. "National Security Act of 1947." Blog post. Department of State. Web.

33 Presidential Policy Directive – 1 (March 2, 2009). Print.

34 Memorandum for Heads of Executive Departments and Agencies, January 21, 2009, https://www/whitehouse.gov/sites/default/files/omb/assets/memoranda_fy2009/m09-12.pdf.

35 Exec. Order No. 12835 (1993). Print.

36 Exec. Order No. 13704. (2015). Print.

37 "About Us." *The U.S. Digital Service*. The White House. Web.

38 "Technology." *Issues*. The White House, 18 May 2015. Web.

39 United States. The White House. Office of Management and Budget. *CIRCULAR NO. A-119 Revised*. By Franklin D. Raines. February 10, 1998. Print.

40 National Technology Transfer and Advancement Act of 1995, Section 12(d), Public Law 104-113.

41 Criminal Division of the Department of Justice and Enforcement Division of the U.S. Securities and Exchange Commission. *A Resource Guide to the U.S. Foreign Corrupt Practices Act*. November 2012. Print.

42 Inskeep, Steven. "Transcript: NSA Deputy Director John Inglis." NPR, 10 Jan. 2014. Web.

43 Phillips, Macon. "We the People: Announcing White House Petitions & How They Work." The White House, 01 Sept. 2011. Web.

44 Macon Phillips, Victoria Espinel, Aneesh Chopra, and Howard A. Schmidt. "Obama Administration Responds to We the People Petitions on SOPA and Online Piracy." Blog post. The White House, 14 Jan. 2012. Web.

45 Liptak, Kevin. "Obama Bristles at Suggestion He's Shifted on Snooping." *CNN*18 June 2013. Print.

46 Kirschbaum, Erik. "Merkel, Hollande to Discuss European Communication Network Avoiding U.S." *Reuters* 15 Feb. 2014. Print.

47 Sterling, Bruce. "Pres. Dilma Rousseff at the UN General Assembly." Wired.com. Conde Nast Digital, 24 Sept. 2013. Web.

48 European Union. Court of Justice. *The Court of Justice Declares That the Commission's US Safe Harbour Decision Is Invalid*. Luxembourg. October 6, 2015. Print.

49 *Protecting Internet Freedom: Implications of Ending U.S. Oversight of the Internet*, 114th Cong. (2016) (testimony of Lawrence E. Strickling, Assistant Secretary for Communications and Information National Telecommunications and Informa-

tion Administration). Print.

50 U.S. Department of Commerce. *Overview of the EU-U.S. Privacy Shield Framework for Interested Participants*. Issue brief. July 12, 2016. Print.

51 United States. Cong. House. Judiciary; Intelligence; Financial Services. *USA FREEDOM Act 2015*. By James F. Sensenbrenner. 114th Cong., 1st sess. HR 2048. Print.

52 United States. Cong. Judiciary; Oversight and Government Reform; Senate Judiciary. *Judicial Redress Act of 2015*. By James F. Sensenbrenner. 114th Cong., 1st sess. Cong 1428. Print.

53 BBC. "China Internet: Xi Jinping Calls for 'Cyber Sovereignty'" 16 Dec. 2015. Print.

54 United States. Cong. Senate. Foreign Relations. *Digital GAP Act*. By Edward R. Royce. 114th Cong., 2nd sess. S 5537. Print.

55 United States. Cong. Appropriations; Senate Appropriations. *Consolidated Appropriations Act of 2015*. By Charles W. Dent. 114th Cong., 2nd sess. Cong 2029. Print.

56 Boulden, Jim. "WhatsApp Was Blocked for 100 Million Brazilians - Now Its Back!" *CNN Money* 17 Dec. 2015. Print.

57 "Right to Delisting: Google Informal Appeal Rejected." CNIL, 21 Sept. 2015. Web.

58 Ely, Alex. "Second Circuit Oral Argument in the Microsoft-Ireland Case: An Overview." Lawfare. Lawfare Institute, 10 Sept. 2015. Web.

59 NATO. Cooperative Cyber Defense Centre of Excellence. *Tallinn Manual 2.0*. 2016. Print.

60 United States. Congress. Government Printing Office. *United States Government Policy and Supporting Positions (Plum Book)*. Washington: Government Printing Office, 2012. 1 Dec. 2012. Web.

GOVERNANCE STUDIES

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

EDITING
Liz Sablich

PRODUCTION & LAYOUT
Cathy Howell

EMAIL YOUR COMMENTS TO GSCOMMENTS@BROOKINGS.EDU