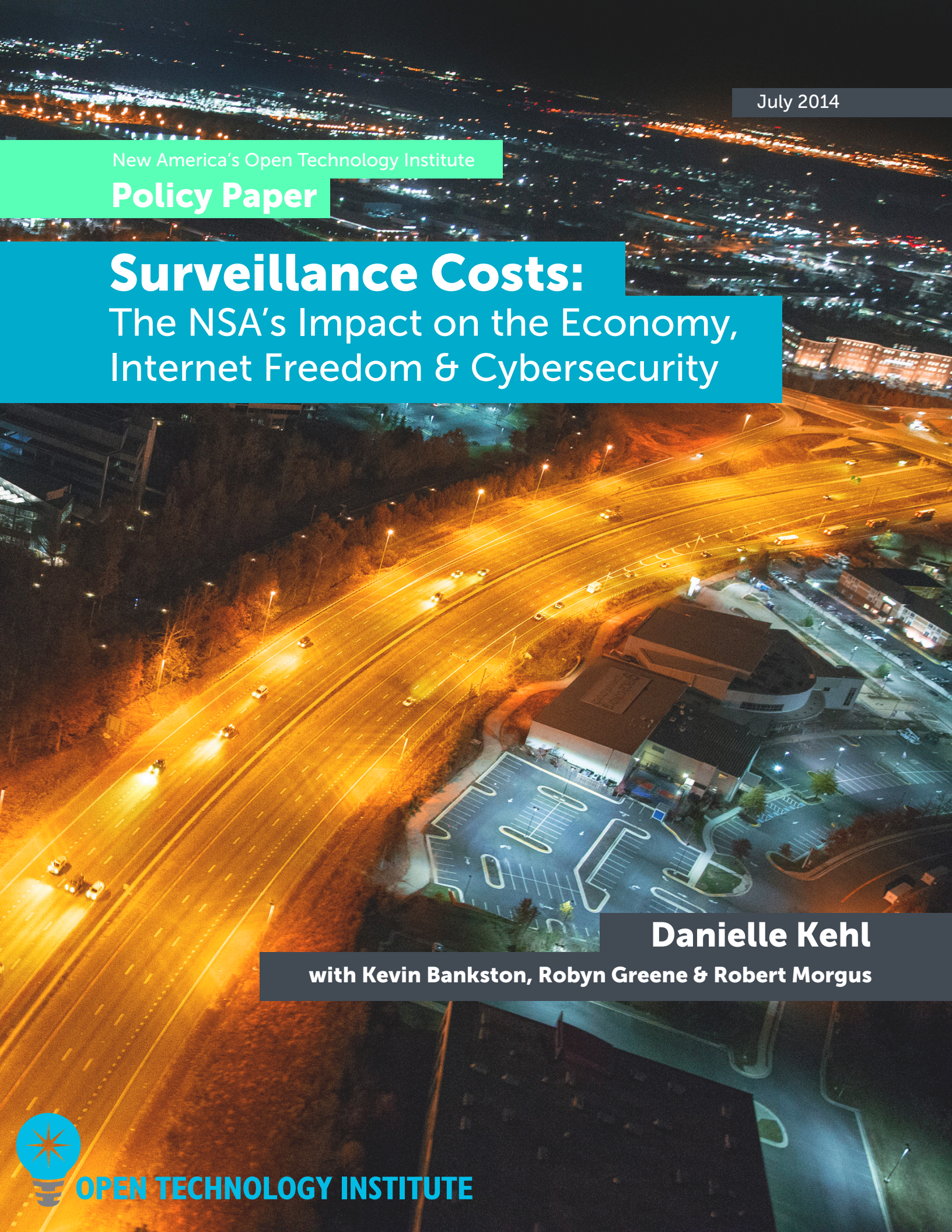

July 2014

New America's Open Technology Institute

Policy Paper

Surveillance Costs:

The NSA's Impact on the Economy, Internet Freedom & Cybersecurity

Danielle Kehl

with Kevin Bankston, Robyn Greene & Robert Morgus

OPEN TECHNOLOGY INSTITUTE

About the Authors

Danielle Kehl is a Policy Analyst at New America's Open Technology Institute (OTI). Kevin Bankston is the Policy Director at OTI, Robyn Greene is a Policy Counsel at OTI, and Robert Morgus is a Research Associate at OTI.

Acknowledgements

The authors would like to thank a number of individuals for their guidance and assistance on this paper, including Alan Davidson, Joseph Lorenzo Hall, Katharine Kendrick, Rebecca MacKinnon, Ben Scott, and Cynthia Wong. The authors would also like to express their gratitude to Martin Sigalow and Patrick Lucey for their assistance on this paper.

About New America

New America is a nonprofit, nonpartisan public policy institute that invests in new thinkers and new ideas to address the next generation of challenges facing the United States.

New America's Open Technology Institute formulates policy and regulatory reforms to support open architectures and open source innovations and facilitates the development and implementation of open technologies and communications networks. OTI promotes affordable, universal, and ubiquitous communications networks. OTI provides in-depth, objective research, analysis, and findings for policy decision-makers and the general public.

The cover photo depicts the National Reconnaissance Office in Chantilly, Virginia. The photograph was taken by Trevor Paglen and is available for reuse here: https://firstlook.org/theintercept/article/2014/02/10/new-photos-of-nsa-and-others/.

Contents

Executive Summary **2**

I. Background & Introduction **4**
What is the NSA doing? 4
What is it costing us? 5

II. Direct Economic Costs to American Companies **7**
Costs to the U.S. Cloud Computing Industry and Related Business 7
Cost to Overseas Tech Sales 10
Cost to Public Trust in American Companies 11

III. Economic and Technological Costs of Data Localization and Protection Proposals **14**
Mandatory Data Localization and the Costs of a Bordered Internet 14
Case Studies: Germany, India, and Brazil 15
Data Protection Proposals and Cost to European Trade Relations 17
The Combined Costs of Data Localization and Data Protection Proposals 18

IV. Political Costs to U.S. Foreign Policy **20**
Costs to the Internet Freedom Agenda and U.S. Credibility in Internet Governance 20
Costs to Internet Freedom Beyond Internet Governance 23
Broader Foreign Policy Costs 24

V. Costs to Cybersecurity **26**
Compromising Security Standards 27
Creating Security Vulnerabilities 29
Withholding Security Vulnerabilities 31
Hacking the Internet 32

VI. Conclusion and Recommendations **35**

Executive Summary

It has been over a year since *The Guardian* reported the first story on the National Security Agency's surveillance programs based on the leaks from former NSA contractor Edward Snowden, yet the national conversation remains largely mired in a simplistic debate over the tradeoffs between national security and individual privacy. It is time to start weighing the overall costs and benefits more broadly.

While intelligence officials have vigorously defended the merits of the NSA programs, they have offered little hard evidence to prove their value—and some of the initial analysis actually suggests that the benefits of these programs are dubious. Three different studies—from the President's Review Group on Intelligence and Communications Technologies, the Privacy and Civil Liberties Oversight Board, and the New America Foundation's International Security Program—question the value of bulk collection programs in stopping terrorist plots and enhancing national security. Meanwhile, there has been little sustained discussion of the costs of the NSA programs beyond their impact on privacy and liberty, and in particular, how they affect the U.S. economy, American foreign policy, and the security of the Internet as a whole.

This paper attempts to quantify and categorize the costs of the NSA surveillance programs since the initial leaks were reported in June 2013. Our findings indicate that the NSA's actions have already begun to, and will continue to, cause significant damage to the interests of the United States and the global Internet community. Specifically, we have observed the costs of NSA surveillance in the following four areas:

- **Direct Economic Costs to U.S. Businesses:** American companies have reported declining sales overseas and lost business opportunities, especially as foreign companies turn claims of products that can protect users from NSA spying into a competitive advantage. The cloud computing industry is particularly vulnerable and could lose billions of dollars in the next three to five years as a result of NSA surveillance.

- **Potential Costs to U.S. Businesses and to the Openness of the Internet from the Rise of Data Localization and Data Protection Proposals:** New proposals from foreign governments looking to implement data localization requirements or much stronger data protection laws could compound economic losses in the long term. These proposals could also force changes to the architecture of the global network itself, threatening free expression and privacy if they are implemented.

- **Costs to U.S. Foreign Policy:** Loss of credibility for the U.S. Internet Freedom agenda, as well as damage to broader bilateral and multilateral relations, threaten U.S. foreign policy interests. Revelations about the extent of NSA surveillance have already colored a number of critical interactions with nations such as Germany and Brazil in the past year.

- **Costs to Cybersecurity:** The NSA has done serious damage to Internet security through its weakening of key encryption standards, insertion of surveillance backdoors into widely-used hardware and software products, stockpiling rather than responsibly disclosing information about software security vulnerabilities, and a variety of offensive hacking operations undermining the overall security of the global Internet.

The U.S. government has already taken some limited steps to mitigate this damage and begin the slow, difficult process of rebuilding trust in the United States as a responsible steward of the Internet. But the reform efforts to date have been relatively narrow, focusing primarily on the surveillance programs' impact on the rights of U.S. citizens. Based on our findings, we recommend that the U.S. government take the following steps to address the broader concern that the NSA's programs are impacting our economy, our foreign relations, and our cybersecurity:

1. **Strengthen privacy protections** for both Americans and non-Americans, within the United States and extraterritorially.

2. Provide for **increased transparency around government surveillance**, both from the government and companies.

3. **Recommit to the Internet Freedom agenda** in a way that directly addresses issues raised by NSA surveillance, including moving toward international human-rights based standards on surveillance.

4. Begin the **process of restoring trust in cryptography standards** through the National Institute of Standards and Technology.

5. Ensure that the U.S. government **does not undermine cybersecurity by inserting surveillance backdoors into hardware or software** products.

6. **Help to eliminate security vulnerabilities in software**, rather than stockpile them.

7. Develop clear policies about **whether, when, and under what legal standards it is permissible for the government to secretly install malware** on a computer or in a network.

8. **Separate the offensive and defensive functions of the NSA** in order to minimize conflicts of interest.

I. Background & Introduction

What is the NSA doing?

As Congress debated the reauthorization of the USA PATRIOT Act's Section 215 in 2011, Senator Ron Wyden (D-OR) began a slow but steady drumbeat for reform by raising concerns about how the National Security Agency (NSA) was secretly interpreting and using the law. "When the American people find out how their government has secretly interpreted the Patriot Act," he warned, "they will be stunned and they will be angry."[1] Over two years later, on June 5, 2013, *The Guardian* published the first leaked document by former NSA contractor Edward Snowden. Readers around the world were shocked to learn about what Senator Wyden had been referring to all along: for years, the NSA has been collecting nearly all of the phone records generated by major telephone companies such as Verizon on an ongoing, daily basis under Section 215's authority[2]—and has been using a secret, and now widely discredited, interpretation of the law to do it.[3]

Over the course of the past year, the world has learned that this bulk collection program was just one small part of the NSA's massive surveillance apparatus.[4] Just a day after the first leak, *The Washington Post* ran a story about PRISM, the NSA's "downstream" collection program authorized under Section 702 of the Foreign Intelligence Surveillance Act (FISA). Under the PRISM program, the NSA compels major tech companies like Google, Yahoo, Microsoft, Facebook, and Twitter to turn over the contents of communications stored on company servers that have been sent or received by targets that the NSA reasonably believes are outside of the United States.[5] While few details are known about the programs the NSA operates under Section 702, and several of the details regarding the PRISM program are a subject of debate,[6] a declassified 2011 Foreign Intelligence Surveillance Court opinion revealed that the NSA collects more than 250,000,000 Internet communications annually using Section 702 and that "the vast majority of these communications are obtained from Internet service providers" through the PRISM program.[7] The remainder of those communications comes from Section 702 surveillance that is conducted "upstream"—that is, surveillance conducted not by obtaining stored communications from cloud providers' servers but by tapping directly into the U.S. Internet backbone network that carries domestic, international, and foreign communications.[8]

Beyond NSA surveillance inside the United States under Section 215 and Section 702, the NSA engages in massive surveillance of Internet and telephone communications outside of the country as well. Unconstrained by statute and subject only to Executive Branch oversight under the Reagan-era Executive Order 12333,[9] this extraterritorial surveillance was revealed in October 2013 to include the monitoring of key private data links that connect Google and Yahoo data centers around the world—monitoring that in just 30 days processed 181,280,466 new records that traversed those links.[10] Similarly, the NSA is using Executive Order 12333 to authorize the collection of millions of email address books globally,[11] and the recording of vast numbers of international phone calls—sometimes all of the phone traffic in an entire country.[12] Executive Order 12333 is also presumably the authority under which the NSA is assisting British intelligence agencies in acquiring millions of webcam photos sent by users of Yahoo,[13] and under which the NSA is collecting over five billion cell phone location data points per day, enabling it to track individuals' movements and relationships with others.[14]

In addition to the mass surveillance operations that have dominated the past year's headlines, leaked documents revealed that the NSA employs a unit of elite hackers called the Office of Tailored Access Operations that engages in extensive and highly secretive cyber operations.[15] These operations include cracking and undermining encryption standards, inserting vulnerabilities into widely-used software and hardware products, secretly stockpiling information about software vulnerabilities that the NSA discovers so that they can be exploited for intelligence purposes rather than fixed, and developing a global network of malware that has been secretly installed on computers and in networks around the world to better facilitate the NSA's surveillance.[16]

What is it costing us?

One year after the initial leaks, it is time to start evaluating how the programs impact U.S. interests both at home and abroad. The national conversation around NSA surveillance in the past year has remained largely mired in a debate over the tradeoffs between individual privacy and national security, but this framing is overly simplistic. As the President's Review Group on Intelligence and Communications Technologies explained in its December 2013 report and recommendations, "Some people believe that [national security and privacy] are in irreconcilable conflict with one another... We firmly reject this view. It is unsupported by the facts. It is inconsistent with our traditions and our law."[17] The Review Group's report echoes calls that have been made by a wide range of individuals in the past year, from government officials to journalists and privacy advocates: that we must evaluate the actions of the NSA not only with regard to how they infringe upon civil liberties and human rights in the name of protecting national security, but also how these programs can be detrimental to our economic stability and cybersecurity. It is time to more broadly weigh the overall costs versus the net benefits of the NSA's activities.

> **"Some people believe that [national security and privacy] are in irreconcilable conflict with one another. They contend that in the modern era... the nation must choose between them. We firmly reject this view."**
>
> *-The President's Review Group on Intelligence and Communications Technologies*

So far, the purported benefits of the programs remain unsubstantiated. While intelligence officials and representatives of the Obama Administration have defended the merits of the NSA programs,[18] they have offered little hard evidence to prove their value. To the contrary, initial analyses of the NSA's bulk records collection program suggest that its benefits are dubious at best, particularly compared to the program's vast breadth. A January 2014 study from the New America Foundation's International Security Program, for example, concluded that "the government's claims about the role that NSA 'bulk' surveillance of phone and email communications records has had in keeping the United States safe from terrorism... are overblown and even misleading."[19] Similarly, in its review of the telephone records collection program under Section 215 of the USA PATRIOT Act, the Privacy and Civil Liberties Oversight Board (PCLOB) could not identify a single instance in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation.[20] The President's Review Group concurred, emphasizing that "there is always a possibility that acquisition of more information—whether in the US or abroad—might ultimately prove helpful. But that abstract possibility does not, by itself, provide a sufficient justification for acquiring more information."[21] Although the PCLOB did find in a separate report that "the information the [Section 702] program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence,"[22] it provided no details and did not weigh those purported benefits against the various costs of the surveillance. Furthermore, its conclusions were undermined just days later when *The Washington Post* revealed that nine out of ten of the Internet users swept up in the NSA's Section 702 surveillance are not legally targeted foreigners.[23]

Meanwhile, there has been little sustained discussion of the tangible costs of the NSA programs beyond their impact on privacy and liberty. First, there is the direct cost to American taxpayers, totaling many billions of dollars.[24] Moreover, the NSA programs also impact the U.S. economy, foreign policy, and the security of the Internet as a whole. This paper seeks to categorize and quantify these impacts. We have observed a significant erosion in trust in the past year, not only in the actions and motives of the American government but also in major technology companies and the security of the Internet itself. This lack of confidence translates to real costs, which we discuss at length in the paper:

- In Part II, we discuss the economic impact of NSA surveillance, focusing on the cost to the cloud computing industry, which is projected to lose billions of dollars in the next three to five years, and declining technology sales overseas, as individuals and governments

> **"The government's claims about the role that NSA 'bulk' surveillance of phone and email communications records has had in keeping the United States safe from terrorism... are overblown and even misleading."**
>
> -Peter Bergen *et al., "Do NSA's Bulk Surveillance Programs Stop Terrorists?"*

turn to foreign alternatives that claim to be more secure than American products.

- In Part III, we discuss the rise of data localization and data protection proposals from foreign governments, which could compound economic losses in the long term and force changes to the architecture of the global network that threaten free expression and privacy.
- In Part IV, we discuss the impact of NSA surveillance on U.S. foreign policy interests, focusing on the loss of credibility for the U.S. Internet Freedom agenda and the damage to broader bilateral and multilateral relations.
- In Part V, we discuss the cost to Internet security, examining how the NSA has weakened encryption standards, inserted backdoors into Internet products, stockpiled security vulnerabilities, and carried out a variety of offensive hacking operations on commercial products that individual users rely on.

Based on these findings, in Part VI we lay out a series of recommendations aimed at restoring faith in American tech companies, the U.S. government, and the security of the Internet as a whole.

II. Direct Economic Costs to American Companies

"It is becoming clear that the post-9/11 surveillance apparatus may be at cross-purposes with our high-tech economic growth," declared Third Way's Mieke Eoyang and Gabriel Horowitz in December 2013. "The economic consequences [of the recent revelations] could be staggering."[25] A *TIME* magazine headline projected that "NSA Spying Could Cost U.S. Tech Giants Billions," predicting losses based on the increased scrutiny that economic titans like Google, Microsoft, Facebook, and Yahoo have faced both at home and abroad since last June.[26] The NSA's actions pose a serious threat to the current value and future stability of the information technology industry, which has been a key driver of economic growth and productivity in the United States in the past decade.[27] In this section, we examine how emerging evidence about the NSA's extensive surveillance apparatus has already hurt and will likely continue to hurt the American tech sector in a number of ways, from dwindling U.S. market share in industries like cloud computing and webhosting to dropping tech sales overseas. The impact of individual users turning away from American companies in favor of foreign alternatives is a concern. However, the major losses will likely result from diminishing confidence in U.S. companies as trustworthy choices for foreign government procurement of products and services and changing behavior in the business-to-business market.

Costs to the U.S. Cloud Computing Industry and Related Business

Trust in American businesses has taken a significant hit since the initial reports on the PRISM program suggested that the NSA was directly tapping into the servers of nine U.S. companies to obtain customer data for national security investigations.[28] *The Washington Post*'s original story on the program provoked an uproar in the media and prompted the CEOs of several major companies to deny knowledge of or participation in the program.[29] The exact nature of the requests made through the PRISM program was later clarified,[30] but the public attention on the relationship between American companies and the NSA still created a significant trust gap, especially in industries where users entrust companies to store sensitive personal and commercial data. "Last year's national security leaks have also had a commercial and financial impact on American technology companies that have provided these records," noted Representative Bob Goodlatte, a prominent Republican leader and Chairman of the House Judiciary Committee, in May 2014. "They have experienced backlash from both American and foreign consumers and have had their competitive standing in the global marketplace damaged."[31]

"Last year's national security leaks have also had a commercial and financial impact on American technology companies that have provided these records. They have experienced backlash from both American and foreign consumers and have had their competitive standing in the global marketplace damaged."

-Rep. Bob Goodlatte, Chairman of the House Judiciary Committee

Given heightened concerns about the NSA's ability to access data stored by U.S. companies, it is no surprise that American companies offering cloud computing and webhosting services are among those experiencing the most acute economic fallout from NSA surveillance. Within just a few weeks of the first disclosures, reports began to emerge that American cloud computing companies like Dropbox and Amazon Web Services were starting to lose business to overseas competitors.[32] The CEO of Artmotion, one of Switzerland's largest offshore hosting

providers, reported in July 2013 that his company had seen a 45 percent jump in revenue since the first leaks,[33] an early sign that the country's perceived neutrality and strong data and privacy protections[34] could potentially be turned into a serious competitive advantage.[35] Foreign companies are clearly poised to benefit from growing fears about the security ramifications of keeping data in the United States. In a survey of 300 British and Canadian businesses released by PEER 1 in January 2014,[36] 25 percent of respondents indicated that they were moving data outside of the U.S. as a result of the NSA revelations. An overwhelming number of the companies surveyed indicated that security and data privacy were their top concerns, with 81 percent stating that they "want to know exactly where their data is being hosted." Seventy percent were even willing to sacrifice performance in order to ensure that their data was protected.[37]

In a survey of 300 British and Canadian businesses released by PEER 1 in January 2014, 25 percent of respondents indicated that they were moving data outside of the U.S. as a result of the NSA revelations.

It appears that little consideration was given over the past decade to the potential economic repercussions if the NSA's secret programs were revealed.[38] This failure was acutely demonstrated by the Obama Administration's initial focus on reassuring the public that its programs primarily affect non-Americans, even though non-Americans are also heavy users of American companies' products. Facebook CEO Mark Zuckerberg put a fine point on the issue, saying that the government "blew it" in its response to the scandal. He noted sarcastically: "The government response was, 'Oh don't worry, we're not spying on any Americans.' Oh, wonderful: that's really helpful to companies [like Facebook] trying to serve people around the world, and that's really going to inspire confidence in American internet companies."[39] As Zuckerberg's comments reflect, certain parts of the American technology industry are particularly vulnerable to international backlash since growth is heavily dependent on foreign markets. For example, the U.S. cloud computing industry has grown from an estimated $46 billion in 2008 to $150 billion in 2014, with nearly 50 percent of worldwide cloud-computing revenues coming from the U.S.[40] R Street Institute's January 2014 policy study concluded that in the next few years, new products and services that rely on cloud computing will become increasingly pervasive. "Cloud computing is also the root of development for the emerging generation of Web-based applications—home security, outpatient care, mobile payment, distance learning, efficient energy use and driverless cars," writes R Street's Steven Titch in the study. "And it is a research area where the United States is an undisputed leader."[41] This trajectory may be dramatically altered, however, as a consequence of the NSA's surveillance programs.

Economic forecasts after the Snowden leaks have predicted significant, ongoing losses for the cloud-computing industry in the next few years. An August 2013 study by the Information Technology and Innovation Foundation (ITIF) estimated that revelations about the NSA's PRISM program could cost the American cloud computing industry $22 to $35 billion over the next three years.[42] On the low end, the ITIF projection suggests that U.S. cloud computing providers would lose 10 percent of the foreign market share to European or Asian competitors, totaling in about $21.5 billion in losses; on the high-end, the $35 billion figure represents about 20 percent of the companies' foreign market share. Because the cloud computing industry is undergoing rapid growth right now—a 2012 Gartner study predicted global spending on cloud computing would increase by 100 percent from 2012 to 2016, compared to a 3 percent overall growth rate in the tech industry as a whole[43]—vendors in this sector are particularly vulnerable to shifts in the market. Failing to recruit new customers or losing a competitive advantage due to exploitation by rival companies in other countries can quickly lead to a dwindling market share. The ITIF study further notes that "the percentage lost to foreign competitors could go higher if foreign governments enact protectionist trade barriers that effectively cut out U.S. providers," citing early calls from German data protection authorities to suspend the U.S.-EU Safe Harbor program (which will be discussed at length in the next section).[44] As the R Street Policy Study highlights, "Ironically, the NSA turned the competitive edge U.S. companies have in cloud computing into a liability, especially in Europe."[45]

In a follow up to the ITIF study, Forrester

Research analyst James Staten argued that the think tank's estimates were low, suggesting that the actual figure could be as high as $180 billion over three years.[46] Staten highlighted two additional impacts not considered in the ITIF study. The first is that U.S. customers—not just foreign companies—would also avoid US cloud providers, especially for international and overseas business. The ITIF study predicted that American companies would retain their domestic market share, but Staten argued that the economic blowback from the revelations would be felt at home, too. "You don't have to be a French company, for example, to be worried about the US government snooping in the data about your French clients," he wrote.[47] Moreover, the analysis highlighted a second and "far more costly" impact: that foreign cloud providers, too, would lose as much as 20 percent of overseas and domestic business because of similar spying programs conducted by other governments. Indeed, the NSA disclosures "have prompted a fundamental re-examination of the role of intelligence services in conducting coordinated cross-border surveillance," according to a November 2013 report by Privacy International on the "Five Eyes" intelligence partnership between the United States, the United Kingdom, Canada, Australia, and New Zealand.[48] Staten predicts that as the surveillance landscape around the world becomes more clear, it could have a serious negative impact on all hosting and outsourcing services, resulting in a 25 percent decline in the overall IT services market, or about $180 billion in losses.[49]

> **"Frankly I think the government blew it... The government response was, 'Oh don't worry, we're not spying on any Americans.' Oh, wonderful: that's really helpful to companies trying to serve people around the world, and that's really going to inspire confidence in American internet companies."**
>
> -Mark Zuckerberg, CEO of Facebook

Recent reports suggest that things are, in fact, moving in the direction that analysts like Castro and Staten suggested.[50] A survey of 1,000 "[Information and Communications Technology (ICT)] decision-makers" from France, Germany, Hong Kong, the UK, and the USA in February and March 2014 found that the disclosures "have had a direct impact on how companies around the world think about ICT and cloud computing in particular."[51] According to the data from NTT Communications, 88 percent of decision-makers are changing their purchasing behavior when it comes to the cloud, with the vast majority indicating that the location of the data is very important. The results do not bode well for recruitment of new customers, either—62 percent of those currently not storing data in the cloud indicated that the revelations have since prevented them from moving their ICT systems there. And finally, 82 percent suggested that they agree with proposals made by German Chancellor Angela Merkel in February 2014 to have separate data networks for Europe, which will be discussed in further detail in Part III of this report. Providing direct evidence of this trend, Servint, a Virginia-based webhosting company, reported in June 2014 that international clients have declined by as much as half, dropping from approximately 60 percent of its business to 30 percent since the leaks began.[52]

With faith in U.S. companies on the decline, foreign companies are stepping in to take advantage of shifting public perceptions. As Georg Mascolo and Ben Scott predicted in a joint paper published by the Wilson Center and the New America Foundation in October 2013, "Major commercial actors on both continents are preparing offensive and defensive strategies to battle in the market for a competitive advantage drawn from Snowden's revelations."[53] For example, Runbox, a small Norwegian company that offers secure email service, reported a 34 percent jump in customers since June 2013.[54] Runbox markets itself as a safer email and webhosting provider for both individual and commercial customers, promising that it "will never disclose any user data unauthorized, track your usage, or display any advertisements."[55] Since the NSA revelations, the company has touted its privacy-centric design and the fact that its servers are located in Norway as a competitive advantage. "Being firmly located in Norway, the Runbox email service is governed by strict privacy regulations and is a safe alternative to American email services as well as cloud-based services that move data across borders and jurisdictions," company representatives wrote on

> **"Major commercial actors on both continents are preparing offensive and defensive strategies to battle in the market for a competitive advantage drawn from Snowden's revelations."**
>
> -Georg Mascolo and Ben Scott, *"Lessons from the Summer of Snowden"*

its blog in early 2014.[56] F-Secure, a Finnish cloud storage company, similarly emphasizes the fact that "its roots [are] in Finland, where privacy is a fiercely guarded value."[57] Presenting products and services as 'NSA-proof' or 'safer' alternatives to American-made goods is an increasingly viable strategy for foreign companies hoping to chip away at U.S. tech competiveness.[58]

Costs to Overseas Tech Sales

The economic impact of NSA spying does not end with the American cloud computing industry. According to *The New York Times*, "Even as Washington grapples with the diplomatic and political fallout of Mr. Snowden's leaks, the more urgent issue, companies and analysts say, is economic."[59] In the past year, a number of American companies have reported declining sales in overseas markets like China (where, it must be noted, suspicion of the American government was already high before the NSA disclosures), loss of customers including foreign governments, and increased competition from non-U.S. services marketing themselves as 'secure' alternatives to popular American products.

There is already significant evidence linking NSA surveillance to direct harm to U.S. economic interests. In November 2013, Cisco became one of the first companies to publicly discuss the impact of the NSA on its business, reporting that orders from China fell 18 percent and that its worldwide revenue would decline 8 to 10 percent in the fourth quarter, in part because of continued sales weakness in China.[60] New orders in the developing world fell 12 percent in the third quarter, with the Brazilian market dropping roughly 25 percent of its Cisco sales.[61] Although John Chambers, Cisco's CEO, was hesitant to blame all losses on the NSA, he acknowledged that it was likely a factor in declining Chinese sales[62] and later admitted that he had never seen as fast a decline in an emerging market as the drop in China in late 2013.[63] These numbers were also released *before* documents in May 2014 revealed that the NSA's Tailored Access Operations unit had intercepted network gear—including Cisco routers—being shipped to target organizations in order to covertly install implant firmware on them before they were delivered.[64] In response, Chambers wrote in a letter to the Obama Administration that "if these allegations are true, these actions will undermine confidence in our industry and in the ability of technology companies to deliver products globally."[65]

Much like Cisco, Qualcomm, IBM, Microsoft, and Hewlett-Packard all reported in late 2013 that sales were down in China as a result of the NSA revelations.[66] Sanford C. Bernstein analyst Toni Sacconaghi has predicted that after the NSA revelations, "US technology companies face the most revenue risk in China by a wide margin, followed by Brazil and other emerging markets."[67] Industry observers have also questioned whether companies like Apple—which hopes to bring in significant revenue from iPhone sales in China—will feel the impact overseas.[68] Even AT&T reportedly faced intense scrutiny regarding its proposed acquisition of Vodafone, a European wireless carrier, after journalists revealed the extent of AT&T's collaboration with the NSA.[69]

American companies are also losing out on business opportunities and contracts with large companies and foreign governments as a result of NSA spying. According to an article in *The New York Times*, "American businesses are being left off some requests for proposals from foreign customers that previously would have included them."[70] This refers to German companies, for example, that are increasingly uncomfortable giving their business to American firms. Meanwhile, the German government plans to change its procurement rules to prevent American companies that cooperate with the NSA or other intelligence organizations from being awarded federal IT contracts.[71] The government has already announced it intends to end its contract with Verizon, which provides Internet service to a number of government departments.[72] "There are indications that Verizon is legally required to provide certain things to the NSA, and that's one of the reasons the cooperation with Verizon won't continue," a spokesman for the German Interior Ministry told the Associated Press in June.[73]

The NSA disclosures have similarly been blamed for Brazil's December 2013 decision to award a $4.5 billion contract to Saab over Boeing, an American company that had previously been the frontrunner in a deal to replace Brazil's fleet of fighter jets.[74] Welber Barral, a former Brazilian trade secretary, suggested to *Bloomberg News* that Boeing would have won the contract a year earlier,[75] while a source in the Brazilian government told Reuters that "the NSA problem ruined it for the Americans."[76] As we will discuss in greater depth in the next section, Germany and Brazil are also considering data localization proposals that could harm U.S. business interests and prevent American companies from entering into new markets because of high compliance costs.

Outside of the cloud computing industry, it is still too early to tell which of these shifts may be temporary and which will have a more lasting impact. Despite an interest in finding alternatives, foreign companies and governments are also discovering the challenges of avoiding U.S. businesses altogether—either because of path dependence, because switching costs are too high, or because there simply are not enough alternative providers in certain markets that offer comparable products at the same prices.[77] This is particularly true for large government deals and enterprise solutions, markets that many American businesses dominate, because of the amount of time, money, and effort it would take to move away from U.S. companies. Some have cynically argued that the biggest "winners" in the long run will be Chinese companies like Huawei, which are also vulnerable to state eavesdropping but may be cheaper than the American alternatives.[78]

> **"If these allegations [about the NSA tampering with foreign-bound routers] are true, these actions will undermine confidence in our industry and in the ability of technology companies to deliver products globally."**
>
> -John Chambers, CEO of Cisco, in a letter to the Obama Administration

Cost to Public Trust in American Companies

The pressure is increasing on American companies to respond to the revelations in order to mitigate potential backlash and prevent foreign companies from poaching their business. According to the R Street Institute study, "It appears the NSA's aggressive surveillance has created an overall fear among U.S. companies that there is 'guilt by association' from which they need to proactively distance themselves."[79] Some companies have tried to regain trust by publicly stating that they are not part of PRISM or other NSA programs, issuing disclaimers along the lines of those published by Amazon and Salesforce in June 2013.[80] Others that have been directly linked to the NSA programs have publicly criticized the American government and called for greater transparency in order to rebuild user confidence and counteract potential economic harms.[81] To that end, nine major American companies—AOL, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo—joined together in the "Reform Government Surveillance" campaign in January 2014, where they launched a website and wrote an open letter to government leaders laying out principles for surveillance reform, including an end to bulk collection and opposition to data localization requirements.[82] Since the launch, the coalition has urged reform on Capitol Hill through outreach and letters to Congress, supported the February 2014 "The Day We Fight Back" activist campaign, and hired a lobbyist to bolster their efforts to curb the NSA's reach.[83] This unlikely, public partnership of some of Internet's biggest rivals speaks to the seriousness of the threats to their collective business interests.[84] Indeed, according to an April 2014 Harris poll commissioned by a data security company, nearly half of the 2,000 respondents (47 percent) have changed their online behavior since the NSA leaks, paying closer attention not only to the sites they visit but also to what they say and do on the Internet.[85] In particular, 26 percent indicated that they are now doing less online shopping and banking since learning the extent of government surveillance programs. Clearly, there are significant financial incentives for companies to distance themselves from the programs, and as a result, they are expending capital—actual and political—to do so.

Other companies have taken it a step further, developing new products or taking additional precautions to assure customers that their data is safe from the NSA. "Many tech companies feel

they have no choice but to try to develop NSA-resistant products because customers from China to Germany threaten to boycott American hardware and cloud services they view as compromised," wrote *USA Today* in February 2014.[86] Companies like Yahoo and Google have devoted increased resources to hardening their systems against NSA surveillance in order to assure users that their data is adequately protected.[87] Yahoo implemented automatic encryption on its email service in January 2014, and in March 2014 began encrypting all traffic that moved between its data centers, as well as queries on its homepage and its messaging service.[88] Google's Vice President for Security Engineering, Eric Grosse, referred to efforts to protect users' data from government surveillance as "an arms race," when discussing the company's move last fall to encrypt all information travelling between its data centers.[89] In June 2014, Google unveiled a source code extension for the Chrome browser called "End-to-End" which is designed to make email encryption easy, and announced a new section of its transparency report called "Safer Email" which details the percentage of email that is encrypted in transit and identifies the providers who support encryption.[90] These changes are part of a new focus on encouraging users and companies to harden their systems against NSA surveillance, and the strategy appears to be working. Almost immediately, Comcast announced its plans to work with Google to encrypt all email traffic exchanged with Gmail after the cable company was described as one of the worst offenders in the new report.[91]

> **"Many tech companies feel they have no choice but to try to develop NSA-resistant products because customers from China to Germany threaten to boycott American hardware and cloud services they view as compromised."**
>
> -*USA Today,* February 2014

Meanwhile, Microsoft has been publicizing its policy that allows customers to store their data in Microsoft data centers in specific countries.[92] John E. Frank, deputy general counsel at Microsoft, told *The New York Times*, "We're hearing from customers, especially global enterprise customers, that they care more than ever about where their content is stored and how it is used and secured."[93] IBM is reportedly spending over a billion dollars to build overseas data centers in an effort to reassure foreign customers that their data is protected from U.S. surveillance.[94] In reference to foreign customers asking about whether their data is protected from government snooping, an IBM executive said, "My response is protect your data against any third party — whether it's the NSA, other governments, hackers, terrorists, whatever," adding that it is time to "start talking about encryption and VPNs and all the ways you can protect yourself."[95]

SURVEILLANCE COSTS?

According to an April 2014 Harris poll of 2000 people:

- 47 percent of the respondents said that they have changed their online behavior since the NSA leaks, paying closer attention not only to the sites they visit but also to what they say and do on the Internet.
- 26 percent of respondents indicated that they are now doing less online shopping and banking since learning the extent of government surveillance programs.

Finally, faced with an impossible choice between maintaining user trust and complying with government requests, a handful of American companies that provide secure email services have had to shut down their operations altogether. Lavabit, a secure email service provider that experienced a 1,900 percent increase in account registrations after the Snowden revelations, shuttered its business after it became clear that user data could not be protected from government surveillance. When the NSA could not read Lavibit's communications directly by breaking its encryption, the agency obtained orders compelling the company to hand over information related to its encryption keys, which would have given the NSA the ability to decrypt the communications of all 400,000 of Lavabit's customers.[96] Silent Circle, a secure

communications provider that saw a 400 percent revenue increase following the Snowden revelations, followed Lavabit's lead and shut down its secure mail service, explaining that the decision was made because "we see the writing on the wall."[97]

It is abundantly clear that the NSA surveillance programs are currently having a serious, negative impact on the U.S. economy and threatening the future competitiveness of American technology companies. Not only are U.S. companies losing overseas sales and getting dropped from contracts with foreign companies and governments—they are also watching their competitive advantage in fast-growing industries like cloud computing and webhosting disappear, opening the door for foreign companies who claim to offer "more secure" alternative products to poach their business. Industry efforts to increase transparency and accountability as well as concrete steps to promote better security by adopting encryption and other best practices are positive signs, but U.S. companies cannot solve this problem alone. "It's not blowing over," said Microsoft General Counsel Brad Smith at a recent conference. "In June of 2014, it is clear it is getting worse, not better."[98] Without meaningful government reform and better oversight, concerns about the breadth of NSA surveillance could lead to permanent shifts in the global technology market and do lasting damage to the U.S. economy.

> **"It's not blowing over... In June of 2014, it is clear it is getting worse, not better."**
>
> -Brad Smith,
> Microsoft General Counsel

III. Economic and Technological Costs of Data Localization and Protection

The NSA disclosures have prompted some foreign leaders to propose new policies for data localization and data protection that could have serious ramifications for the Internet ecosystem. In the name of strengthening privacy and security, many of these changes could hurt American tech companies, impact the future growth of the network as a whole, and endanger human rights and Internet Freedom.[99] In particular, proposals that would require data localization or strengthen data protection laws could fundamentally alter the way traffic flows over the Internet and create significant additional compliance costs for American technology companies operating overseas. Major economic powers such as Germany, Brazil, and India have discussed requiring that all Internet traffic be routed or stored locally. Various leaders in these countries have also urged government agencies and their citizens to stop using American tools altogether because of concerns about backdoors or other arrangements with the NSA.[100] Meanwhile, legislators in the European Union have passed strict new data protection rules for the continent and considered various privacy-focused proposals, including the development of "national clouds" and the suspension of key trade agreements with the United States.[101] "The vast scale of online surveillance revealed by Edward Snowden is leading to the breakup of the Internet as countries scramble to protect privacy or commercially sensitive emails and phone records from UK and US security services," reported *The Guardian* in November 2013.[102] In combination, these various proposals could threaten the Internet economy while endangering privacy and free expression.

> **"The vast scale of online surveillance revealed by Edward Snowden is leading to the breakup of the Internet as countries scramble to protect privacy or commercially sensitive emails and phone records from UK and US security services."**
>
> -*The Guardian,* November 2013

Mandatory Data Localization and the Costs of a Bordered Internet

Internet jurisdiction and borders were contentious issues long before the Snowden leaks, but the debate has become significantly more complex in the past year. For decades, the borderless nature of cyberspace[103] has raised concerns about sovereignty and how governments can regulate and access their citizens' personal information or speech when it is stored on servers that may be located all over the world.[104] Various data localization and national routing proposals have been put forth by governments that seek greater control of the information that flows within their borders, often in order to make censorship and surveillance over the local population easier.[105] On the other side, free speech advocates, technologists, and civil society organizations generally advocate for a borderless cyberspace governed by its own set of internationally-agreed upon rules that promote the protection of human rights, individual privacy, and free expression.[106] The revelations about NSA surveillance have heightened concerns on both sides of this debate. But the disclosures appear to have given new ammunition to proponents of greater governmental control over traffic and network infrastructure, accelerating the number and scope of national control proposals from both long-time advocates as well as governments with relatively solid track records on human rights.[107]

There are now more than a dozen countries that have introduced or are actively discussing data localization laws.[108] Broadly speaking, data localization can be defined as any measures that "specifically encumber the transfer of data across national borders," through rules that prevent or limit these information flows.[109] The data localization proposals being considered post-Snowden generally require that foreign ICT companies

maintain infrastructure located within a country and store some or all of their data on that country's users on local servers.[110] Brazil, for example, has proposed that Internet companies like Facebook and Google must set up local data centers so that they are bound by Brazilian privacy laws.[111] The Indian government's draft policy would force companies to maintain part of their IT infrastructure in-country, give local authorities access to the encrypted data on their servers for criminal investigations, and prevent local data from being moved out of country.[112] Germany, Greece, Brunei, and Vietnam have also put forth their own data sovereignty proposals. Proponents argue that these policies would provide greater security and privacy protection because local servers and infrastructure can give governments both physical control and legal jurisdiction over the data being stored on them—although the policies may come with added political and economic benefits for those countries as well. "Home grown and guaranteed security in data storage, hardware manufacture, cloud computing services and routing are all part of a new discussion about 'technological sovereignty,'" write Mascolo and Scott. "It is both a political response and a marketing opportunity." [113] At the same time, data localization can also facilitate local censorship and surveillance, making it easier for governments to exert control over the Internet infrastructure.

Case Studies: Germany, India, and Brazil

Germany has been one of the most vocal critics of the U.S. surveillance dragnet in the past year, especially since evidence emerged that the NSA directly targeted the communications of German Chancellor Angela Merkel.[114] After the news broke in October 2013, Merkel was widely quoted about the loss of trust between Germany and the United States, reportedly telling lawmakers at a European Union leaders summit that they needed to discuss "what sort of data protection" and transparency rules should be implemented to address concerns about the NSA spying on German citizens.[115] In February 2014, she suggested that Europe should build out its own Internet infrastructure in order to keep data within the continent, arguing that "European providers [could] offer security for our citizens, so that one shouldn't have to send emails and other information across the Atlantic." [116] Meanwhile, German lawmakers had already been considering domestic data localization and protection proposals for months. In fact, data protection authorities in Germany announced stricter policies toward privacy violations involving countries outside of the EU shortly after the first leaks.[117] The sixteen German state data protection commissioners were also among the first to call for the suspension of the U.S.-EU Safe Harbor Program, which since the year 2000 has allowed the personal information of European citizens to be transferred to American companies who self-certify to the Commerce Department that they will follow EU data protection regulations.[118]

"Home grown and guaranteed security in data storage, hardware manufacture, cloud computing services and routing are all part of a new discussion about 'technological sovereignty.' It is both a political response and a marketing opportunity."

-Ben Scott and Georg Mascolo, *"Lessons from the Summer of Snowden"*

Since April, any company that cannot guarantee that they will protect data stored in Germany from foreign services or authorities will be excluded from contracts with the German federal government, a new rule which "seem[s] to be aimed primarily at American companies."[119] Hans-Peter Friedrich, the former German Minister of the Interior, also suggested that concerned German citizens should avoid using any Internet services that transmit data over U.S. networks.[120] And Deutsche Telekom, a major German telecommunications company in which the German government has a 32 percent ownership stake, has similarly promised to keep communications within the country to address the privacy concerns of German users.[121] Deutsche Telekom has been a vocal proponent of the idea of a "Schengen routing" network for data traveling between the 26 EU countries that have agreed to remove passport restrictions.[122] Regardless of whether these moves are public relations gambits or serious proposals, they nonetheless reflect the growing support

for 'email made in Germany' and other locally-controlled communications channels.[123] The German government's recent decision to drop its contract with Verizon has been described as a victory for Deutsche Telekom in particular.[124]

The government of India has also pushed for policies that require storage of all data within the country as well as ensure that it has local control and management of servers.[125] The Indian government has historically had an interest in data localization and has, for example, been engaged in a public dispute with Research in Motion (RIM) since the 2008 Mumbai terrorist attacks, primarily over requests for localized data storage and encryption keys in order to gain access to BlackBerry communications.[126] But proposals of this nature appear to have gained renewed traction since the NSA leaks began. According to reports from *The Hindu* newspaper in December 2013, an internal note prepared for the Sub-Committee on International Cooperation on Cyber Security under the Indian National Security Council Secretariat said: "We should insist that data of all domain names originating from India…should be stored in India. Similarly, all traffic originating/landing in India should be stored in India."[127] In essence, these proposals would prevent data on Indian citizens, government organizations, and businesses from being moved out of the country, forcing foreign companies to ensure that it was all stored on local servers.[128] The Indian National Security Advisor has requested that the Department of Telecommunications require Indian Internet providers and telecom companies to route all local data through the National Internet Exchange of India to keep domestic packets primarily within the country.[129] In October 2013, the Indian government also announced that it would be implementing an internal email policy to avoid relying on major American email service providers such as Gmail, Yahoo, and Outlook.com.[130] It has been reported that government workers were not only advised not to use Gmail, but also to avoid using computers altogether when typing up sensitive documents.[131]

Some of the most vocal response to the NSA revelations has come from Brazil.[132] In September 2013, Brazilian President Dilma Rousseff announced a number measures that her government planned to implement in order to better protect its citizens from NSA snooping. These proposals included increasing domestic Internet bandwidth and international Internet connectivity as well as encouraging domestic content production and the use of network equipment built in Brazil.[133] The government has announced its intent abandon Microsoft Outlook in favor of a domestic email system that relies on data centers located only in Brazil.[134] Rousseff's government has also been one of the most outspoken proponents of the idea that Internet traffic should be routed and stored locally to provide greater privacy protections.[135] "There is a serious problem of storage databases abroad," she said in early 2014. "That certain situation we will no longer accept."[136] In addition to maximizing the amount of data stored locally, Brazil is also seeking to minimize the amount of Brazilians' data that traverses the U.S. In February 2014, Brazil announced plans to build its own undersea cables so that data can travel between Brazil and the European Union without going through the United States. It has contracted with Brazilian and Spanish companies to lay fiber optic cables that will connect Brazil and Portugal directly.[137] Additional fiber optic cables such as this one can improve routing efficiency and speeds, but only if they come without routing restrictions.[138]

It remains unclear whether any of these data localization proposals are actually viable in the short term. In many of these countries, domestic markets may not yet be developed enough to support such a shift. The German government has begun backing away from proposals for "Schengen routing" and a German cloud, questioning their efficacy. As Neelie Kroes, the European Commissioner for the Digital Agenda, told *Der Spiegel* in February, "It is not realistic to contain data within Europe. You cannot put up border controls. That would destroy the openness of the Internet."[139] In contrast to his predecessor, Thomas De Maiziere, the new German Interior Minister, has also questioned whether these proposals are realistic.[140]

Similarly, the Brazilian posture has softened in recent months, especially as Brazil shifted to a more moderate stance in the lead up to the NETMundial conference in April 2014 (which will be discussed in greater depth in Part IV).[141] The controversial proposal to add new language on a local data storage rule for foreign companies to the Marco Civil[142] was dropped from the bill in March 2014 before the legislation passed.[143] Yet another provision that remained in the legislation requires that Brazilian law be extended to any Internet service in the world that has Brazilian users, which means that a U.S. based firm with Brazilian customers could be penalized for complying with domestic data laws if they conflict with Brazil law.[144] Brazil's Minister

> **"You cannot put up border controls. That would destroy the openness of the Internet."**
>
> -Neelie Kroes, European Commissioner for the Digital Agenda

of Communications, Paulo Bernardo, was also quoted in Brazil's largest newspaper saying that the government had not completely given up on the desire to pursue local data storage requirements despite the removal of the clause from the Marco Civil.[145]

Moreover, while the recent developments may temper short-term concerns, they could also set the stage for more troubling changes in the long run. Until recently, most foreign countries have accepted the fact that the U.S. has a comparative advantage in the technology industry that is extremely difficult to challenge. In a number of cases, however, the threat of NSA surveillance may be the catalyst that forces countries to invest heavily in markets that they would otherwise have left to the U.S., including cloud computing and data storage—a shift that will be worth huge amounts of money over time.[146] There is some risk at the moment that the short-term logistical challenges of requiring data localization or turning away from U.S. companies will create a false sense of security among U.S. policymakers and business leaders, obscuring the fact that the United States will squander massive economic value in the long term if it fails to address issues raised by NSA surveillance.

Data Protection Proposals and Costs to European Trade Relations

In addition to requiring local data storage, a number of countries, particularly in the EU, are proposing stricter domestic privacy regulations to ensure that their citizens are better protected against NSA snooping, which could lead to increased transaction costs for American companies that need to comply with them. "The effect of these proposed EU rules could serious undermine the position of some U.S. firms… Business models aside, the rules if adopted may require U.S. firms to place their servers, and European citizen data they hold, permanently in Europe, potentially a prohibitively expensive—or technically unfeasible—requirement," writes Jonah Force Hill, a scholar at Harvard University's Belfer Center for Science and International Affairs.[147] In March 2014, members of the European Parliament passed the EU's much-debated Data Protection Regulation and Directive by an enormous margin.[148] The rules impose strict limitations on what can be done with the data of EU citizens. Individuals would have to explicitly consent to having their personal data processed—and would retain the right to withdraw their consent if given. They would also be able to request their personal data from anyone who holds it and have it erased.[149] The new rules apply to the processing of EU citizens' data no matter where that data is located, ensuring that personal information from Europe is still protected by EU laws when it travels elsewhere, especially to the United States.[150] And the deterrent fines are significant, with a maximum penalty of up to five percent of revenues for non-compliance. That could translate to billions of dollars for large tech companies.

The new rules build upon the principles established in Europe's 1995 Data Protection Directive with updates that reflect the modern Internet ecosystem. After the regulation passed, the European Commissioner for Justice, Fundamental Rights and Citizenship, Viviane Reding, declared that the rules both preserve fundamental European values and offer a competitive opportunity for Europe to distinguish itself after the NSA revelations. "Data Protection is made in Europe. Strong data protection rules must be Europe's trade mark," she said. "Following the U.S. data spying scandals, data protection is more than ever a competitive advantage."[151]

The NSA disclosures also threaten to upset existing U.S.-EU trade relationships. On the same day that the Data Protection Regulation and Directive passed, members of the European Parliament voted in favor of a resolution from the Civil Liberties, Justice and Home Affairs Committee on the mass surveillance of EU citizens.[152] Among other things, the resolution called for the suspension of the U.S.-EU "Safe Harbor" deal that lets American firms self-certify via the Commerce Department that they are in compliance with EU privacy laws. The actual authority to suspend the Safe Harbor agreement lies in the hands of the European Commission, but the Parliament's affirmative vote heightens concerns that restrictive proposals could move

> **"Data Protection is made in Europe. Strong data protection rules must be Europe's trade mark... Following the U.S. data spying scandals, data protection is more than ever a competitive advantage."**
>
> -Viviane Reding, European Commissioner for Justice, Fundamental Rights, and Citizenship

forward, which would directly threaten U.S. business interests. Over 3,000 American companies, including Facebook and Google, currently rely on the Safe Harbor framework to process data from European citizens without violating the continent's privacy laws.[153] Yet both local and pan-European officials have become increasingly concerned that the Safe Harbor makes it easier for U.S. tech companies to sidestep the EU's stricter privacy protections, especially in light of revelations about the companies' compliance with the U.S. government under a number of the NSA programs. In June 2014, for example, the Irish courts referred a case to the European Court of Justice "questioning the adequacy of privacy protections for data transfers" under the Safe Harbor agreement.[154] The Parliament's resolution also calls for the European Parliament to withhold consent for the final Transatlantic Trade and Investment Partnership (TTIP) and suspend the Terrorist Finance Tracking Program (TFTP) until the U.S. makes various related concessions.[155]

Even though additional steps are still required before implementation, these actions are part of a meaningful shift in EU policy away from the previously favorable digital trade relationship it has enjoyed with the United States. The final agreement on the Data Protection Regulation and Directive is expected in 2015 as the European Parliament enters negotiations with the European Commission and the Council of Ministers (representing the member countries) over the final version of the legislation.[156] The demands in the resolution on mass surveillance, which represent the opinion of the members of Parliament, would need to be actively taken up by the European Commission to move forward. Minister Reding has also publicly stated that she wants to see "the development of European clouds" which meet new, stricter European privacy standards, arguing that European governments can promote this "by making sure that data processed by them are only stored in clouds to which E.U. data protection laws and European jurisdiction applies."[157] In June 2014, she further asserted that "EU data protection law will apply to non-European companies if they do business in our territory."[158] The challenge, of course, is that since U.S. law has traditionally given law enforcement and intelligence agencies a legal right to demand data from U.S. companies even if it is stored overseas, it creates a potentially significant contradiction with EU rules as well as with attempts by U.S. tech companies like Microsoft to reassure customers that their data is secure by offering the option to store that data outside the U.S.[159]

The Combined Costs of Data Localization and Data Protection Proposals

Some analysts have questioned whether data localization and protection proposals are politically motivated and if they would actually enhance privacy and security for ordinary individuals living in foreign countries,[160] especially given the existence of similar laws in a number of countries and Mutual Legal Assistance Treaties (MLATs) between nations that provide cross-border access to data stored for lawful investigations.[161] Yet there is no doubt that American companies will pay a steep price if these policies move forward. Mandatory data localization laws could lead to soaring costs for major Internet companies such as Google, Facebook, and Twitter, who would be faced with the choice of investing in additional, duplicative infrastructure and data centers in order to comply with new regulations or pulling their business out of the market altogether.[162] In testimony before Congress last November, for example, Google's Director of Law Enforcement and Information Security suggested that requirements being discussed in Brazil could be so onerous that they would effectively bar Google from doing business in the country.[163] The penalties that companies face for violating these new rules are also significant. In some cases, unless U.S. policy changes, it may be virtually impossible for American companies to avoid violating either domestic or foreign laws when operating overseas.[164] The costs and legal challenges could easily prevent firms from expanding in the first

place or cause them to leave existing markets because they are no longer profitable.[165] ITIF's Daniel Castro has suggested that data privacy rules and other restrictions could slow the growth of the U.S. technology-services industry by as much as four percent.[166]

"Ironically, data localization policies will likely degrade – rather than improve – data security for the countries considering them, making surveillance, protection from which is the ostensible reason for localization, easier for domestic governments, if not foreign powers, to achieve."

-Jonah Force Hill, *"The Growth of Data Localization Post-Snowden"*

Data localization proposals also threaten to undermine the functioning of the Internet, which was built on protocols that send packets over the fastest and most efficient route possible, regardless of physical location. If actually implemented, policies like those suggested by India and Brazil would subvert those protocols by altering the way Internet traffic is routed in order to exert more national control over data.[167] The localization of Internet traffic may also have significant ancillary impacts on privacy and human rights by making it easier for countries to engage in national surveillance, censorship, and persecution of online dissidents, particularly where countries have a history of violating human rights and ignoring rule of law.[168] "Ironically, data localization policies will likely degrade – rather than improve – data security for the countries considering them, making surveillance, protection from which is the ostensible reason for localization, easier for domestic governments, if not foreign powers, to achieve," writes Jonah Force Hill.[169] The rise in data localization and data protection proposals in response to NSA surveillance threatens not only U.S. economic interests, but also Internet Freedom around the world.

IV. Political Costs to U.S. Foreign Policy

Mandatory data localization proposals are just one of a number of ways that foreign governments have reacted to NSA surveillance in a manner that threatens U.S. foreign policy interests, particularly with regard to Internet Freedom. There has been a quiet tension between how the U.S. approaches freedom of expression online in its foreign policy and its domestic laws ever since Secretary of State Hillary Clinton effectively launched the Internet Freedom agenda in January 2010.[170] But the NSA disclosures shined a bright spotlight on the contradiction: the U.S. government promotes free expression abroad and aims to prevent repressive governments from monitoring and censoring their citizens while simultaneously supporting domestic laws that authorize surveillance and bulk data collection. As cybersecurity expert and Internet governance scholar Ron Deibert wrote a few days after the first revelations: "There are unintended consequences of the NSA scandal that will undermine U.S. foreign policy interests – in particular, the 'Internet Freedom' agenda espoused by the U.S. State Department and its allies."[171] Deibert accurately predicted that the news would trigger reactions from both policymakers and ordinary citizens abroad, who would begin to question their dependence on American technologies and the hidden motivations behind the United States' promotion of Internet Freedom. In some countries, the scandal would be used as an excuse to revive dormant debates about dropping American companies from official contracts, score political points at the expense of the United States, and even justify local monitoring and surveillance. Deibert's speculation has so far proven quite prescient. As we will describe in this section, the ongoing revelations have done significant damage to the credibility of the U.S. Internet Freedom agenda and further jeopardized the United States' position in the global Internet governance debates.

> **"There are unintended consequences of the NSA scandal that will undermine U.S. foreign policy interests – in particular, the 'Internet Freedom' agenda espoused by the U.S. State Department and its allies."**
>
> -Ron Deibert,
> *"Why NSA Spying Scares the World"*

Moreover, the repercussions from NSA spying have bled over from the Internet policy realm to impact broader U.S. foreign policy goals and relationships with government officials and a range of other important stakeholders abroad. In an essay entitled, "The End of Hypocrisy: American Foreign Policy in the Age of Leaks," international relations scholars Henry Farrell and Martha Finnemore argue that a critical, lasting impact of information provided by leakers like Edward Snowden is "the documented confirmation they provide of what the United States is actually doing and why. When these deeds turn out to clash with the government's public rhetoric, as they so often do, it becomes harder for U.S. allies to overlook Washington's covert behavior and easier for U.S. adversaries to justify their own."[172] Toward the end of the essay, Farrell and Finnemore suggest, "The U.S. government, its friends, and its foes can no longer plausibly deny the dark side of U.S. foreign policy and will have to address it head-on." Indeed, the U.S. is currently working to repair damaged bilateral and multilateral relations with countries from Germany and France to Russia and Israel,[173] and it is likely that the effects of the NSA disclosures will be felt for years in fields far beyond Internet policy.[174]

Costs to the Internet Freedom Agenda and U.S. Credibility in Internet Governance

"As the birthplace for so many of these technologies, including the internet itself, we have a responsibility to see them used for good," declared Secretary of State Hillary Clinton in January 2010.[175] Her speech at the Newseum in Washington DC effectively launched the United States' Internet Freedom agenda, articulating a leading role for the U.S. in using the Internet

> **"The U.S. government, its friends, and its foes can no longer plausibly deny the dark side of U.S. foreign policy and will have to address it head-on."**
>
> -Henry Farrell and Martha Finnemore, *"The End of Hypocrisy: American Foreign Policy in an Age of Leaks"*

to promote freedom of expression, freedom of worship, and the freedom to connect around the world. Clinton went on to give two other major addresses on Internet Freedom, becoming the first global leader to emphasize Internet Freedom as a foreign policy priority and urging "countries everywhere... to join us in the bet we have made, a bet that an open internet will lead to stronger, more prosperous countries."[176] As Richard Fontaine and Will Rogers describe in a seminal paper on the subject in June 2011, "Internet Freedom, broadly defined, is the notion that universal rights, including the freedoms of expression, assembly and association, extend to the digital sphere."[177]

Although there were questions from the beginning about whether the United States would hold itself to the same high standards domestically that it holds others to internationally,[178] the American government has successfully built up a policy and programming agenda in the past few years based on promoting an open Internet.[179] These efforts include raising concerns over Internet repression in bilateral dialogues with countries such as Vietnam and China,[180] supporting initiatives including the Freedom Online Coalition, and providing over $120 million in funding for "groups working to advance Internet freedom – supporting counter-censorship and secure communications technology, digital safety training, and policy and research programs for people facing Internet repression."[181] However, the legitimacy of these efforts has been thrown into question since the NSA disclosures began. "Trust has been the principal casualty in this unfortunate affair," wrote Ben FitzGerald and Richard Butler in December 2013. "The American public, our nation's allies, leading businesses and Internet users around the world are losing faith in the U.S. government's role as the leading proponent of a free, open and integrated global Internet."[182]

Prior to the NSA revelations, the United States was already facing an increasingly challenging political climate as it promoted the Internet Freedom agenda in global Internet governance conversations. At the 2012 World Conference on International Telecommunications (WCIT), the U.S. and diverse group of other countries refused to sign the updated International Telecommunications Regulations based on concerns that the document pushed for greater governmental control of the Internet and would ultimately harm Internet Freedom.[183] Many observers noted that the split hardened the division between two opposing camps in the Internet governance debate: proponents of a status quo multistakeholder Internet governance model, like the United States, who argued that the existing system was the best way to preserve key online freedoms, and those seeking to disrupt or challenge that multistakeholder model for a variety of political and economic reasons, including governments like Russia and China pushing for greater national sovereignty over the Internet.[184] Many of the proposals for more governmental control over the network could be understood as attempts by authoritarian countries to more effectively monitor and censor their citizens, which allowed the U.S. to reasonably maintain some moral high ground as its delegates walked out of the treaty conference.[185] Although few stakeholders seemed particularly pleased by the outcome of the WCIT, reports indicate that by the middle of 2013 the tone had shifted in a more collaborative and positive direction following the meetings of the 2013 World Telecommunications/ICT Policy Forum (WTPF) and the World Summit on Information Society + 10 (WSIS+10) review.[186]

However, the Internet governance conversation took a dramatic turn after the Snowden disclosures. The annual meeting of the Freedom Online Coalition occurred in Tunis in June 2013, just a few weeks after the initial leaks. Unsurprisingly, surveillance dominated the conference even though the agenda covered a wide range of topics from Internet access and affordability to cybersecurity.[187] Throughout the two-day event, representatives from civil society used the platform to confront and criticize governments about their monitoring practices.[188] NSA surveillance would continue to be the focus of international convenings on Internet Freedom and Internet governance for months to come, making civil society representatives and foreign governments far less willing to embrace the United States' Internet Freedom agenda or to accept its defense of the

> **"Trust has been the principle casualty of this unfortunate affair. The American public, our nation's allies, leading businesses and Internet users around the world are losing faith in the U.S. government's role as the leading proponent of a free, open and integrated global Internet."**
>
> -Ben FitzGerald and Richard Butler, *"NSA Revelations: Fallout Can Serve Our Nation"*

multistakeholder model of Internet governance as a anything other than self-serving. "One can come up with all kinds of excuses for why US surveillance is not hypocrisy. For example, one might argue that US policies are more benevolent than those of many other regimes... And one might recognize that in several cases, some branches of government don't know what other branches are doing... and therefore US policy is not so much hypocritical as it is inadvertently contradictory," wrote Eli Dourado, a researcher from the Mercatus Center at George Mason University in August 2013. "But the fact is that the NSA is galvanizing opposition to America's internet freedom agenda."[189] The scandal revived proposals from both Russia and Brazil for global management of technical standards and domain names, whether through the ITU or other avenues. Even developing countries, many of whom have traditionally aligned with the U.S. and prioritize access and affordability as top issues, "don't want US assistance because they assume the equipment comes with a backdoor for the NSA. They are walking straight into the arms of Russia, China, and the ITU."[190]

Consequently, NSA surveillance has shifted the dynamics of the Internet governance debate in a potentially destabilizing manner. The Snowden revelations "have also been well-received by those who seek to discredit existing approaches to Internet governance," wrote the Center for Democracy & Technology's Matthew Shears. "There has been a long-running antipathy among a number of stakeholders to the United States government's perceived control of the Internet and the dominance of US Internet companies. There has also been a long-running antipathy, particularly among some governments, to the distributed and open management of the Internet."[191] Shears points out that evidence of the NSA's wide-ranging capabilities has fueled general concerns about the current Internet governance system, bolstering the arguments of those calling for a new government-centric governance order. At the UN Human Rights Council in September 2013, the representative from Pakistan—speaking on behalf of Cuba, Venezuela, Zimbabwe, Uganda, Ecuador, Russia, Indonesia, Bolivia, Iran, and China—explicitly linked the revelations about surveillance programs to the need for reforming Internet governance processes and institutions to give governments a larger role.[192] Surveillance issues continued to dominate the conversation at the 2013 Internet Governance Forum in Bali as well, where "debates on child protection, education and infrastructure were overshadowed by widespread concerns from delegates who said the public's trust in the internet was being undermined by reports of US and British government surveillance."[193]

Further complicating these conversations is the fact that several of the institutions that govern the technical functions of the Internet are either tied to the American government or are located in the United States. Internet governance scholar Milton Mueller has described how the reaction to the NSA disclosures has become entangled in an already contentious Internet governance landscape. Mueller argues that, in addition to revealing the scale and scope of state surveillance and the preeminent role of the United States and its partners, the NSA disclosures may push other states toward a more nationally partitioned Internet and "threaten... in a very fundamental way the claim that the US had a special status as neutral steward of Internet governance."[194] These concerns were publicly voiced in October 2013 by the heads of a number of key organizations, including the President of the Internet Corporation for Assigned Names and Numbers (ICANN) and the chair of the Internet Engineering Task Force (IETF), in the Montevideo Statement on the Future of Internet Cooperation. Their statement expressed "strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance" and "called for accelerating the globalization of ICANN and Internet Assigned Numbers Authority (IANA) functions, towards an environment in which all stakeholders, including

all governments, participate on an equal footing."[195] In particular, the process of internationalizing ICANN—which has had a contractual relationship with the Commerce Department's National Telecommunications and Information Association (NTIA) since 1998—has progressed in recent months.[196]

There have been positive signs that the U.S. is taking steps to rebuild its credibility in the Internet governance debates and restore some of the goodwill that was previously associated with the Internet Freedom agenda. In parallel to the process of ICANN internationalization, the NTIA announced in March, that it does not intend to renew its contract with ICANN when it expires in 2015.[197] The NTIA's decision to voluntarily transfer oversight of the IANA functions to a multistakeholder body demonstrates that it is willing to fulfill longstanding commitments to the Internet governance community rather than fighting to maintain the status quo, as the U.S. has sometimes done in the past.[198] In a speech earlier that month, Scott Busby, the Deputy Assistant Secretary for Democracy, Human Rights & Labor at the State Department, also identified six principles to guide U.S. signals intelligence with respect for human rights: rule of law, legitimate purpose, non-arbitrariness, competent authority, oversight, transparency, and democratic accountability.[199] Although the speech contained few details on how such policies would be implemented going forward, Busby's remarks indicated that the U.S. believes that international human rights norms should apply to surveillance.[200] The language also echoed several of the thirteen "International Principles on the Application of Human Rights to Communications Surveillance" that were put forth by a coalition of civil society groups, technology and privacy experts in July 2013[201] and incorporated into a speech by Swedish Foreign Minister Carl Bildt in October 2013.[202]

> **"One can come up with all kinds of excuses for why US surveillance is not hypocrisy... But the fact is that the NSA is galvanizing opposition to America's internet freedom agenda."**
>
> -Eli Dourado, *"So much for America's internet freedom agenda"*

Costs to Internet Freedom Beyond Internet Governance

The effects of the NSA disclosures on the Internet Freedom agenda go beyond the realm of Internet governance. The loss of the United States as a model on Internet Freedom issues has made it harder for local civil society groups around the world—including the groups that the State Department's Internet Freedom programs typically support[203]—to advocate for Internet Freedom within their own governments.[204] The Committee to Protect Journalists, for example, reports that in Pakistan, "where freedom of expression is largely perceived as a Western notion, the Snowden revelations have had a damaging effect. The deeply polarized narrative has become starker as the corridors of power push back on attempts to curb government surveillance."[205] For some of these groups, in fact, even the appearance of collaboration with or support from the U.S. government can diminish credibility, making it harder for them to achieve local goals that align with U.S. foreign policy interests.[206] The gap in trust is particularly significant for individuals and organizations that receive funding from the U.S. government for free expression activities or circumvention tools. Technology supported by or exported from the United States is, in some cases, inherently suspect due to the revelations about the NSA's surveillance dragnet and the agency's attempts to covertly influence product development.

Moreover, revelations of what the NSA has been doing in the past decade are eroding the moral high ground that the United States has often relied upon when putting public pressure on authoritarian countries like China, Russia, and Iran to change their behavior. In 2014, Reporters Without Borders added the United States to its "Enemies of the Internet" list for the first time, explicitly linking the inclusion to NSA surveillance. "The main player in [the United States'] vast surveillance operation is the highly secretive National Security Agency (NSA) which, in the light of Snowden's revelations, has come to symbolize the abuses by the world's intelligence agencies," noted the 2014 report.[207] The damaged perception of the United States[208] as a leader on Internet Freedom and its diminished ability to legitimately criticize other countries for censorship and surveillance opens the door

for foreign leaders to justify—and even expand—their own efforts.[209] For example, the Egyptian government recently announced plans to monitor social media for potential terrorist activity, prompting backlash from a number of advocates for free expression and privacy.[210] When a spokesman for the Egyptian Interior Ministry, Abdel Fatah Uthman, appeared on television to explain the policy, one justification that he offered in response to privacy concerns was that "the US listens in to phone calls, and supervises anyone who could threaten its national security."[211] This type of rhetoric makes it difficult for the U.S. to effectively criticize such a policy. Similarly, India's comparatively mild response to allegations of NSA surveillance have been seen by some critics "as a reflection of India's own aspirations in the world of surveillance," a further indication that U.S. spying may now make it easier for foreign governments to quietly defend their own behavior.[212] It is even more difficult for the United States to credibly indict Chinese hackers for breaking into U.S. government and commercial targets without fear of retribution in light of the NSA revelations.[213] These challenges reflect an overall decline in U.S. soft power on free expression issues.

> **"[The Snowden revelations] have also been well-received by those who seek to discredit existing approaches to Internet governance."**
>
> -Matthew Shears, *"Snowden and the Politics of Internet Governance"*

Broader Foreign Policy Costs

Beyond Internet Freedom, the NSA disclosures "have badly undermined U.S. credibility with many of its allies," Ian Bremmer argued in *Foreign Policy* in November 2013.[214] Similarly, as Georg Mascolo and Ben Scott point out about the post-Snowden world, "the shift from an open secret to a published secret is a game changer... it exposes the gap between what governments will tolerate from one another under cover of darkness and what publics will tolerate from other governments in the light of day."[215] From stifled negotiations with close allies like France and Germany to more tense relations with emerging powers including Brazil and China, the leaks have undoubtedly weakened the American position in international relations, opening up the United States to new criticism and political maneuvering that would have been far less likely a year ago.[216]

U.S. allies like France, Israel, and Germany are upset by the NSA's actions, as their reactions to the disclosures make clear.[217] Early reports about close allies threatening to walk out of negotiations with the United States—such as calls by the French government to delay EU-U.S. trade talks in July 2013 until the U.S. government answered European questions about the spying allegations[218]—appear to be exaggerated, but there has certainly been fallout from the disclosures. For months after the first Snowden leaks, German Chancellor Angela Merkel would not visit the United States until the two countries signed a "no-spy" agreement—a document essentially requiring the NSA to respect German law and rights of German citizens in its activities. When Merkel finally agreed come to Washington, D.C. in May 2014, tensions rose quickly because the two countries were unable to reach an agreement on intelligence sharing, despite the outrage provoked by news that the NSA had monitored Merkel's own communications.[219] Even as Obama and Merkel attempted to present a unified front while they threatened additional sanctions against Russia over the crisis in the Ukraine, it was evident that relations are still strained between the two countries. While President Obama tried to keep up the appearance of cordial relations at a joint press conference, Merkel suggested that it was too soon to return to "business as usual" when tensions still remain over U.S. spying allegations.[220] *The Guardian* called the visit "frosty" and "awkward."[221] The German Parliament has also begun hearings to investigate the revelations and suggested that it is weighing further action against the United States.[222]

Moreover, the disclosures have weakened the United States' relationship with emerging powers like Brazil, where the fallout from NSA surveillance threatens to do more lasting damage. Brazilian President Dilma Rousseff has seized on the NSA disclosures as an opportunity to broaden Brazil's influence not only in the Internet governance field, but also on a broader range of geopolitical issues. Her decision not to attend an October 2013 meeting with President Barack Obama at the White House was a direct response to NSA spying—and a serious,

> **"The main player in [the United States'] vast surveillance operation is the highly secretive National Security Agency (NSA) which, in the light of Snowden's revelations, has come to symbolize the abuses by the world's intelligence agencies."**
>
> -Reporters Without Borders, 2014 "Enemies of the Internet" Report

high-profile snub. In addition to cancelling what would have been the first state visit by a Brazilian president to the White House in nearly 20 years, Rousseff's decision marked the first time a world leader had turned down a state dinner with the President of the United States.[223] In his statement on the postponement, President Obama was forced to address the issue of NSA surveillance directly, acknowledging "that he understands and regrets the concerns disclosures of alleged U.S. intelligence activities have generated in Brazil and made clear that he is committed to working together with President Rousseff and her government in diplomatic channels to move beyond this issue as a source of tension in our bilateral relationship."[224]

Many observers have noted that the Internet Freedom agenda could be one of the first casualties of the NSA disclosures. The U.S. government is fighting an uphill battle at the moment to regain credibility in international Internet governance debates and to defend its moral high ground as a critic of authoritarian regimes that limit freedom of expression and violate human rights online. Moreover, the fallout from the NSA's surveillance activities has spilled over into other areas of U.S. foreign policy and currently threatens bilateral relations with a number of key allies. Going forward, it is critical that decisions about U.S. spying are made in consideration of a broader set of interests so that they do not impede—or, in some cases, completely undermine—U.S. foreign policy goals.

V. Costs to Cybersecurity

We have previously focused on the economic and political repercussions of the NSA disclosures both in the United States and abroad. In this section, we consider the impact on the Internet itself and the ways in which the NSA has both weakened overall trust in the network and directly harmed the security of the Internet.

Certainly, the actions of the NSA have created a serious trust and credibility problem for the United States and its Internet industry. "All of this denying and lying results in us not trusting anything the NSA says, anything the president says about the NSA, or anything companies say about their involvement with the NSA," wrote security expert Bruce Schneier in September 2013.[225] However, beyond undermining faith in American government and business, a variety of the NSA's efforts have undermined trust in the security of the Internet itself. When Internet users transmit or store their information using the Internet, they believe—at least to a certain degree—that the information will be protected from unwanted third-party access. Indeed, the continued growth of the Internet as both an economic engine and an as avenue for private communication and free expression relies on that trust. Yet, as the scope of the NSA's surveillance dragnet and its negative impact on cybersecurity comes into greater focus, that trust in the Internet is eroding.[226]

Trust is essential for a healthy functioning society. As economist Joseph Stiglitz explains, "Trust is what makes contracts, plans and everyday transactions possible; it facilitates the democratic process, from voting to law creation, and is necessary for social stability."[227]

> **"All of this denying and lying results in us not trusting anything the NSA says, anything the president says about the NSA, or anything companies say about their involvement with the NSA."**
>
> -Bruce Schneier, *"The Only Way to Restore Trust in the NSA"*

Individuals rely on online systems and services for a growing number of sensitive activities, including online banking and social services, and they must be able to trust that the data they are transmitting is safe. In particular, trust and authentication are essential components of the protocols and standards engineers develop to create a safer and more secure Internet, including encryption.[228] The NSA's work to undermine the tools and standards that help ensure cybersecurity—especially its work to thwart encryption—also undermines trust in the safety of the overall network. Moreover, it reduces trust in the United States itself, which many now perceive as a nation that exploits vulnerabilities in the interest of its own security.[220] This loss of trust can have a chilling effect on the behavior of Internet users worldwide.[230] Unfortunately, as we detail below, the growing loss of trust in the security of Internet as a result of the latest disclosures is largely warranted. Based on the news stories of the past year, it appears that the Internet is far less secure than people thought—a direct result of the NSA's actions. These actions can be traced to a core contradiction in NSA's two key missions: information assurance—protecting America's and Americans' sensitive data—and signals intelligence—spying on telephone and electronic communications for foreign intelligence purposes.

In the Internet era, these two missions of the NSA are in obvious tension. The widespread adoption of encryption technology to secure Internet communications is considered one of the largest threats to the NSA's ability to carry out the goals of its signals intelligence mission. As the *National Journal* explained, "strong Internet security actually makes the NSA's job harder."[231] In the 1990s, the NSA lost the public policy battle to mandate that U.S. technology companies adopt a technology called the "Clipper Chip" that would give the government the ability to decrypt private communications,[232] and since then strong encryption technology has become a bedrock technology when it comes to the security of the Internet. The NSA lost that early battle against encryption, sometimes called the "Crypto War,"[233] not only due to vocal opposition from privacy and civil liberties stakeholders, but also because the private sector convinced policymakers that subverting the security of American communications technology products would undermine the U.S. technology industry and the growth of

the Internet economy as a whole.[234] However, as an explosive *New York Times* story first revealed in September 2013, the NSA has apparently continued to fight the "Crypto War" in secret, clandestinely inserting backdoors into secure products and working to weaken key encryption standards.[235] "For the past decade, N.S.A. has led an aggressive, multipronged effort to break widely used Internet encryption technologies," said a 2010 memo from the Government Communications Headquarters (GCHQ), the NSA's British counterpart. "Cryptanalytic capabilities are now coming online. Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable."[236]

"For the past decade, N.S.A. has led an aggressive, multipronged effort to break widely used Internet encryption technologies... Cryptanalytic capabilities are now coming online. Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable."

-British Government Communications Headquarters (GCHQ) Internal Memo

Given the amount of information the NSA is collecting, it is not surprising that the agency would also take aggressive steps to improve its ability to read that information. According to the "black budget" released by *The Washington Post* in August 2013, 21 percent of the intelligence budget (roughly $11 billion) goes toward the Consolidated Cryptologic Program, with a staff of 35,000 in the NSA and the armed forces' surveillance and code breaking units.[237] "The resources devoted to signals intercepts are extraordinary," wrote Barton Gellman and Greg Miller.[238] However, the agency has employed a variety of methods to achieve this goal far beyond simple code-breaking—methods that directly undermine U.S. cybersecurity, not just against the NSA, but also against foreign governments, organized crime, and other malicious actors. In this section, we consider four different ways that the NSA has damaged cybersecurity in pursuit of its signals intelligence goals: (1) by deliberately engineering weaknesses into widely-used encryption standards; (2) by inserting surveillance backdoors in widely-used software and hardware products; (3) by stockpiling information about security vulnerabilities for its own use rather than disclosing those vulnerabilities so that they can be remedied; and (4) by engaging in a wide variety of offensive hacking techniques to compromise the integrity of computer systems and networks around the world, including impersonating the web sites of major American companies like Facebook and LinkedIn.

Compromising Security Standards: How the NSA deliberately engineers weaknesses into widely-used encryption standards

Because of United States' critical role in the development of the Internet, U.S.-based organizations and government agencies have historically been central to standards setting and oversight of key Internet functions, particularly through the National Institute of Standards and Technology (NIST). NIST is the Commerce Department agency responsible for setting scientific and technical standards that both the government and the private sector rely upon.[239] As outlined in the 2002 Federal Information Security Management Act (FISMA), NIST has a statutory obligation to consult with the NSA on certain standards and guidelines "to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems."[240] The Snowden leaks revealed that the NSA took advantage of that position to influence the standards-setting process to weaken encryption standards to the agency's benefit. According to documents released by *The Guardian*, *The New York Times*, and *ProPublica* in September 2013, the NSA "worked covertly to get its own version of a draft security standard issued by the US National Institute of Standards and Technology approved for worldwide use in 2006."[241] This standard was later adopted by the International Organization for Standardization, a body with membership from countries all over the world. A number of experts suspected that the NSA had engineered a weakness in the standard that two Microsoft cryptographers discovered in 2007, and the classified memos released last year apparently confirm that this was the case. According to *The*

New York Times, "The N.S.A. wrote the standard and aggressively pushed it on the international group, privately calling the effort 'a challenge in finesse.'"[242]

A few days after details about the compromised standard were revealed by the press, RSA Security—an American network security company that publicly fought against the Clipper Chip in the 1990s[243]—privately alerted its customers that they should stop using an encryption algorithm that had been influenced by the NSA. Officials advised customers that one of the cryptography components in the BSAFE toolkit and Data Protection Manager by default used a specification known as Dual_EC_DRBG when generating keys.[244] Although NIST approved Dual_EC_DRBG in 2006, the Snowden documents revealed that the random number generator contained a vulnerability engineered by the NSA. According to the *Wall Street Journal*, the announcement marked one of the first times that a security company had acknowledged the U.S. government's involvement in direct tampering with a product in order to facilitate access.[245] The BSAFE library has been used in a number of products, including some versions of the McAfee Firewall Enterprise Control Center, and, according to *Ars Technica*, the backdoor "means that an untold number of third-party products may be bypassed not only by advanced intelligence agencies, but possibly by other adversaries who have the resources to carry out attacks that use specially designed hardware to quickly cycle through possible keys until the correct one is guessed."[246] Documents released a few months later, in December 2013, revealed that RSA had a secret $10 million contract with the NSA wherein the security company agreed to set the compromised standard as the default in a number of its BSAFE products.[247]

> **"The allegation that NSA has, or had, a program designed to insert weaknesses into global cryptographic standards… calls into question the integrity… of all the cryptographic standards developed by NIST."**
>
> -Ellen Richey,
> Executive Vice President of Visa

Many cryptographers and security researchers have been skeptical of the NIST process for years, although they are heavily reliant upon the organization for everything from random number generators to more complex functions.[248] While NIST has said it would never "deliberately weaken a cryptographic standard," it is unclear whether the agency was aware that the NSA was aggressively pushing for it to adopt a compromised standard.[249] Both NIST and the NSA issued statements after the stories broke in September 2013 defending the standard, although NIST's statement indicated that the agency would also evaluate its processes to ensure that they were open, transparent, and held to high professional standards.[250] Yet, it is clear that, at least in part as a result of the NSA's effort to exert its pervasive influence and perceived security expertise, NIST issued a compromised algorithm that was included for almost a decade in the cryptographic libraries of major tech companies, including Microsoft, Cisco, Symantec and RSA, because it was required for eligibility for government contracts.[251] "The impact of weakening a standard may be even greater than a weakening a specific product or service because that one standard may be used in so many different products and services," notes a recent report from the Institute of Electrical and Electronics Engineers in the U.S.[252] Although some have argued that the compromised algorithm was not widely-used, its presence in a number of products nonetheless diminishes America's reputation as a standards-setter, which is viewed as increasingly critical as foreign competition for products and software intensifies. Meddling with standards can undermine American industry, adding economic costs on top of security concerns.[253]

Weakening cryptographic standards demonstrably harms Internet security. It also hurts the credibility of NIST, which has been directed by President Obama to draft cybersecurity guidelines for critical infrastructure including telephone systems and power plants. "Suspicions of NSA intervention in NIST standards in support of the NSA intelligence mission have a negative effect on NIST's reputation and the credibility of the standards NIST develops… [T]hey also have a negative effect on the credibility of US industry that implements those standards and thus on international competitiveness," observed Microsoft's Steven B. Lipner.[254] Put simply, "NIST is operating with a trust deficit right now," said Chris Soghoian of the American Civil Liberties Union to the *National Journal*.[255] As part of an effort to begin rebuilding that trust, NIST announced in May 2014 that it would begin a

review of its cryptographic standards and guidelines program with the help of a panel of outside experts known as the Visiting Committee on Advanced Technology (VCAT).[256] In July 2014, the VCAT issued a report that examined the agency's processes and relationship with the NSA, outlining a series of recommendations to rebuild its credibility.[257] These recommendations included improving transparency and openness around NIST processes, increasing the technical staff at NIST, and clarifying NIST's relationship with the NSA.[258] As Ellen Richey, an Executive Vice President at Visa, Inc. and member of the VCAT, noted in her assessment, "The allegation that NSA has, or had, a program designed to insert weaknesses into global cryptographic standards… calls into question the integrity… of all the cryptographic standards developed by NIST," adding that, "Participants in the development process should understand that the risk from conflicts of interest arises from the appearance of impropriety, even in the absence of actual misconduct."[259]

With regard to redefining or clarifying NIST's statutory relationship to the NSA, parallel efforts are underway in Congress as well. In May 2014, the House Science and Technology Committee voted to adopt an amendment to the Frontiers in Innovation, Research, Science, and Technology (FIRST) Act offered by Representative Alan Grayson (D-FL) which would remove the requirement that the NSA be consulted on encryption standards, allowing NIST to request NSA assistance on an as-needed basis instead.[260] A similar amendment proposed by Representative Grayson that would prohibit the NSA from using appropriations funds to interfere with NIST's security standards was approved by the House in June 2014 as part of a defense appropriations bill.[261] However, it remains to be seen if such a measure will ultimately be passed into law.

Creating Security Vulnerabilities: How the NSA secretly inserts surveillance backdoors into widely-used hardware and software products

In addition to influencing standards-setting bodies, the NSA also goes straight to American and international tech companies to ensure that it can exploit vulnerabilities in their products. The NSA spends $250 million a year—more than 20 times what it spends on the much-discussed PRISM program—on a project to develop relationships with companies in order to weaken standards and convince them to insert backdoors into their products. According to documents released by *ProPublica*, the NSA's SIGINT Enabling Project "actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection."[262] The Fiscal Year 2013 budget documents indicate that the goals of the project include inserting vulnerabilities into commercial encryption systems, IT networks, and communications devices as well as making it easier to exploit next generation encryption used for 4G wireless networks. The documents reference "continued partnerships with major telecommunications carriers to shape the global network to benefit other collection accesses" and other relationships with commercial IT providers.[263] One of the goals for that year is to "shape the worldwide commercial cryptography marketplace to make it more tractable to advanced cryptanalytic capabilities being developed by NSA/CSS [Central Security Service]."[264] Programs like SIGINT Enabling are a central piece of the NSA's covert strategy to weaken commercial encryption, demonstrating how the agency switched from a public approach for a government mandate in the 1990s to developing a set of private partnerships with the tech industry over the past two decades. "Basically, the NSA asks companies to subtly change their products in undetectable ways: making the random number generator less random, leaking the key somehow, adding a common exponent to a public-key exchange protocol, and so on," explains Bruce Schneier. "If the back door is discovered, it's explained away as a mistake. And as we now know, the NSA has enjoyed enormous success from this program."[265]

Beyond SIGINT Enabling, the NSA appears to have other programs aimed at leveraging private sector relationships to insert and maintain vulnerabilities in commercial products as well. According to *The Guardian*, the NSA's Commercial Solutions center—the program which offers technology companies an opportunity to have their security products assessed and presented to prospective government buyers[266]—is also quietly used by the NSA to "leverage sensitive, co-operative relationships with specific industry partners" to insert vulnerabilities into those security tools.[267] Similarly, a general classification guide details

the relationships between industry partners and the NSA, as well as the agency's ability to modify commercial encryption software and devices to "make them exploitable" and obtain otherwise proprietary information about the nature of company's cryptographic systems.[268] Even before SIGINT Enabling was disclosed, *The Guardian* reported that the NSA worked with Microsoft directly to circumvent the encryption on popular services including Skype, Outlook, and SkyDrive,[269] although Microsoft denies those allegations.[270] New information has also come to light about backdoors planted in foreign-bound network routers from companies like Cisco, apparently without the knowledge of the companies that sell them.[271] Cisco CEO John Chambers also spoke out after the May 2014 revelations that the NSA had inserted backdoors into network routers, writing a letter to the Obama Administration asking it to curtail the NSA's surveillance activities and institute reforms that rein in its seemingly-unchecked power.[272] In a blog post, Cisco's Senior Vice President Mark Chandler wrote, "We comply with US laws... we ought to be able to count on the government to then not interfere with the lawful delivery of our products in the form in which we have manufactured them. To do otherwise, and to violate legitimate privacy rights of individuals and institutions around the world, undermines confidence in our industry."[273]

> **"We comply with US laws... we ought to be able to count on the government to then not interfere with the lawful delivery of our products in the form in which we have manufactured them."**
>
> -Mark Chandler,
> Cisco Senior Vice President

The existence of these programs, in addition to undermining confidence in the Internet industry, creates real security concerns. The SIGINT Enabling budget request suggests that the secrecy of the endeavor acts as a safeguard against any security concerns about the manufactured vulnerabilities, including an assurance that "to the consumer and other adversaries, however, the systems' security remains intact."[274] This assertion relies on the false assumption that if the program is not made public, then others will never discover or exploit those vulnerabilities—and that the program's benefits outweigh the cost.[275] Stephanie Pell, a non-resident fellow at the Center for Internet and Society at Stanford Law School and a former prosecutor at the Department of Justice, explains in a recent paper that "building in back door access...inevitably produces security vulnerabilities" because such back doors "create additional 'attack surfaces.'"[276] And as security researcher Dr. Susan Landau noted in testimony to Congress, "building wiretapping [capabilities] into communications infrastructure creates serious risk that the communications system will be subverted either by trusted insiders or skilled outsiders, including foreign governments, hackers, identity thieves and perpetrators of economic espionage.[277] Furthermore, creating a back door in an encrypted communications service requires access to the unencrypted data, which means that "if and when security flaws in the system are discovered and exploited, the worst case scenario will be unauthorized access to users' communications... [W]hen compromised, an encrypted communications system with a lawful interception back door is far more likely to result in the catastrophic loss of communications confidentiality than a system that never has access to the unencrypted communications of its users."[278]

The fact that only the NSA was supposed to know about these backdoors does not alleviate the concerns. Matthew Green, a cryptography researcher at Johns Hopkins University, warned in T*he New York Times* that "the risk is that when you build a back door into systems, you're not the only one to exploit it," since anyone else who discovers the weakness, including U.S. adversaries, can exploit it as well.[279] These risks are not theoretical; there are numerous examples where technologies intended to facilitate lawful intercepts of communications have created additional vulnerabilities and security holes that have been exploited by unauthorized actors.[280] As the white paper from the Institute of Electrical and Electronics Engineers concludes, "While the debate over how we should value both privacy and security is important, it misses a critical point: The United States might have compromised both security and privacy in a failed attempt to improve security."[281]

Withholding Security Vulnerabilities: How the NSA stockpiles information about software and hardware vulnerabilities rather than responsibly disclosing them to companies

In April 2014, *Bloomberg* reported that the NSA had known for at least two years about the Heartbleed bug, a security vulnerability in the OpenSSL protocol that reportedly affected millions of websites worldwide, "and regularly used it to gather critical intelligence."[282] Although the allegations—which the Office of the Director of National Intelligence quickly denied—appear to be false,[283] the story turned the spotlight on one of the least reported NSA practices: that the agency routinely stockpiles knowledge about security holes that it discovers so that it can later exploit the vulnerabilities to collect information or infect target devices with malware, rather than disclosing the vulnerabilities to companies so that they can be patched.[284] The practice was referred to indirectly or in passing in a number of the stories about the NSA programs, particularly in the December 2013 *Der Spiegel* series describing the behavior of the NSA's Tailored Access Operations Unit.[285] But the emphasis at that time was on the malicious activity the NSA was able to carry out as a result of those vulnerabilities, and not on the security risk created by the stockpiling itself, which leaves companies and ordinary users open to attack not just from the NSA but from anyone who discovers or learns about the flaws.

> **"While the debate over how we should value both privacy and security is important, it misses a critical point: *The United States might have compromised both security and privacy in a failed attempt to improve security.*"**
>
> -IEEE-USA,
> *"Risking it All: Unlocking the Backdoor to the Nation's Cybersecurity"*

In recent years, a substantial market for information about security vulnerabilities has sprung up, with governments joining companies and security researchers in hunting for and trading information about how to exploit holes in mass-market software and services.[286] According to the leaks, the NSA and related branches of the U.S. intelligence apparatus spend millions of dollars looking for software flaws and other vulnerabilities, targeting everything from the commercial software sold by American companies to widely used open-source protocols like OpenSSL.[287] The NSA employs more than a thousand researchers and experts using a variety of sophisticated techniques to look for bugs.[288] 'Zero-day' exploits, a term that refers to vulnerabilities that have been discovered but have not yet been disclosed to the public or the vendor,[289] are particularly coveted because it is much harder to protect systems from an attack against an unknown weakness. "Not surprisingly, officials at the N.S.A. and at its military partner, the United States Cyber Command, warned that giving up the capability to exploit undisclosed vulnerabilities would amount to 'unilateral disarmament,'" wrote cybersecurity expert David E. Sanger.[290] According to Sanger, one senior White House official told him, "I can't imagine the president — any president — entirely giving up a technology that might enable him some day to take a covert action that could avoid a shooting war."[291]

In theory, the NSA's dual mission of carrying out signals intelligence (SIGINT) and protecting communications security (COMSEC) for military and diplomatic communications should be mutually beneficial when it comes to vulnerabilities and exploits, because SIGINT could inform COMSEC about potential weaknesses and vice versa. However, as Steven Bellovin, Matt Blaze, Sandy Clark, and Susan Landau write, "reality is in fact very different. COMSEC's awareness of the need to secure certain communications channels has often been thwarted by SIGINT's desire that patching be delayed so that it can continue to exploit traffic using the vulnerability in question."[292] When the NSA discovers vulnerabilities in communications technologies and other products, it has a strong disincentive to promptly disclose those vulnerabilities to the companies since the companies will patch them, forcing the NSA to look for new ways to access the information it seeks. Thus—as in the case of encryption standards—the NSA's signals intelligence mission has interfered with the NSA's information assurance mission, and the agency has built a massive catalogue of software and

hardware vulnerabilities that is has stockpiled for its own purposes rather than disclosing them to vendors so that they can be fixed.[293]

> **"US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks... Eliminating the vulnerabilities—'patching' them—strengthens the security of US Government, critical infrastructure, and other computer systems."**
>
> -The President's Review Group on Intelligence and Communications Technologies

The Director of National Intelligence recently revealed the existence of an interagency process—referred to as the "Vulnerabilities Equities Process"—designed to facilitate the responsible disclosure of vulnerabilities,[294] but the extent to which the NSA provides information through the process is unclear.[295] NSA Director and Commander of U.S. Cyber Command Vice Admiral Michael S. Rogers explained to the Senate Armed Services Committee during his confirmation that "within NSA, there is a...process for handling '0-day' vulnerabilities discovered in any commercial product or system (not just software) utilized by the U.S. and its allies... [where] all vulnerabilities discovered by NSA... are documented, subject to full analysis, and acted upon promptly."[296] However, NSA representatives revealed few details about the depth of information on zero-day vulnerabilities the agency holds, its internal process for deciding when to disclose a vulnerability, and whether or how that process interacts with the interagency process.[297] Meanwhile, the White House has stated that a review of the interagency process is currently underway in response to the recommendations of the President's NSA Review Group. Michael Daniel, a Special Assistant to the President and Cybersecurity Coordinator, asserted that the Intelligence Community should not abandon the use of vulnerabilities as a tactic for intelligence collection, but did acknowledge that "building up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected would not be in our national security interest."[298]

The White House purports to maintain a "bias" in the Vulnerabilities Equities Process toward public disclosure in the absence of a clear national security or law enforcement need,[299] but the scope of the NSA's vulnerabilities stockpile calls into question how effective this mysterious disclosure process really is. Furthermore, the government's repeated assertions that it has "reinvigorated" the interagency process in response to the President's NSA Review Group report suggests that it has not previously been strongly implemented or consistently followed.[300] The President's Review Group report recommended that "US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks."[301] The authors went on to explain that "eliminating the vulnerabilities—'patching' them—strengthens the security of US Government, critical infrastructure, and other computer systems." The group did carve out a narrow exception for a brief authorization for the delay of notification or patching of a zero-day vulnerability, but only for "high priority intelligence collection, following senior, interagency review involving all appropriate departments."[302] Security experts like Bellovin et al. also highlight that disclosure should be the default response, especially when the vulnerability itself may create a national security risk, such as affecting network routers and switches.[303]

Hacking the Internet: How the NSA uses a wide variety of offensive hacking techniques to compromise computer systems and networks around the world

Relying on weakened encryption standards, surveillance backdoors created with or without company knowledge and assistance, and its massive catalogue of security vulnerabilities, the NSA engages in a wide variety of offensive hacking through which it has built a massive network of compromised computers systems and networks around the world. Much of this

is done through an elite group known as the Tailored Access Operations (TAO) unit, which Der Spiegel likened to "a squad of plumbers that can be called in when normal access to a target is blocked."[304] TAO employees specialize in Computer Network Exploitation to "subvert endpoint devices" such as computers, routers, phones, servers, and SCADA systems. They have developed a range of sophisticated tools to help them effectuate network intrusions that are undetectable by anti-virus software and are otherwise nearly impossible to find.[305] As Schneier puts it, "TAO has a menu of exploits it can serve up against your computer... and a variety of tricks to get them on to your computer... These are hacker tools designed by hackers with an essentially unlimited budget."[306]

One tactic for quietly scooping up vast amounts of data is to target the infrastructure around networks and network providers, including the undersea fiber optic cables that carry global Internet traffic from one continent to another. Leaked documents reveal that in February 2013 the NSA successfully hacked the SEA-ME-WE-4 cable system, which originates in France and connects Europe to the Middle East and North Africa.[307] Reports also suggest that the NSA has hacked fiber optic links connecting Google and Facebook data centers located outside of the United States.[308] For access to messages that are encrypted, the NSA maintains an internal database through its Key Provisioning Service which has encryption keys for a wide array of commercial products. A separate unit within the agency, the Key Recovery Service, exists for the purpose of trying to obtain keys that are not already a part of the NSA's database. According to *The New York Times*, "How keys are acquired is shrouded in secrecy, but independent cryptographers say many are probably collected by hacking into companies' computer servers, where they are stored."[309]

> **"TAO has a menu of exploits it can serve up against your computer... and a variety of tricks to get them on to your computer... These are hacker tools designed by hackers with an essentially unlimited budget."**
>
> -Bruce Schneier, *"NSA Surveillance: A Guide to Staying Secure"*

The NSA has also been working on ways to track and access the communications of users of anonymity tools such as Tor. According to *The Guardian*, the NSA "has made repeated attempts to develop attacks against people using Tor," including targeting the Firefox web browser used with Tor and tracking signals entering and leaving the Tor network to try to de-anonymize its users.[310] Originally a project of the U.S. Naval Research Laboratory, Tor is a service that attempts to protect user identities by routing traffic through a network of virtual tunnels. According to the project website, "Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination."[311] One de-anonymization technique the NSA has tried against Tor is "based on a long-discussed theoretical weakness of the network: that if one agency controlled a large number of the 'exits' from the Tor network, they could identify a large amount of the traffic passing through it"—although it remains unclear how many Tor nodes the NSA actually operates and whether the tracking was successfully implemented.[312] A different program called EgotisticalGiraffe exploits a vulnerability in the Firefox browser to perform a 'man-in-the-middle' attack on Tor users.[313] Still other projects attempt to identify users by measuring the timing of messages going in and out of the network and by deliberately trying to disrupt or degrade Tor traffic to force users off of the service. As *The Guardian* points out, attempts by the NSA to undermine the Tor network are particularly interesting given the fact that Tor is largely funded by other parts of the U.S. government, including the State Department's Internet Freedom program, as part of an effort to protect free expression online.[314]

One of the crown jewels of the NSA's offensive capabilities is the "QUANTUMTHEORY" toolbox, which the agency deploys to insert malware on to target computers through a variety of tactics.[315] According to *Der Spiegel*, an internal NSA presentation about QUANTUM capabilities lists a wide range of popular American companies as targets, including Facebook, Google, Yahoo, LinkedIn, and YouTube. The agency has used the program to spy on high-ranking members of the Organization of the Petroleum Exporting Countries (OPEC), while its British counterpart GCHQ relied on the capabilities to

> **"The US government should be the champion for the internet, not a threat."**
>
> -Mark Zuckerberg, CEO of Facebook

attack computers of Belgacom, a telecommunications company partly owned by the Belgian government.[316] One QUANTUM tactic is to insert malware by impersonating these companies and redirecting traffic to the NSA's own servers to obtain access to sensitive information or insert malware.[317] The NSA and GCHQ have masqueraded as both LinkedIn and Facebook on various occasions, and have reportedly attempted to spoof Google as well.[318] The reaction to this news from major American tech companies has been swift, public, and decisively critical of the U.S. government. Facebook CEO Mark Zuckerberg publicly blasted the Obama administration in March for the breach of trust as well as personally calling the President to voice his concerns.[319] "The US government should be the champion for the internet, not a threat," Zuckerberg wrote in a post on his Facebook page, expressing his frustration about the slow speed of the reform process.[320]

Using capabilities like those in its QUANTUM toolbox to insert malware and the TURBINE system for command and control of that malware, the NSA has exploited innumerable computers and networks across the globe. Each computer or network that is infected enables the infection of even more computers and networks—with NSA's ultimate goal being the insertion of millions of software implants across the Internet.[321]

Taken together, the NSA activities described in this section—the undermining of encryption, the insertion of backdoors, the stockpiling of vulnerabilities, and the building of a massive malware network that relies on the impersonation of American companies—represent a fundamental threat not just to the U.S. Internet economy but to cybersecurity itself. Yet, like the other costs discussed in this paper, they are often ignored when discussing the NSA's surveillance programs, in favor of a simplistic debate over security versus liberty.

We literally cannot afford to continue ignoring these costs.

VI. Conclusion and Recommendations

This paper has attempted to quantify and categorize a variety of the costs of the NSA surveillance programs, demonstrating the negative impact on the U.S. and global economy, American foreign policy interests, and the security of the Internet itself. Our findings indicate that the actions of the National Security Agency have already begun and will continue to cause significant damage to the interests of the United States and the global Internet community. American companies have reported declining sales overseas and lost business, especially as foreign companies turn protection from NSA spying into a competitive advantage. This erosion in trust threatens to do the most immediate damage to the cloud computing industry, which could lose billions of dollars in the next three to five years as a result. The rise of proposals from foreign governments looking to implement data localization requirements or much stronger data protection laws could also compound these losses and force changes to the architecture of the global network itself. In its foreign policy objectives, the United States has lost significant credibility not only with respect to the Internet Freedom agenda, but also in terms of broader bilateral and multilateral relations with both friendly and adversarial nations. Revelations about the extent of NSA surveillance have already colored a number of critical interactions with nations such as Germany and Brazil in the past year. And finally, the NSA has seriously undermined Internet security in the past decade, by weakening international encryption standards, mandating the insertion of backdoors into Internet products, stockpiling security vulnerabilities rather than responsibly disclosing them to vendors, and carrying out a variety of other offensive hacking operations.

The U.S. government has already taken limited steps to mitigate this damage and begin the slow, difficult process of rebuilding trust in the United States as a responsible steward of the Internet. However, the reform efforts to date have been relatively narrow, focusing primarily on the surveillance programs' impact on the rights of U.S. citizens, and failing to address other key concerns. In addition to the risk of violating the privacy and civil liberties of Americans, the President's NSA Review Group highlights a number of other areas where the NSA programs threaten our national interests. The potential effects of surveillance in our relations with other nations are concerning, especially among "our close allies and others with whom we share values, interests, or both. Unnecessary or excessive surveillance can create risks that outweigh any gain."[322] The Review Group adds that "surveillance and the acquisition of information might have harmful effects on commerce, especially if it discourages people – either citizens of the United States or others – from using certain communications providers."[323] Given the diverse array of concerns, we make the following recommendations aimed at restoring trust in American companies and the credibility of the U.S. government, as well as fostering a more open and secure Internet for users worldwide:

1. Strengthen privacy protections for both Americans and non-Americans, within the United States and extraterritorially.

2. Provide for increased transparency around government surveillance, both from the government and companies.

3. Recommit to the Internet Freedom agenda in a way that directly addresses issues raised by NSA surveillance, including moving toward international human rights-based standards on surveillance.

4. Begin the process of restoring trust in cryptography standards through the National Institute of Standards and Technology.

5. Ensure that the U.S. government does not undermine cybersecurity by inserting surveillance backdoors into hardware or software products.

6. Help to eliminate security vulnerabilities in software, rather than stockpile them.

7. Develop clear policies about whether, when, and under what legal standards it is permissible for the government to secretly install malware on a computer or in a network.

8. Separate the offensive and defensive functions of the NSA in order to minimize conflicts of interest.

1 Strengthen privacy protections for both Americans and non-Americans, within the United States and extraterritorially.

The NSA mass surveillance programs described in the introduction, conducted domestically pursuant to USA PATRIOT Act Section 215 and FISA Amendments Act Section 702 and conducted outside the U.S. under Executive Order 12333, have arguably had the greatest and most immediate impact on America's tech industry and global standing. Strictly limiting the scope and purpose of surveillance under these authorities—not just in regard to surveillance of Americans but of non-Americans as well—will be critical to regaining the trust of individuals, companies and countries around the world, as well as stemming the economic and political costs of the NSA programs.

The President's NSA Review Group acknowledged the need for such reform in its report on surveillance programs, affirming that "the right of privacy has been recognized as a basic human right that all nations should respect," and cautioned that "unrestrained American surveillance of non-United States persons might alienate other nations, fracture the unity of the Internet, and undermine the free flow of information across national boundaries."[324] In addition to recommending a variety new protections for U.S. persons, the Review Group urged in its Recommendation 13 that surveillance of non-U.S. persons under Section 702 or "any other authority"—a reference intended to include Executive Order 12333[325] — should be strictly limited to the purpose of protecting national security, should not be used for economic espionage, should not be targeted based solely on a person's political or religious views, and should be subject to careful oversight and the highest degree of transparency possible.[326] Fully implementing this recommendation—and particularly restricting Section 702 and Executive Order 12333 surveillance to specific national security purposes rather than foreign intelligence collection generally—would indicate significant progress toward addressing the concerns raised in the recent Report of the Office of the United Nations High Commissioner for Human Rights on "The Right to Privacy in the Digital Age." The UN report highlights how, despite the universality of human rights, the common distinction between "'foreigners' and 'citizens'...within national security surveillance oversight regimes" has resulted in "significantly weaker – or even non-existent – privacy protection for foreigners and non-citizens, as compared with those of citizens."[327]

> **"The right of privacy has been recognized as a basic human right that all nations should respect... unrestrained American surveillance of non-United States persons might alienate other nations, fracture the unity of the Internet, and undermine the free flow of information across national boundaries."**
>
> -The President's Review Group on Intelligence and Communications Technologies

The leading legislative reform proposal in the U.S. Congress, the USA FREEDOM Act, would go a long way to protecting both U.S. and non-U.S. persons against the bulk collection under Section 215 of records held by American telephone and Internet companies.[328] On that basis, passage of the law would very much help address the trust gap that the NSA programs have created. However, with regard to Section 702, the bill as originally introduced only added new protections for U.S. persons or for wholly domestic communications,[329] and even those protections were stripped out or weakened in the version of the bill that was passed by the House of Representatives in May 2014.[330] Meanwhile, neither the bill as introduced nor as passed by the House addresses surveillance conducted extraterritorially under Executive or 12333. Therefore, even if USA FREEDOM is eventually approved by both the House and the Senate and signed into law by the President, much more will ultimately need to be done to reassure foreign users of U.S.-based communications networks, services, and products that their rights are being respected.

Provide for increased transparency around government surveillance, both from the government and companies.

2

Increased transparency about how the NSA is using its authorities, and how U.S. companies do—or do not—respond when the NSA demands their data is critical to rebuilding the trust that has been lost in the wake of the Snowden disclosures. In July 2013, a coalition of large Internet companies and advocacy groups provided a blueprint for the necessary transparency reforms, in a letter to the Obama Administration and Congress calling for "greater transparency around national security-related requests by the US government to Internet, telephone, and web-based service providers for information about their users and subscribers."[331] Major companies including Facebook, Google, and Microsoft—joined by organizations such as the Center for Democracy and Technology, New America's Open Technology Institute, and the American Civil Liberties Union—demanded that the companies be allowed to publish aggregate numbers about the specific types of government requests they receive, the types of data requested, and the number of people affected. They also also urged the government to issue its own transparency reports to provide greater clarity about the scope of the NSA's surveillance programs.[332] "This information about how and how often the government is using these legal authorities is important to the American people, who are entitled to have an informed public debate about the appropriateness of those authorities and their use, and to international users of US-based service providers who are concerned about the privacy and security of their communications," the letter stated.[333]

Two months later, many of the same companies and organizations issued another letter supporting surveillance transparency legislation proposed by Senator Al Franken (D-MN) and Representative Zoe Lofgren (D-CA) that would have implemented many of the original letter's recommendations.[334] Elements of both bills, consistent with the coalition's recommendations, were included in the original version of the USA FREEDOM Act introduced in the House and the Senate—as were new strong transparency provisions requiring the FISA court to declassify key legal opinions to better educate the public and policymakers about how it is interpreting and implementing the law. Such strong new transparency requirements are consistent with several recommendations of the President's Review Group[335] and would help address concerns about lack of transparency raised by the UN High Commissioner for Human Rights.[336]

Unfortunately, all of these transparency provisions from the original USA FREEDOM Act were substantially weakened in the version of the bill that was passed by the House of Representatives in May 2014.[337] Congress will need to include stronger transparency provisions in any final version of the USA FREEDOM Act if it intends to meaningfully restore trust in the U.S. Internet and telecommunications industries and stem the loss of business that has begun as a result of the NSA programs. As commentator Mieke Eoyang put it, "If reforms do not deliver sufficient protections and transparency for [tech companies'] customers, especially those abroad who have the least constitutional protections, they will vote with their feet."[338]

"If reforms do not deliver sufficient protections and transparency for [tech companies'] customers, especially those abroad who have the least constitutional protections, they will vote with their feet."

-Mieke Eoyang,
"To judge NSA reforms, look to the tech industry"

3 Recommit to the Internet Freedom agenda in a way that directly addresses issues raised by NSA surveillance, including moving toward international human-rights based standards on surveillance.

The United States must act immediately to restore the credibility of the Internet Freedom agenda, lest it become another casualty of the NSA's surveillance programs. As described in Part IV, various agencies within the U.S. government have taken initial steps to demonstrate goodwill in this area, particularly through the NTIA's announcement that it intends to transition stewardship of the IANA functions to a global multistakeholder organization and the State Department's speech outlining six principles to guide signals intelligence collection grounded in international human rights norms. However, it will take a broader effort from across the government to demonstrate that the United States is fully committed to Internet Freedom, including firmly establishing the nature of its support for the evolving multistakeholder system of Internet governance and directly engaging with issues raised by the NSA surveillance programs in international conversations.

> **"The United States should counter the view that Internet Freedom is merely an American project cooked up in Washington, rather than a notion rooted in universal human rights... The response to [concerns about the Internet Freedom agenda's ties to U.S. foreign policy should be] to internationalize the effort."**
>
> -Richard Fontaine and Will Rogers, *"Internet Freedom: A Foreign Policy Imperative in the Digital Age"*

Supporting international norms that increase confidence in the security of online communications and respect for the rights of Internet users all around the world is integral to restoring U.S. credibility in this area. "We have surveillance programmes that abuse human rights and lack in transparency and accountability precisely because we do not have sufficiently robust, open, and inclusive debates around surveillance and national security policy," writes Matthew Shears of the Center for Democracy & Technology.[339] It is time to begin having those conversations on both a national and an international level, particularly at key upcoming Internet governance convenings including the 2014 Internet Governance Forum, the International Telecommunications Union's plenipotentiary meeting, and the upcoming WSIS+10 review process.[340] Certainly, the United States will not be able to continue promoting the Internet Freedom agenda at these meetings without addressing its national security apparatus and the impact of NSA surveillance on individuals around the world. Rather than being a problem, this presents an opportunity for the U.S. to assume a leadership role in the promotion of better international standards around surveillance practices.

Moreover, the U.S. should take steps to further internationalize its Internet Freedom efforts writ large and work with foreign governments to broadly promote democracy and human rights online. In 2011, Richard Fontaine and Will Rogers of the Center for a New American Security wrote that "the United States should counter the view that Internet Freedom is merely an American project cooked up in Washington, rather than a notion rooted in universal human rights... The response to [concerns about the Internet Freedom agenda's ties to U.S. foreign policy

should be] to internationalize the effort."[341] Today, more than ever, it is critical that the United States heed this advice and take steps to broaden the base of support for the Internet Freedom agenda. Future meetings and activities of the Freedom Online Coalition, which the State Department played a key role in convening, will serve as one test of these efforts as the group attempts to transition from a discussion forum for like-minded governments into a more action-oriented coalition.[342] The United States has the opportunity to urge other member countries to live up to the commitments they made at the 2014 meeting in Tallinn with respect to accountability, transparency, and other policies grounded in human rights. As Toomas Hendrik Ilves, the President of Estonia, articulated in his remarks at the 2014 meeting, "We must be honest with ourselves and admit that recent developments regarding purported surveillance by the NSA and similar organisations in different countries make the defense of an open Internet more difficult. That, too, is a challenge that Freedom Online Coalition must face."[343] Outside of the Freedom Online Coalition, but consistent with its goals, the U.S. can urge both companies and foreign governments to join organizations like the Global Network Initiative or commit to other voluntary processes that promote the centrality of human rights in the policymaking process.[344]

Begin the process of restoring trust in cryptography standards through the National Institute of Standards and Technology.

4

It is wholly inappropriate for the U.S. government to covertly influence security standards-setting processes in a way that may weaken those standards or introduce security flaws. The NSA's efforts in this area have undermined overall trust in the security of the Internet and diminished confidence in the National Institute of Standards and Technology (NIST). As the President's Review Group explains, "Encryption is an essential basis for trust on the Internet... The use of reliable encryption software to safeguard data is critical to many sectors and organizations, including financial services, medicine and health care, research and development, and other critical infrastructures in the United States and around the world."[345] Consequently, Recommendation 29 of its report urges the U.S. government to: "(1) fully support and not undermine efforts to create encryption standards; (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage."[346] Confidence in U.S. encryption standards is critical not only to the security of commercial products, but also to interoperability and the health and competitiveness of the American technology industry.[347]

Insofar as the NSA continues to provide technical expertise on encryption standards, the Federal Information Security Management Act should be amended so that NIST is no longer required to consult with the NSA when it seeks to issue new or updated encryption standards. Rather, these consultations should happen only on an as-needed basis and should focus entirely on the technical questions at hand. This will help to prevent these consultations from becoming an opportunity for the NSA to exploit or influence the standards setting process. This would also help the United States to send a message that it supports strong, widespread use of encryption instead of seeking to undermine it to increase the monitoring capabilities of the NSA. Representative Alan Grayson's amendment to the Frontiers in Innovation, Research, Science and Technology Act (H.R. 4186), which was approved by the House Committee on Science, Space, & Technology in May 2014,[348] provides a good model for how to enact this reform, and is consistent with recommendations made by the Visiting Committee on Advanced Technology (VCAT) in its July 2014 report.[349] A similar measure was approved in June 2014 by a voice vote of the House of Representatives when it was offered by Representative Grayson as an amendment to the National Defense Authorization Act (NDAA) for

> **"Encryption is an essential basis for trust on the Internet... The use of reliable encryption software to safeguard data is critical to many sectors and organizations, including financial services, medicine and health care, research and development, and other critical infrastructures in the United States and around the world."**
>
> -The President's Review Group on Intelligence and Communications Technologies

Fiscal Year 2015 (H.R. 4435),[350] though it remains to be seen whether that amendment will make it into the final appropriations bill.

Policymakers at NIST can also take proactive steps to rebuild confidence in its standards-setting process. In February 2014, the agency published a draft document that "outlines the principles, processes, and procedures of NIST's cryptographic standards efforts."[351] The document lays out the factors that drive NIST's development efforts to ensure that standards are "robust and have the confidence of the cryptographic community in order to be widely adopted and effective at securing information systems worldwide."[352] While this is a positive first step, substantial efforts are still required to reestablish the agency's credibility and trust in its work, particularly by increasing transparency and openness associated with the standard setting process. The VCAT lays out a series of recommendations in its July 2014 report that are worthy of consideration.[353] Specifically, NIST should publish information about whom it consults in the development process, as well as more technical proof establishing the efficacy of the standards that it issues. The failure to publish these technical proofs was a key criticism of the standard setting process associated with the 2006 NSA-compromised encryption standard.[354] In order to succeed at its core mission, NIST must take affirmative steps to address concerns about its role in promoting weaker encryption standards and clarify its relationship with other partners and parts of the U.S. government.

5 Ensure that the U.S. government does not undermine cybersecurity by inserting surveillance backdoors into hardware or software products.

The U.S. government should not require or request that new surveillance capabilities or security vulnerabilities be built into communications technologies and services, even if these are intended only to facilitate lawful surveillance. There is a great deal of evidence that backdoors fundamentally weaken the security of hardware and software, regardless of whether only the NSA purportedly knows about said vulnerabilities, as some of the documents suggest. A policy statement from the Internet Engineering Task Force in 2000 emphasized that "adding a requirement for wiretapping will make affected protocol designs considerably more complex. Experience has shown that complexity almost inevitably jeopardizes the security of communications."[355] More recently, a May 2013 paper from the Center for Democracy and Technology on the risks of wiretap modifications to endpoints concludes that "deployment of an intercept capability in... communications services, systems and applications poses serious security risks."[356] The authors add that "on balance mandating that endpoint software vendors build intercept functionality into their products will be much more costly to personal, economic and governmental security overall than the risks associated with not being able to wiretap all communications."[357] While NSA programs such as SIGINT Enabling—much like proposals from domestic law enforcement agencies to update the Communications Assistance for Law Enforcement Act (CALEA) to require digital wiretapping capabilities in modern Internet-based communications services[358]—may aim to

promote national security and law enforcement by ensuring that federal agencies have the ability to intercept Internet communications, they do so at a huge cost to online security overall.

Because of the associated security risks, the U.S. government should not mandate or request the creation of surveillance backdoors in products, whether through legislation, court order, or the leveraging industry relationships to convince companies to voluntarily insert vulnerabilities. As Bellovin *et al*. explain, complying with these types of requirements would also hinder innovation and impose a "tax" on software development in addition to creating a whole new class of vulnerabilities in hardware and software that undermines the overall security of the products.[359] An amendment offered to the NDAA for Fiscal Year 2015 (H.R. 4435) by Representatives Zoe Lofgren (D-CA) and Rush Holt (D-NJ) would have prohibited inserting these kinds of vulnerabilities outright.[360] The Lofgren-Holt proposal aimed to prevent "the funding of any intelligence agency, intelligence program, or intelligence related activity that mandates or requests that a device manufacturer, software developer, or standards organization build in a backdoor to circumvent the encryption or privacy protections of its products, unless there is statutory authority to make such a mandate or request."[361] Although that measure was not adopted as part of the NDAA, a similar amendment sponsored by Lofgren along with Representatives Jim Sensenbrenner (D-WI) and Thomas Massie (R-KY), did make it into the House-approved version of the NDAA—with the support of Internet companies and privacy organizations[362]—passing on an overwhelming vote of 293 to 123.[363] Like Representative Grayson's amendment on NSA's consultations with NIST around encryption, it remains to be seen whether this amendment will end up in the final appropriations bill that the President signs. Nonetheless, these legislative efforts are a heartening sign and are consistent with recommendations from the President's Review Group that the U.S. government should not attempt to deliberately weaken the security of commercial encryption products. Such mandated vulnerabilities, whether required under statute or by court order or inserted simply by request, unduly threaten innovation in secure Internet technologies while introducing security flaws that may be exploited by a variety of bad actors. A clear policy against such vulnerability mandates is necessary to restore international trust in U.S. companies and technologies.

"Adding a requirement for wiretapping will make affected protocol designs considerably more complex. Experience has shown that complexity almost inevitably jeopardizes the security of communications."

-The Internet Engineering Task Force, *"IETF Policy on Wiretapping"*

6 Help to eliminate security vulnerabilities in software, rather than stockpile them.

The NSA's apparent stockpiling of security vulnerabilities in widely-used hardware and software products (rather than responsibly disclosing them to vendors so that they may be patched) threatens cybersecurity writ large. The U.S. government needs to establish a clear and consistent policy of disclosing vulnerabilities to vendors by default. To the extent such a policy allows vulnerability stockpiling at all, it must explicitly define when, under what circumstances, and for how long the government may delay disclosure, if ever. A central tenet of this policy should be that if the U.S. government holds onto security vulnerabilities for future exploitation at all, it should only do so in extraordinarily rare cases, such as where there are no other legitimate means to access information that is necessary to protect against an immediate national security threat. It is critical that any such policy authorizing the stockpiling of vulnerabilities spell out in explicit and precise terms the limited circumstances that would qualify for such an exception, as well as specific guidelines for when and how vendors should be informed of the flaw after it has been used for that limited purpose.

> **"In a world of great cybersecurity risk... public safety and national security are too critical to take risks and leave vulnerabilities unreported and unpatched... [L]aw enforcement should always err on the side of caution in deciding whether to refrain from informing a vendor of a vulnerability."**
>
> -Steven Bellovin, *et al.*, *"Lawful Hacking"*

As Bellovin *et al*. write, "In a world of great cybersecurity risk... public safety and national security are too critical to take risks and leave vulnerabilities unreported and unpatched... Law enforcement should always err on the side of caution in deciding whether to refrain from informing a vendor of a vulnerability. Any policy short of full and immediate reporting is simply inadequate."[364] Similarly, Recommendation #30 from the President's Review Group recommends that "US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks," carving out an exception for rare instances when "US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments."[365] Additionally, any decision not to disclose a vulnerability should be subject to a rigorous review process. The President's Review Group recommends the creation of an interagency process to regularly review "the activities of the US government regarding attacks that exploit a previously unknown vulnerability in a computer application or system."[366] To the extent such a "Vulnerabilities Equities Process" already exists as the Administration now claims, the government must be much more transparent about its operation and the standards under which it operates, in order to reassure users of American hardware and software products that both industry and government are fully dedicated ensuring the security of those products.

7 Develop clear policies about whether, when, and under what legal standards it is permissible for the government to secretly install malware on a computer or in a network.

Since the Snowden revelations, the public has learned that the NSA has a massive capability to conduct remote intrusions against computers and networks around the globe, compromising the security of tens or hundreds of thousands of systems with a goal of compromising millions more. Yet, the rules of the road for whether, when, and under what legal standards it is permissible for the government to engage in such secret hacking operations—especially foreign intelligence operations conducted outside of the U.S. under Executive Order 12333—are wholly unclear. Federal computer crime law generally forbids unauthorized intrusion into computers—including most computers outside of the United States—but does not apply to lawfully authorized investigative or intelligence activities of law enforcement or intelligence agencies.[367] Therefore, how the law regulates when the government can hack into computers to search their contents or install secret spyware is still a contested issue. This question has finally begun to be debated in earnest by courts and commentators in the context of law enforcement investigations here in the U.S.,[368] but we still have not begun a similar conversation about the NSA's hacking activities both domestically and abroad. Such a conversation, leading to clear and privacy-protective policy on the matter, is urgently necessary to ensure and reassure that NSA's program of computer intrusions—which appear to be vast—is subject to clear regulation and strict oversight.

Separate the offensive and defensive functions of the NSA in order to minimize conflicts of interest.

8

The NSA's multi-pronged efforts to weaken Internet security in order to facilitate signals intelligence collection demonstrate the inherent conflict of interest that has resulted from the agency's multiple mandates. In theory, it is possible to strike a middle ground between foreign intelligence collection and the protection of domestic communications, but as Professor Jon M. Peha explained in comments to the President's Review Group, "If the balance is wrong, a well-intentioned government agency can severely undermine security rather than strengthen it, and endanger the very American citizens that the agency hopes to protect."[369] The recent disclosures suggest that this is, in fact, the case. "NSA's two fundamental missions – one defensive, one offensive – are fundamentally incompatible, and that they can't both be handled credibly by the same government agency," wrote the Cato Institute's Julian Sanchez in April 2014, adding that "because Internet security depends on trust and cooperation between researchers, the mission of a security-breaking agency is fundamentally incompatible with that of a security-protecting agency."[370] The President's Review Group agreed that the agency "has multiple missions and mandates, some of which are blurred, inherently conflicting, or both," concluding that the "NSA is and should be a foreign intelligence organization. It should not be a domestic security service, a military command, or an information assurance organization."[371]

The President's Review Group recommends that non-foreign intelligence missions should generally be assigned to other agencies, urging the President to create greater separation between the NSA and U.S. Cyber Command and to spin off the "defensive" parts of the agency and place that work within the Department of Defense instead.[372] Their report argues that "in keeping with the concept that NSA should be a foreign intelligence agency, the large and important Information Assurance Directorate (IAD) of NSA should be organizationally separate and have a different reporting structure. IAD's primary mission is to ensure the security of the DOD's communications systems."[373] We recommend ensuring against a conflict of interest with the Defense Department by going one step farther than the Review Group recommends, and placing the government's domestic cybersecurity mission firmly within civilian control at a civilian agency such as the Department of Homeland Security.[374] As the past year's revelations have demonstrated, placing the Defense Department in charge of the security of the Internet, while it is also responsible for conducting surveillance over the Internet, is a conflict of interest too costly to leave in place: costly to our Internet economy, to our foreign relations, and to the openness and security of the Internet itself.

"NSA's two fundamental missions – one defensive, one offensive – are fundamentally incompatible, and... they can't both be handled credibly by the same government agency... Because Internet security depends on trust and cooperation between researchers, the mission of a security-breaking agency is fundamentally incompatible with that of a security-protecting agency."

-Julian Sanchez,
"The NSA's Heartbleed problem is the problem with the NSA"

Notes and References

1. Charlie Savage, "Senators Say Patriot Act is Being Misinterpreted," *The New York Times*, May 26, 2011, http://www.nytimes.com/2011/05/27/us/27patriot.html?_r=0 (accessed July 25, 2014).
2. Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian,* June 6, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (accessed July 25, 2014); "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court," *Privacy and Civil Liberties Oversight Board*, January 23, 2014, http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf (hereinafter "PCLOB 215 Report"), at 8-10 (briefly describing and giving the history of the Section 215 program).
3. *See* PCLOB 215 Report at 16 ("The Section 215 bulk telephone records program lacks a viable legal foundation under Section 215, implicates constitutional concerns under the First and Fourth Amendments, raises serious threats to privacy and civil liberties as a policy matter, and has shown only limited value.") and 10 ("[T]he board concludes that Section 215 does not provide an adequate legal basis to support this program.").
4. *See* "Timeline of Edward Snowden's Revelations," *Al Jazeera America*, n.d., http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html (accessed July 25, 2014). See also Kayla Robinson, "What we know now: 365 days of surveillance revelations," *Access*, June 5, 2014, https://www.accessnow.org/blog/2014/06/05/what-we-know-now (accessed July 25, 2014).
5. Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *The Washington Post*, June 7, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (accessed July 25, 2014); Barton Gellman and Laura Poitras, "NSA slides explain the PRISM data-collection program," *The Washington Post*, June 6, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (accessed July 25, 2014).
6. Although initial reports indicated—based on the imprecise wording of leaked NSA slides—that the NSA had "direct access" to Internet companies' servers, those allegations were refuted by a number of sources. *See, e.g.,* Declan McCullagh, "No evidence of NSA's 'direct access' to tech companies," *CNET*, June 7, 2013, http://www.cnet.com/news/no-evidence-of-nsas-direct-access-to-tech-companies/ (accessed July 25, 2014); see also Amir Efrati, "How Google Transfers Data To NSA," *Wall Street Journal*, June 11, 2013, http://blogs.wsj.com/digits/2013/06/11/how-google-transfers-data-to-nsa/ (accessed July 25, 2014) which describes how Google provides data to NSA via secure file transfer protocol or physical handover rather than via direct access to Google servers; Kashmir Hill, "Facebook Denies Giving NSA Direct Access To Its Servers; Microsoft Says It Only Turns Over Info For 'Specific Accounts'," *Forbes*, July 6, 2013, http://www.forbes.com/sites/kashmirhill/2013/06/06/facebook-denies-giving-nsa-direct-access-to-its-servers/ (accessed July 25, 2014).
7. Foreign Intelligence Surveillance Court opinion, October 3, 2011 (hereinafter "FISC Opinion") at 29, available at https://www.aclu.org/files/assets/fisc_opinion_10.3.2011.pdf. NSA slides obtained by *The Washington Post* state that in April 2013, for example, there were 117,675 surveillance targets associated with the PRISM program (Gellman and Poitras, "NSA slides explain the PRISM data-collection program.").
8. *See* FISC Opinion at 29-30 ("upstream collection constitutes only approximately 9% of the total Internet communications being acquired by NSA under Section 702") and Craig Timberg, "The NSA slide you haven't seen," *The Washington Post*, July 10, 2013, http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html (describing upstream collection) (accessed July 25, 2014). For an extensive summary of both the "downstream" and "upstream" aspects of NSA's Section 702 surveillance, see "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," *Privacy and Civil Liberties Oversight Board* (hereinafter "PCLOB 702 Report"), January 23, 2014, at 32-41, http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report.pdf (describing both the PRISM "downstream" program and the "upstream" wiretapping programs).
9. John Napier Tye, "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans," *The Washington Post*, July 18, 2014, http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html (accessed July 25, 2014).
10. Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post*, October 30, 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (accessed July 25, 2014).
11. Barton Gellman and Ashkan Soltani, "NSA collects millions of e-mail address books globally," *The Washington Post*, October 14, 2013, http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html (accessed July 25, 2014).
12. Barton Gellman and Ashkan Soltani, "NSA surveillance program reaches 'into the past' to retrieve, replay phone calls," *The Washington Post*, March 18, 2014, http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (accessed July 25, 2014).
13. Spencer Ackerman and James Ball, "Optic Nerve:

millions of Yahoo webcam images intercepted by GCHQ," *The Guardian*, February 27, 2014, http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo (accessed July 25, 2014).

14. Barton Gellman and Ashkan Soltani, "NSA tracking cellphone locations worldwide, Snowden documents show," *The Washington Post*, December 4, 2013, http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html (accessed July 25, 2014).
15. Spiegel Staff, "Inside TAO: Documents Reveal Top NSA Hacking Unit," *Der Spiegel*, December 29, 2013, http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html (accessed July 25, 2014).
16. *Id.*; Nicole Perlroth, Jeff Larson & Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *The New York Times*, September 5, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0 (accessed July 25, 2014).
17. "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies," *The White House*, December 12, 2013, at 45-46, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed July 25, 2014).
18. *See, e.g.*, Tom McCarthy, "Obama defends secret NSA surveillance programs – as it happened," *The Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/07/obama-administration-nsa-prism-revelations-live (accessed July 25, 2014); David E. Sanger and Thom Shanker, "N.S.A. Director Firmly Defends Surveillance Efforts," *The New York Times*, October 12, 2013, http://www.nytimes.com/2013/10/13/us/nsa-director-gives-firm-and-broad-defense-of-surveillance-efforts.html (accessed July 25, 2014); Walter Pincus, "The other side of the surveillance story," *The Washington Post*, August 14, 2013, http://www.washingtonpost.com/world/national-security/the-intelligence-communitys-side-of-the-collection-programs-debate/2013/08/14/02674a96-043b-11e3-9259-e2aafe5a5f84_story.html (accessed July 25, 2014).
19. Peter Bergen, David Sterman, Emily Schneider & Bailey Cahall, "Do NSA's Bulk Surveillance Programs Stop Terrorists?" *New America Foundation*, January 13, 2014, http://newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists. In an analysis of 225 cases of individuals that had been recruited by foreign terrorist organizations and charged with acts of terrorism in the United States since September 11th, the report found that traditional investigative methods were used to initiate the vast majority. "Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group," the authors wrote.
20. PCLOB 215 Report at 146.
21. "Liberty and Security in a Changing World" at 51.
22. PCLOB 702 Report at 2.
23. Barton Gellman, Julie Tate & Ashkan Soltani, "In NSA-intercepted data, those not targeted far outnumber the foreigners who are," *The Washington Post*, July 5, 2014, http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html (accessed July 25, 2014).
24. Wilson Andrews and Todd Lindeman, "$52.6 Billion: The Black Budget," *The Washington Post*, August 29, 2013, http://www.washingtonpost.com/wp-srv/special/national/black-budget/ (accessed July 25, 2014); Steve H. Hanke, "The NSA's Rent is Too Damn High," *The Cato Institute*, October 28, 2013, http://www.cato.org/blog/nsas-rent-too-damn-high (accessed July 25, 2014).
25. Mieke Eoyang and Gabriel Horowitz, "NSA Snooping's Negative Impact On Business Would Have the Founding Fathers 'Aghast,'" *Forbes*, December 20, 2013, http://www.forbes.com/sites/realspin/2013/12/20/nsa-snoopings-negative-impact-on-business-would-have-the-founding-fathers-aghast/ (accessed July 25, 2014).
26. Sam Gustin, "NSA Spying Scandal Could Cost U.S. Tech Giants Billions," *TIME*, December 10, 2013, http://business.time.com/2013/12/10/nsa-spying-scandal-could-cost-u-s-tech-giants-billions/ (accessed July 25, 2014).
27. *See, e.g.*, Ian Hathaway, "Tech Starts: High-Technology Business Formation and Job Creation in the United States," *Ewing Marion Kauffman Foundation*, August 2013, http://www.kauffman.org/~/media/kauffman_org/research%20reports%20and%20covers/2013/08/bdstechstartsreport.pdf; Dale W. Jorgenson, Mun Ho & Jon Samuels, "Information Technology and U.S. Productivity Growth: Evidence from a Prototype Industry Production Account," *Harvard University*, November 19, 2010, http://scholar.harvard.edu/files/jorgenson/files/02_jorgenson_ho_samuels19nov20101_2.pdf.
28. Gellman and Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program."
29. *See, e.g.*, Dominic Rushe, "Facebook and Google insist they did not know of Prism surveillance program," *The Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/07/google-facebook-prism-surveillance-program (accessed July 25, 2014). *See also* McCullagh, "No evidence of NSA's 'direct access' to tech companies"; Efrati, "How Google Transfers Data To NSA"; K. Hill, "Facebook Denies Giving NSA Direct Access To Its Servers; Microsoft Says It Only Turns Over Info For 'Specific Accounts.'"
30. *The Washington Post* updated its PRISM slides on July 10, 2013 to add further explanation of how the program works. See "NSA slides explain the PRISM data-collection program," *The Washington Post*, June 6, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (accessed July 25, 2014).
31. "Statement of Judiciary Committee Chairman Bob Goodlatte House Consideration of H.R. 3361, The "USA FREEDOM Act," *United States House of Representatives Judiciary Committee*, May 22, 2014, http://judiciary.house.gov/index.cfm/2014/5/statement-of-judiciary-committee-chairman-bob-goodlatte-house-consideration-of-h-r-3361-the-usa-freedom-act (accessed July 25, 2014).
32. David Gilbert, "Companies Turn to Switzerland for Cloud Storage Following NSA Spying Revelations," *International Business Times*, July 4, 2013, http://www.

ibtimes.co.uk/business-turns-away-dropbox-towards-switzerland-nsa-486613 (accessed July 25, 2014).

33. *Id.*

34. Irene Bodle, "Why You Should Be Hosting Your Data in Switzerland not the USA," *Web Analytics World*, February 28, 2012, http://www.webanalyticsworld.net/2012/02/why-you-should-be-hosting-your-data-in-switzerland-not-the-usa.html (accessed July 25, 2014).

35. Archana Venkatraman, "Is Switzerland turning into a cloud haven in the wake of Prism scandal?" *Computer Weekly,* July 5, 2013, http://www.computerweekly.com/news/2240187513/Is-Switzerland-turning-into-a-cloud-haven-in-the-wake-of-Prism-scandal (accessed July 25, 2014).

36. PEER 1 is a Vancouver-based web infrastructure and cloud hosting provider. See "About us," *Peer 1 Hosting*, n.d., http://www.peer1.com (accessed July 25, 2014).

37. "NSA Scandal: UK and Canadian Business Weary of Storing Data in the US," *Peer 1 Hosting*, January 8, 2014, http://www.peer1.com/news-update/nsa-scandal-uk-and-canadian-businesses-wary-storing-data-in-us (accessed July 25, 2014).

38. Mary DeRosa, "U.S. Cloud Services Companies are Paying Dearly for NSA Leaks," *NextGov*, March 24, 2014, http://www.nextgov.com/technology-news/tech-insider/2014/03/us-cloud-services-companies-are-paying-dearly-nsa-leaks/81100/ (accessed July 25, 2014); Allan Friedman, "Why Wasn't the NSA Prepared?" *The Atlantic*, August 2, 2013, http://www.theatlantic.com/national/archive/2013/08/why-wasnt-the-nsa-prepared/278310/ (accessed July 25, 2014).

39. Dominic Rushe, "Zuckerberg: US government 'blew it' on NSA surveillance," *The Guardian*, September 11, 2013, http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance (accessed July 25, 2014).

40. Awesome Cloud "Cloud Computing Growth," Infographic, *n.d.*, http://www.awesomecloud.com/wp-content/uploads/cloud_computing_growth_infographic.pdf (accessed July 25, 2014).

41. Steven Titch, "Has the NSA Poisoned the Cloud?" *R Street Policy Study No. 17*, January 2014, http://www.rstreet.org/wp-content/uploads/2014/01/RSTREET17.pdf.

42. Daniel Castro, "How Much Will PRISM Cost the US Cloud Computing Industry?" *The Information Technology and Innovation Foundation*, August 5, 2013, http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry.

43. "Gartner Predict Cloud Computing Spending to Increase by 100% in 2016, Says AppsCare," *PRWeb*, July 19, 2012, http://www.prweb.com/releases/2012/7/prweb9711167.htm (accessed July 25, 2014).

44. Castro, "How Much Will PRISM Cost the US Cloud Computing Industry?" at 4.

45. Titch, "Has the NSA Poisoned the Cloud?" at 5.

46. James Staten, "The Cost of PRISM Will Be Larger Than ITIF Projects," *Forrester*, August 14, 2013, http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects (accessed July 25, 2014).

47. *Id.*

48. "Eyes Wide Open," *Privacy International*, November 28, 2013, https://www.privacyinternational.org/reports/eyes-wide-open.

49. Staten, "The Cost of PRISM Will Be Larger Than ITIF Predicts."

50. Aarti Shahani, "A Year After Snowden, U.S. Tech Losing Trust Overseas," *NPR*, June 5, 2014, http://www.npr.org/blogs/alltechconsidered/2014/06/05/318770896/a-year-after-snowden-u-s-tech-losing-trust-overseas?sc=17&f=1001 (accessed July 25, 2014).

51. "NSA After-shocks: How Snowden has changed ICT decision-makers' approach to the Cloud," *NTT Communications*, March 2014, http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf.

52. Julian Hattem, "Tech takes hit from NSA," *The Hill*, June 30, 2014, http://thehill.com/policy/technology/210880-tech-takes-hit-from-nsa (accessed July 25, 2014).

53. Georg Mascolo and Ben Scott, "Lessons from the Summer of Snowden: The Hard Road Back to Trust," *New America Foundation and the Wilson Institute*, October 2013, 2, http://www.newamerica.net/sites/newamerica.net/files/policydocs/NAF-OTI-WC-SummerOfSnowdenPaper.pdf.

54. Claire Cain Miller, "Revelations of NSA Spying Cost US Tech Companies," *The New York Times*, March 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=2 (accessed July 25, 2014).

55. See "Offshore Privacy," *Runbox*, *n.d.*, https://runbox.com/ (accessed July 25, 2014).

56. "Runbox Mentioned in the New York Times," *Runbox Blog*, February 19, 2014, http://blog.runbox.com/2014/02/runbox-mentioned-in-the-new-york-times/ (accessed July 25, 2014).

57. "Look North for a Safe, Private Cloud," *F-Secure*, June 12, 2013, http://www.f-secure.com/en/web/home_global/news-info/product-news-offers/view/story/983046/Look%20North%20for%20a%20Safe,%20Private%20Cloud (accessed July 25, 2014).

58. Mark Scott, "European Firms Turn Privacy Into Sales Pitch," *The New York Times*, June 11, 2014, http://bits.blogs.nytimes.com/2014/06/11/european-firms-turn-privacy-into-sales-pitch/?_php=true&_type=blogs&_r=0 (accessed July 25, 2014).

59. C. Miller, "Revelations of NSA Spying Cost US Tech Companies."

60. Sean Gallagher, "NSA leaks blamed for Cisco's falling sales overseas," *Ars Technica*, December 10, 2013, http://arstechnica.com/information-technology/2013/12/nsa-leaks-blamed-for-ciscos-falling-sales-overseas/ (accessed July 25, 2014). In May 2014, Cisco reported better than expected earnings – which were mostly a reflection of the dismal numbers it released at the end of the previous year and steps the company had taken to rebuild trust through additional security measures. (Quentin Hardy, "For Cisco, Higher Stock Price is Still Chasing Ambition," *The New York Times*, May 14, 2014, http://bits.blogs.nytimes.com/2014/05/14/for-cisco-higher-stock-price-is-still-chasing-ambition/ [accessed July 25, 2014].)

61. Paul Taylor, "Cisco warns emerging market weakness is no blip," *Financial Times*, December 13, 2013, http://www.ft.com/intl/cms/s/0/fb757c4e-637b-11e3-a87d-00144feabdc0.html?siteedition=uk#axzz2yAhAnfN3 (accessed July 25, 2014).

62. S. Gallagher, "NSA leaks blamed for Cisco's falling sales overseas."

63. Matthew Miller, "In China, US Tech Firms Weigh 'Snowden Effect,'" *Reuters*, January 21, 2014, http://www.reuters.com/article/2014/01/21/us-ibm-china-idUSBREA0K0FB20140121 (accessed July 25, 2014).

64. Sean Gallagher, "Photos of an NSA 'upgrade' factory show Cisco router getting implant," *Ars Technica*, May 14, 2014, http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/ (accessed July 25, 2014).

65. Arik Hesseldahl, "In Letter to Obama, Cisco CEO Complains About NSA Allegations," *re/code*, May 18, 2014, http://recode.net/2014/05/18/in-letter-to-obama-cisco-ceo-complains-about-nsa-allegations/ (accessed July 25, 2014).

66. Spencer E. Ante, "Qualcomm CEO Says NSA Fallout Impacting China Business," *The Wall Street Journal*, November 22, 2013, http://online.wsj.com/news/articles/SB10001424052702304337404579214353783842062 (accessed July 25, 2014). *See also* Eamon Javers, "Is a Snowden effect stalking US telecom sales?" *CNBC*, November 15, 2013, http://www.cnbc.com/id/101202361 (accessed July 25, 2014).

67. M. Miller, "In China, US Tech Firms Weigh 'Snowden Effect."

68. Haydn Shaughnessy, "Will the NSA Hack Wreck Apple's Hopes in China?" *Forbes*, January 7, 2014, http://www.forbes.com/sites/haydnshaughnessy/2014/01/07/will-the-nsa-hack-wreck-apple-hopes-in-china/ (accessed July 25, 2014).

69. Anton Troianovski, Thomas Gryta &Sam Schechner, "NSA Fallout Thwarts AT&T," *The Wall Street Journal*, October 30, 2013, http://online.wsj.com/news/articles/SB10001424052702304073204579167873091999730 (accessed July 25, 2014).

70. C. Miller, "Revelations of NSA Spying Cost US Tech Companies."

71. Frederik Obermaier and Benedikt Strunz, "Germany Plans To Ban Tech Companies That Play Ball With NSA," *Suddeutsche Zeitung International*, May 16, 2014, http://international.sueddeutsche.de/post/85917094540/germany-plans-to-ban-tech-companies-that-play-ball-with (accessed July 25, 2014); Benedikt Strunz, "No-Spy-Garantie als Geschäftsbedingung," *Tagesschau.de*, May 15, 2014, http://www.tagesschau.de/inland/csc106.html (accessed July 25, 2014) (in German).

72. Andrea Peterson, "German government to drop Verizon over NSA spying fears," *The Washington Post*, June 26, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/06/26/german-government-to-drop-verizon-over-nsa-spying-fears/ (accessed July 25, 2014).

73. "NSA Fears Prompt Germany to End Verizon Contract," *Associated Press*, June 26, 2014, http://abcnews.go.com/Technology/wireStory/nsa-fears-prompt-germany-end-verizon-contract-24314604 (accessed July 25, 2014).

74. Alonso Soto and Brian Winter, "3-Saab wins Brazil jet deal after NSA spying sours Boeing bid," *Reuters*, December 18, 2013, http://www.reuters.com/article/2013/12/18/brazil-jets-idUSL2N0JX17W20131218 (accessed July 25, 2014).

75. Carol Matlack, "Is NSA Spying Why Brazil Chose Saab Over Boeing?" *Bloomberg Businessweek*, December 19, 2013, http://www.businessweek.com/articles/2013-12-19/did-boeing-lose-brazils-fighter-order-as-payback-for-nsa-spying (accessed July 25, 2014).

76. *Id.*

77. In a number of industries, the economics of switching can far outweigh any benefits to avoiding surveillance. In a May 2014 white paper, Ross Anderson describes the "lock-in effects in the underlying industries, where (for example) Cisco dominates the router market: those countries that have tried to build US-free information infrastructures (China) or even just government information infrastructures (Russia, Germany) find it's expensive." (Ross Anderson, "Privacy versus government surveillance: where network effects meet public choice," *The 13th Annual Workshop on the Economics of Information Security at Pennsylvania State University*, May 27, 2014, http://weis2014.econinfosec.org/papers/Anderson-WEIS2014.pdf.)

78. Jennifer Scott, "Huawei may be one of the few winners of the NSA revelations," *Computer Weekly*, February 13, 2014, http://www.computerweekly.com/blogs/the-full-spectrum/2014/02/the-western-accusers-need-to-f.html (accessed July 25, 2014).

79. Titch, "Has the NSA Poisoned the Cloud?" at 3.

80. Taylor Armerding, "NSA spying could mean US tech companies lose international business," *ComputerWorld*, June 19, 2013, http://www.computerworld.co.nz/article/487899/nsa_spying_could_mean_us_tech_companies_lose_international_business/ (accessed July 25, 2014).

81. Alina Selukh, "Facebook's Zuckerberg says U.S. spying hurt users trust," *Reuters*, September 18, 2013, http://www.reuters.com/article/2013/09/18/net-us-usa-facebook-washington-idUSBRE98H19P20130918 (accessed July 25, 2014); Jose Pagliery, "Mark Zuckerberg calls Obama to complain about NSA," *CNN Money*, March 14, 2014, http://money.cnn.com/2014/03/13/technology/security/mark-zuckerberg-nsa/ (accessed July 25, 2014); Arik Hesseldahl, "In Letter to Obama, Cisco CEO Complains About NSA Allegations."

82. AOL, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo, "Reform Government Surveillance," January 2014, https://www.reformgovernmentsurveillance.com/ (accessed July 25, 2014).

83. The Reform Government Surveillance Coalition was listed as a supporter of "The Day We Fight Back" protests on February 11, 2014 (*see* https://thedaywefightback.org/) and the coalition sent a letter and took out full page newspaper advertisements on the one-year anniversary of the Snowden leaks urging the Senate to enact strong reforms (*see* "Letter to the Senate on the USA Freedom Act," June 5, 2014, https://www.reformgovernmentsurveillance.com/USAFreedomAct). *See also* Tony Romm, "Tech's biggest players hire first NSA lobbyist," *Politico*, February 6, 2014, http://www.politico.com/story/2014/02/techs-biggest-players-hire-first-nsa-lobbyist-103214.html (accessed July 25, 2014); Joseph Menn, "U.S. Tech Firms Beef Up Security to Thwart Mass Spying," *Reuters*, June 5, 2014. http://www.reuters.com/article/2014/06/05/us-cybersecurity-tech-idUSKBN0EG2BN20140605 (accessed July 25, 2014).

84. David Auerbach, "The NSA Is Bad for Business: And that's why all the biggest tech rivals are joining together to limit government surveillance," *Slate*, January 8, 2014, http://www.slate.com/articles/technology/

bitwise/2014/01/google_apple_facebook_and_the_nsa_tech_companies_come_together_to_limit.html (accessed July 25, 2014).

85. "New Harris Poll Shows NSA Revelations Impact Online Shopping, Banking, and More," *We Live Security*, April 2, 2014, http://www.welivesecurity.com/2014/04/02/harris-poll-nsa-revelations-impact-online-shopping-banking/ (accessed July 25, 2014). *See also* Julian Hattem, "Many say NSA news changed their behavior," *The Hill*, April 2, 2014, http://thehill.com/policy/technology/202434-poll-nearly-half-say-nsa-news-affected-behaior (accessed July 25, 2014).
86. Jon Swartz, "NSA surveillance hurting tech firms' business," *USA Today*, February 28, 2014, http://www.usatoday.com/story/tech/2014/02/27/nsa-resistant-products-obama-tech-companies-encryption-overseas/5290553/ (accessed July 25, 2014).
87. David E. Sanger and Nicole Perlroth, "Internet Giants Erect Barriers to Spy Agencies," *The New York Times*, June 6, 2014, http://www.nytimes.com/2014/06/07/technology/internet-giants-erect-barriers-to-spy-agencies.html?smid=tw-share&_r=0 (accessed July 25, 2014).
88. Alex Stamos, "Status Update: Encryption at Yahoo," *Yahoo*, April 2, 2014, http://yahoo.tumblr.com/post/81529518520/status-update-encryption-at-yahoo (accessed July 25, 2014). See also Lucian Constantin, "Yahoo starts encrypting all email, but implementation is inconsistent," *PC World*, January 8, 2014, http://www.pcworld.com/article/2085700/as-yahoo-makes-encryption-standard-for-email-weak-implementation-seen.html (accessed July 25, 2014).
89. Craig Timberg, "Google encrypts data amid backlash against NSA spying," *The Washington Post*, September 6, 2013, http://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html (accessed July 25, 2014).
90. Brandon Long, "Transparency Report: Protecting emails as they travel across the web," *Google Official Blog*, June 3, 2014, http://googleblog.blogspot.co.uk/2014/06/transparency-report-protecting-emails.html (accessed July 25, 2014).
91. Mark Hachman, "Comcast plans to encrypt email exchanged with Google's Gmail," *PC World*, June 4, 2014, http://www.pcworld.com/article/2359446/comcast-plans-to-encrypt-email-exchaged-with-googles-gmail.html (accessed July 25, 2014).
92. Russell Brandom, "Microsoft offers overseas data in response to NSA concerns," *The Verge*, January 22, 2014, http://www.theverge.com/2014/1/22/5335434/microsoft-offers-overseas-data-storage-in-response-to-nsa-concerns (accessed July 25, 2014).
93. C. Miller, "Revelations of NSA Spying Cost US Tech Companies."
94. C. Miller, "Revelations of NSA Spying Cost US Tech Companies"; Tony Kontzer, "IBM Spends $1.2 Billion on New Cloud Data Centers," *Network Computing*, January 23, 2014, http://www.networkcomputing.com/data-centers/ibm-spends-$12-billion-on-new-cloud-datacenters/d/d-id/1234641 (accessed July 25, 2014).
95. Barb Darrow, "Why we need to stop freaking out about the NSA and get on with business," *GigaOm*, June 7, 2014, http://gigaom.com/2014/06/07/why-we-need-to-stop-freaking-out-about-the-nsa-get-on-with-business/ (accessed July 25, 2014).
96. Nicole Perlroth and Scott Shane, "As F.B.I. Pursued Snowden, and E-Mail Service Stood Firm," *The New York Times*, October 2, 2013, http://www.nytimes.com/2013/10/03/us/snowdens-e-mail-provider-discusses-pressure-from-fbi-to-disclose-data.html?pagewanted=2&_r=0&pagewanted=all (accessed July 25, 2014). *See also* Ladar Levison, "Secrets, lies, and Snowden's email: why I was forced to shut down Lavabit," *The Guardian*, May 20, 2014, http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email (accessed July 25, 2014).
97. Parmy Olson, "Encryption App Silent Circle Shuts Down E-Mail Service 'To Prevent Spying'," *Forbes*, August 9, 2013, http://www.forbes.com/sites/parmyolson/2013/08/09/encryption-app-silent-circle-shuts-down-e-mail-service-to-prevent-spying/ (accessed July 25, 2014).
98. Hattem, "Tech Takes Hit from NSA."
99. Sascha Meinrath, "The Future of the Internet: Balkanization and Borders," *TIME*, October 11, 2013, http://ideas.time.com/2013/10/11/the-future-of-the-internet-balkanization-and-borders/ (accessed July 25, 2014); Leslie Harris, "Don't Gerrymander the Internet," *Index on Censorship*, November 4, 2013, http://www.indexoncensorship.org/2013/11/dont-gerrymander-internet/ (accessed July 25, 2014).
100. Matthew Taylor, Nick Hopkins & Jemima Kiss, "NSA surveillance may cause breakup of Internet, warn experts," *The Guardian*, November 1, 2013, http://www.theguardian.com/world/2013/nov/01/nsa-surveillance-cause-internet-breakup-edward-snowden (accessed July 25, 2014); Daniel Castro, "Digital Trade in a Post-PRISM World," *The Hill*, July 24, 2013, http://thehill.com/blogs/congress-blog/technology/312887-digital-trade-in-a-post-prism-world (accessed July 25, 2014).
101. David Meyer, "Web firms face a strict new set of privacy rules in Europe – here's what to expect," *GigaOm*, March 12, 2014, http://gigaom.com/2014/03/12/web-firms-face-a-strict-new-set-of-privacy-rules-in-europe-heres-what-to-expect/ (accessed July 25, 2014); Danny Hakim, "Europe Aims to Regulate the Cloud," *The New York Times*, October 6, 2013, http://www.nytimes.com/2013/10/07/business/international/europe-aims-to-regulate-the-cloud.html?_r=1& (accessed July 25, 2014); Alex Byers, "Tech Safe Harbor Under Fire in Europe," *POLITICO Morning Tech*, November 6, 2013, http://www.politico.com/morningtech/1113/morningtech12137.html (accessed July 25, 2014).
102. Taylor *et al.*, "NSA surveillance may cause breakup of Internet, warn experts."
103. *See, e.g.*, John Perry Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Frontier Foundation*, February 8, 1996, https://projects.eff.org/~barlow/Declaration-Final.html. Barlow addressed the document to "Governments of the Industrial World," declaring, "You have no sovereignty where we gather... Cyberspace does not lie within your borders."
104. *See, e.g.*, Kristina Irion, "Government Cloud Computing and National Data Sovereignty," *Social Science Research Network*, June 30, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1935859. *See also* Jonah Force Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business

Leaders," *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance*, May 1, 2014 (working paper), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2430275.

105. At a December 2012 summit of the International Telecommunications Union, for example, a block of countries including Russia, the United Arab Emirates, Algeria, Saudi Arabia, and Sudan, tried to define a new term called the "national Internet segment" that would have given countries full regulatory authority over the Internet within their borders (Russia, UAE, China, Saudi Arabia, Algeria, Sudan & Egypt, "Proposals for Work of the Conference at the World Conference on International Telecommunications," *International Telecommunications Union*, December 5, 2012, http://files.wcitleaks.org/public/Merged%20UAE%20081212.pdf). Iran has also been a vocal advocate of national routing and the creation of a "halal net" to keep communications within the country wherever possible (Christopher Rhoads and Farnaz Fassihi, "Iran Vows to Unplug Internet," *The Wall Street Journal*, May 28, 2011, http://online.wsj.com/news/articles/SB10001424052748704889404576277391449002016 [accessed July 25, 2014]).

106. Katherine Maher, "The New Westphalian Web," *Foreign Policy*, February 25, 2013, http://www.foreignpolicy.com/articles/2013/02/25/the_new_westphalian_web (accessed July 25, 2014).

107. Eugene Kaspersky, "What will happen if countries carve up the internet?" *The Guardian*, December 17, 2013, http://www.theguardian.com/media-network/media-network-blog/2013/dec/17/internet-fragmentation-eugene-kaspersky (accessed July 25, 2014).

108. *See case studies of 13 countries considering data localization proposals in* Anupam Chander and Uyen P. Le, "Breaking the Web: Data Localization vs. the Global Internet," *UC Davis School of Law Research Paper No. 378*, April 24, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858.

109. *Id.*

110. For more on types of data localization proposals, *see* Stephen D. Ezell, Robert D. Atkinson & Michelle Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy," *The Information Technology and Innovation Foundation*, September 25, 2013, at 18-23, http://www.itif.org/publications/localization-barriers-trade-threat-global-innovation-economy.

111. Arnaldo Galvao and Raymond Colitt, "Brazil May Require Google, Facebook to Store Data Locally," *Bloomberg News*, September 16, 2013, http://www.bloomberg.com/news/2013-09-17/brazil-may-require-google-facebook-to-store-data-locally.html (accessed July 25, 2014).

112. Ezell *et al.*, "Localization Barriers to Trade" at 18-19.

113. Mascolo and B. Scott, "Lessons from the Summer of Snowden" at 10.

114. *See, e.g.*, "Embassy Espionage: The NSA's Secret Spy Hub in Berlin," *Der Spiegel*, October 27, 2013, http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html (accessed July 25, 2014); Cameron Abadi, "The Betrayal of Angela Merkel: She loved America more than any other European leader. So why did the NSA target her?" *The New Republic*, November 2, 2013, http://www.newrepublic.com/article/115442/angela-merkel-spying-us-just-lost-very-good-friend (accessed July 25, 2014); Ian Traynor and Paul Lewis, "Merkel Compared NSA to Stasi in Heated Encounter with Obama," *The Guardian*, December 17, 2013, http://www.theguardian.com/world/2013/dec/17/merkel-compares-nsa-stasi-obama (accessed July 25, 2014).

115. Laura Smith-Spark, "Germany's Angela Merkel: Relations with U.S. 'severely shaken' over spying claims," *CNN*, October 24, 2013, http://www.cnn.com/2013/10/24/world/europe/europe-summit-nsa-surveillance/ (accessed July 25, 2014).

116. "Weighing a Schengen Zone for Europe's Internet Data," *Deutsche Welle*, February 20, 2014, http://www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482 (accessed July 25, 2014).

117. Jabeen Bhatti, "In Wake of PRISM, German DPAs Threaten to Halt Data Transfers to Non-EU Countries," *Bloomberg BNA*, July 29, 2013, http://www.bna.com/wake-prism-german-n17179875502/ (accessed July 25, 2014).

118. *Id.*

119. Obermaier and Strunz, "Germany Plans To Ban Tech Companies That Play Ball With NSA."

120. Mascolo and B. Scott, "Lessons from the Summer of Snowden" at 10.

121. Amar Toor, "Will the global NSA backlash break the Internet? Brazil and Germany make moves to protect online privacy, but experts see a troubling trend toward Balkanization," *The Verge*, November 8, 2013, http://www.theverge.com/2013/11/8/5080554/nsa-backlash-brazil-germany-raises-fears-of-internet-balkanization (accessed July 25, 2014). *See also* M. Scott, "European Firms Turn Privacy into Sales Pitch."

122. J. Hill, "The Growth of Data Localization Post-Snowden" at 8.

123. Leila Abboud and Peter Maushagen, "Germany wants a German Internet as spying scandal rankles," *Reuters*, October 25, 2013, http://www.reuters.com/article/2013/10/25/us-usa-spying-germany-idUSBRE99O09S20131025 (accessed July 25, 2014). See also Mascolo and B. Scott, "Lessons from the Summer of Snowden" at 10.

124. Hattem, "Tech Takes Hit from NSA."

125. Sandeep Joshi, "India to push for freeing Internet from US control," *The Hindu*, December 7, 2013, http://www.thehindu.com/sci-tech/technology/internet/article5434095.ece (accessed July 25, 2014).

126. R. Jai Krishna, "India Sees Resolution to Blackberry Dispute," *The Wall Street Journal*, August 8, 2012, http://online.wsj.com/news/articles/SB10000872396390443404004577576614174157698 (accessed July 25, 2014).

127. Reported in Joshi, "India to push for freeing Internet from US control."

128. Ezell *et al.*, "Localization Barriers to Trade" at 18-9.

129. Chander and Le, "Breaking the Web: Data Localization vs. the Global Internet" at 19.

130. "Avoiding NSA Clutches: India to launch internal email policy for govt comms," *RT*, October 31, 2013, http://rt.com/news/india-nsa-internal-email-994/ (accessed July 25, 2014).

131. Taylor *et al.*, "NSA surveillance may cause breakup of Internet, warn experts."

132. Carolina Rossini, "Internet and Statecraft: Brazil and the Future of Internet Governance," *New America Foundation's Open Technology Institute*, October

2, 2013, http://oti.newamerica.net/blogposts/2013/internet_and_statecraft_brazil_and_the_future_of_internet_governance-93553 (accessed July 25, 2014).

133. Bill Woodcock, "On Internet, Brazil is Beating US at its own game," *Al Jazeera America*, September 20, 2013, http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html (accessed July 25, 2014).

134. J. Hill, "The Growth of Data Localizaton Post-Snowden" at 12.

135. Ian Brown, "Will NSA revelations lead to the Balkanisation of the internet?" *The Guardian*, November 1, 2013, http://www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet (accessed July 25, 2014). *See also* Chander and Le, "Breaking the Web" at 6.

136. Quoted in Michael Hickens, "American Spying Stymies Tech Firms," *The Wall Street Journal*, February 18, 2014, http://online.wsj.com/news/articles/SB10001424052702303743604579350611848246016 (accessed July 25, 2014).

137. "Brazil presses EU for undersea cable to skirt US links," *Reuters*, February 24, 2014, http://www.reuters.com/article/2014/02/24/eu-brazil-idUSL6N0LP43G20140224 (accessed July 25, 2014). Currently, there is one cable that connects Brazil to Europe without routing through the United States: the Atlantis-2 (or II) cable. It links up with Argentina, Senegal, Cape Verde, and the Canary Islands en route to Portugal and is used primarily for telephony (Spilios E. Makris, Nick Lordi & Malvin G. Linnell," Potential Role of Brazil's Undersea Cable Infrastructure for the FIFA 2014 World Cup & the Rio 2016 Olympic Games: Background, Observations, and Considerations," *Institute of Electrical and Electronics Engineers*, June 9, 2010, http://www.ieee-cqr.org/2010/Day%202/Session%207/3_Spilios_Makris%20FIFAMAKRIS%20-%202014_2016_Olympics_presentation_version.pdf). The new cable, which would cost a reported $185 million and have much higher bandwidth, is scheduled to begin construction in July ("Brazil presses EU For progress on undersea cable to circumvent US spying.").

138. For an in-depth discussion of the impact of such proposals, *see* a forthcoming publication from New America's Open Technology Institute and the Global Public Policy Institute assessing the implications of European technological sovereignty proposals (to be published fall 2014). More information about the Transatlantic Dialogues on Security and Freedom in the Digital Age project is *available at* http://www.digitaldebates.org/.

139. Hilmar Schmundt and Gerald Traufetter, "Digital Independence Boosts German Tech Industry," *Der Spiegel*, February 4, 2014, http://www.spiegel.de/international/business/german-it-industry-looks-for-boom-from-snowden-revelations-a-950786.html (accessed July 25, 2014).

140. In an interview in April 2014, De Maiziere was asked about what it means that Cisco and Huawei, an American and Chinese company, respectively, produce a huge percentage of Internet infrastructure equipment worldwide. He said: "We are a country with open borders in the middle of Europe. To think we could be self-contained in any way, we can forget that. On the other hand, we should ask ourselves whether a country of our size requires a modicum of self-monitoring and independence... The chancellor and, for example, the foreign minister, need to be able to have a conversation that is secure enough that no foreign country can listen to it. We can't be dependent on an industry that, in the worst case, is working together, in this area, with a different country." (Jörg Schindler, Alfred Weinzierl & Peter Müller, "German Minister: 'US Operating Without Any Kind of Boundaries,'" *Der Spiegel*, April 9, 2014, http://www.spiegel.de/international/germany/german-interior-minister-warns-us-spying-has-no-boundaries-a-963179.html [accessed July 25, 2014].)

141. Melody Patry, "Brazil: A new global Internet referee?" *Index on Censorship*, June 2014, http://www.indexoncensorship.org/wp-content/uploads/2014/06/brazil-internet-freedom_web_en.pdf at 21-22. In the spring of 2014, the Brazilian government walked back from some of its more controversial post-Snowden declarations and took critical steps to ensure the passage of the Marco Civil da Internet, Brazil's "Internet bill of rights," which had faced an uphill battle toward passage since it was drafted through a collaborative process in 2009 and 2010. Many observers at NETMundial noted that Brazil embraced a more multistakeholder approach to Internet governance than it had at the 2012 World Conference on International Telecommunications.

142. "Brazilian President Pursues Server Localization Policies," *White & Case*, January 2014, http://www.whitecase.com/alerts-01082014-2/#.U2PRyq1dW4o.

143. Anthony Boadle, "Brazil to drop local data storage rule in Internet bill," *Reuters*, March 18, 2014, http://www.reuters.com/article/2014/03/19/us-brazil-internet-idUSBREA2I03O20140319 (accessed July 25, 2014).

144. J. Hill, "The Growth of Data Localization Post-Snowden" at 13. Article 11 of the Marco Civil states that "Any process of collection, storage, custody and treatment of records, personal data or communications by connection providers and Internet applications providers, in which at least one of these acts occurs in the national territory, shall respect Brazilian law, the rights to Privacy, and the confidentiality of personal data, of private communications and records."

145. Bruno Favero, "Governo nao desistiu de data centers no Brasil, diz Paulo Bernardo," *Folha de S. Paulo*, April 23, 2014, http://www1.folha.uol.com.br/tec/2014/04/1444381-governo-nao-desistiu-de-data-centers-no-brasil-diz-paulo-bernardo.shtml (accessed July 25, 2014) (in Portuguese).

146. J. Hill writes that "powerful business interests undoubtedly see data localization as an effective and convenient strategy for gaining a competitive advantage in domestic IT markets long dominated by U.S. tech firms. To localization proponents of this stripe, the NSA programs serve as a powerful and politically expedient excuse to pursue policies protective of domestic business." (J. Hill, "The Growth of Data Localization Post-Snowden" at 19.)

147. J. Hill, "The Growth of Data Localization Post-Snowden" at 11.

148. "Progress on EU data protection reform now irreversible following European Parliament vote," *European Commission*, March 12, 2014, http://europa.eu/rapid/press-release_MEMO-14-186_en.htm (accessed July 25, 2014).

149. Meyer, "Web firms face a strict new set of privacy rules in Europe—here's what to expect."

150. Glyn Moody, "US-EU Relations After Two Important Votes in European Parliament: It's (More) Complicated)," *TechDirt*, March 14, 2014, http://

www.techdirt.com/articles/20140314/09113926578/us-eu-relations-after-two-important-votes-european-parliament-its-more-complicated.shtml (accessed July 25, 2014).

151. "Progress on EU data protection reform now irreversible following European Parliament vote."

152. "NSA Snooping: MEPs table proposals to protect EU citizens' privacy," *European Parliament*, February 12, 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20140210IPR35501%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN (accessed July 25, 2014).

153. Byers, "Tech Safe Harbor Under Fire in Europe."

154. Stephen Gardner, "Irish Referral of U.S.-EU Safe Harbor to ECJ May Raise Issues on All Adequacy Regimes," *Bloomberg BNA*, June 23, 2014, http://www.bna.com/irish-referral-useu-n17179891493/ (accessed July 25, 2014).

155. Moody, "US-EU Relations After Two Important Votes in European Parliament."

156. Patrizia Simone, Estelle Masse & Raegan MacDonald, "EP adopts the Data Protection Reform Package," *Access*, March 12, 2014, https://www.accessnow.org/blog/2014/03/12/ep-adopts-the-data-protection-reform-package (accessed July 25, 2014); Kenneth Page, "How privacy-friendly is the new European Parliament?" *Privacy International*, June 24, 2014, https://www.privacyinternational.org/blog/how-privacy-friendly-is-the-new-european-parliament (accessed July 25, 2014).

157. Hakim, "Europe Aims to Regulate the Cloud."

158. "Top News – EU Progress on Data Protection," *Electronic Privacy Information Center*, June 9, 2014, http://epic.org/privacy/intl/eu_data_protection_directive.html (accessed July 25, 2014). "The agreement to force Internet companies such as Google and Facebook to abide by EU-wide rules is a first step in a wider reform package to tighten privacy laws – an issue that has gained prominence following revelations of U.S. spying in Europe." (Julia Fioretti, "EU says firms like Google and Facebook must meet privacy rules," *Reuters*, June 6, 2014, http://www.reuters.com/article/2014/06/06/us-eu-dataprotection-idUSKBN0EH1ER20140606 [accessed July 25, 2014].)

159. Brandom, "Microsoft offers overseas data in response to NSA concerns." Notably, the question of whether that tradition of U.S. government access to extraterritorially-stored data still holds is currently the subject of litigation, as Microsoft is challenging a recent U.S. court ruling requiring it to hand over emails stored in one of its Irish data centers based on a federal search warrant. *See* Ellen Nakashima, "Microsoft fights U.S. search warrant for customer e-mails held in overseas server," *The Washington Post*, June 10 2014, http://www.washingtonpost.com/world/national-security/microsoft-fights-us-search-warrant-for-customer-e-mails-held-in-overseas-server/2014/06/10/6b8416ae-f0a7-11e3-914c-1fbd0614e2d4_story.html (accessed July 25, 2014). Case documents, including friend-of-the-court briefs from supporters of the effort such as the Electronic Frontier Foundation and AT&T, are *available at* https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland.

160. Daniel Castro, "The False Promise of Data Nationalism," *The Information Technology and Innovation Foundation*, December 2013, http://www2.itif.org/2013-false-promise-data-nationalism.pdf (accessed July 25, 2014). *See also* J. Hill, "The Growth of Data Localization Post-Snowden."

161. According to a White Paper from Hogan Lovells, "On the fundamental question of governmental access to data in the Cloud, we conclude… that it is not possible to isolate data in the Cloud from governmental access based on the physical location of the Cloud service provider or its facilities. Governmental access to data in the Cloud is ubiquitous, and extends across borders… In addition to governmental access to data within its borders, Mutual Legal Assistance Treaties (MLATs), which are in effect between and among countries around the world, can provide access to data stored in one jurisdiction but needed for lawful investigative purposes in another. Despite the procedural hurdles that may exist to request and obtain information pursuant to MLATs, these treaties make borders and the physical location of data less significant in terms of where a Cloud service provider is located… We conclude that civil rights and privacy protections related to governmental access to data in the Cloud are not significantly stronger or weaker in any one jurisdiction, and that any perceived locational advantage of stored Cloud data can be rendered irrelevant by MLATs. Our review reveals that businesses are misleading themselves and their customers if they contend that restricting Cloud service providers to one jurisdiction better insulates data from government access." (Winton Maxwell and Christopher Wolf, "A Global Reality: Governmental Access to Data in the Cloud," *Hogan Lovells*, May 2012, http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf at 2-3). In contrast, the U.S. government has argued in its litigation with Microsoft that even assuming that an MLAT treaty is in place with the relevant country, an MLAT request "typically takes months to process," and that a provider could—"for legitimate or illegitimate reasons"—effectively prevent access to a user's account by distributing the user's data across servers based in dozens of countries. Full text of the brief for the Southern District of NY District Court is *available at* http://cdn.arstechnica.net/wp-content/uploads/2014/07/federalbrief-microsoftcase.pdf.

162. Esteban Israel and Alonso Soto, "Brazil's anti-spying Internet push could backfire, industry says," *Reuters*, October 2, 2013, http://www.reuters.com/article/2013/10/02/us-brazil-internet-idUSBRE9910F120131002 (accessed July 25, 2014).

163. Claire Cain Miller, "Google Pushes Back Against Data Localization," *The New York Times*, January 24, 2014, http://mobile.nytimes.com/blogs/bits/2014/01/24/google-pushes-back-against-data-localization/ (accessed July 25, 2014).

164. Mascolo and B. Scott explain that "if a European government passed a law that Internet service providers operating in their countries are forbidden to pass data to US law enforcement, they place these companies in a contradiction. They are still American companies and subject to US law. In these circumstances, they cannot be in compliance with the law in both countries… The same contradiction applies for any country that would pass laws to govern the companies governed outside their control." (Mascolo and B. Scott, "Lessons from the Summer of Snowden" at 8.)

165. When he appeared before the Senate Judiciary Committee in December 2013, Computer and Communications Industry Association President and CEO Ed Black testified about the degree to which U.S. economic prosperity is threatened by excessive

Internet surveillance and argued that if the US ignores international concerns related to digital trade it will do serious damage to U.S. competitiveness. (Heather Greenfield, "CCIA Praises Surveillance Reform Plans at Senate Judiciary Hearing," *Computer and Communications Industry Association*, December 11, 2013, https://www.ccianet.org/blog/2013/12/ccia-praises-surveillance-reform-plans-senate-judiciary-hearing-2/.)

166. Hickens, "American Spying Stymies Tech Firms."

167. Harris, "Don't Gerrymander the Internet."

168. Mascolo and B. Scott, "Lessons from the Summer of Snowden" at 12. *See also* Alexander Plaum, "The impact of forced data localisation on fundamental rights," *Access*, June 4, 2014, https://www.accessnow.org/blog/2014/06/04/the-impact-of-forced-data-localisation-on-fundamental-rights.

169. J. Hill, "The Growth of Data Localization Post-Snowden" at 2.

170. Danielle Kehl and Hibah Hussain, "The New Digital Dark Side," *New America Foundation*, May 13, 2013, http://inthetank.newamerica.net/blog/2013/05/new-digital-dark-side (accessed July 25, 2014).

171. Ron Deibert, "Why NSA Spying Scares the World," *CNN*, June 12, 2013, http://www.cnn.com/2013/06/12/opinion/deibert-nsa-surveillance/ (accessed July 25, 2014).

172. Henry Farrell and Martha Finnemore, "The End of Hypocrisy: American Foreign Policy in the Age of Leaks," *Foreign Affairs*, November/December 2013, http://www.foreignaffairs.com/articles/140155/henry-farrell-and-martha-finnemore/the-end-of-hypocrisy (accessed July 25, 2014). *See also* the response to this piece, Michael A. Cohen, "Hypocrisy Hype: Can Washington Still Walk and Talk Differently?" *Foreign Affairs*, March/April 2014, http://www.foreignaffairs.com/articles/140760/michael-a-cohen-henry-farrell-and-martha-finnemore/hypocrisy-hype (accessed July 25, 2014).

173. *See, e.g.*, Joey Cheng, "US 'tremendously' damaged by Snowden disclosures," *Defense Systems*, May 13, 2014, http://defensesystems.com/articles/2014/05/13/fose-donilon-cyber-threats-snowden-damage.aspx (accessed July 25, 2014); Kasia Klimasinska and Raymond Collitt, "Lew Seeks to Repair Brazil Ties in Latin America Trip," *Bloomberg*, March 18, 2014, http://www.bloomberg.com/news/2014-03-18/lew-seeks-to-repair-brazil-ties-in-latin-america-trip.html (accessed July 25, 2014); Harriet Torry, "U.S. and Germany Signal Willingness to Repair Strained Relations," *The Wall Street Journal*, January 31, 2014, http://online.wsj.com/news/articles/SB10001424052702304428004579354432652898774 (accessed July 25, 2014).

174. Editorial Board, "The U.S. needs to adjust its policy toward spying on allies," *The Washington Post*, October 22, 2013, http://www.washingtonpost.com/opinions/the-us-needs-to-adjust-its-policy-toward-spying-on-allies/2013/10/22/e431e978-3b35-11e3-b6a9-da62c264f40e_story.html (accessed July 25, 2014).

175. Remarks of Secretary of State Hillary Clinton, "Remarks on Internet Freedom," *U.S. Department of State,* January 21, 2010, http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm (accessed July 25, 2014).

176. Remarks of Secretary of State Hillary Clinton, "Internet Rights and Wrongs: Choices and Challenges in a Networked World," *U.S. Department of State*, February 15, 2011, http://blogs.state.gov/stories/2011/02/15/internet-rights-and-wrongs-choices-and-challenges-networked-world (accessed July 25, 2014).

177. Richard Fontaine and Will Rogers, "Internet Freedom: A Foreign Policy Imperative in the Digital Age," *Center for a New American Security*, June 2011 at 9, http://www.cnas.org/files/documents/publications/CNAS_InternetFreedom_FontaineRogers_0.pdf. Fontaine and Rogers describe two "linked but distinct concepts" in Internet Freedom: freedom of the Internet, which "denotes the freedoms of online expression, assembly and association – the extension to cyberspace of rights that have been widely recognized to exist outside it" and freedom via the Internet, "the notion that new communications technologies aid the establishment of democracy and liberal society offline."

178. Cecilia Kang, "Hillary Clinton calls for Web freedom, demands China investigate Google attack," *The Washington Post*, January 22, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/21/AR2010012101699.html (accessed July 25, 2014) ("'One of big questions around the speech is 'To what degree are we willing to hold ourselves to these standards?' said Clay Shirky, a new media professor at New York University.").

179. Fontaine and Rogers, "Internet Freedom" at 19-32. More recently, *see* Scott Busby, "10 Things You Need to Know About U.S. Support for Internet Freedom," *IIP Digital*, May 29, 2014, http://iipdigital.usembassy.gov/st/english/article/2014/05/20140530300596.html#axzz32vEtH3C9 (accessed July 25, 2014).

180. See "Internet Freedom" *Humanrights.gov*, n.d., http://www.humanrights.gov/issues/internet-freedom/ (accessed July 25, 2014).

181. For more information, *see* "Internet Freedom," *U.S. Department of State*, n.d., http://www.state.gov/e/eb/cip/netfreedom/index.htm (accessed July 25, 2014).

182. Ben FitzGerald and Robert Butler, "NSA revelations: Fallout can serve our nation," *Reuters*, December 18, 2013, http://blogs.reuters.com/great-debate/2013/12/18/nsa-revelations-fallout-can-serve-our-nation/ (accessed July 25, 2014).

183. Danielle Kehl and Tim Maurer, "Did the UN Internet Governance Summit Actually Accomplish Anything?" *Slate*, December 14, 2012, http://www.slate.com/blogs/future_tense/2012/12/14/wcit_2012_has_ended_did_the_u_n_internet_governance_summit_accomplish_anything.html (accessed July 25, 2014).

184. "Internet regulation: A digital Cold War?" *The Economist*, December 14, 2012, http://www.economist.com/blogs/babbage/2012/12/internet-regulation (accessed July 25, 2014); Larry Downes, "Requiem for Failed UN Telecom Treaty: No One Mourns the WCIT," *Forbes*, December 17, 2012, http://www.forbes.com/sites/larrydownes/2012/12/17/no-one-mourns-the-wcit/ (accessed July 25, 2014); Eli Dourado, "Behind closed doors at the UN's attempted 'takeover of the Internet,'" *Ars Technica*, December 20, 2012, http://arstechnica.com/tech-policy/2012/12/behind-closed-doors-at-the-uns-attempted-takeover-of-the-internet/ (accessed July 25, 2014). For a more in-depth analysis of shifting diplomatic coalitions since the WCIT, *see* Tim Maurer and Robert Morgus, "Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate," Centre for International Governance Innovation, May 2014, http://www.cigionline.org/publications/tipping-scale-analysis-of-global-swing-states-internet-governance-debate.

185. Dourado, "Behind closed doors at the UN's attempted 'takeover of the Internet.'"
186. Emma Llanso, "WTPF: Successful Outcome, but Many Questions Remain," *Center for Democracy and Technology*, May 17, 2013, https://cdt.org/blog/wtpf-successful-outcome-but-many-questions-remain/ (accessed July 25, 2014).
187. "Freedom Online Coalition 2013: Tunis Conference Themes," *Freedom Online Coalition* 17 & 18 June 2013, Tunis: Joint Action for Free Expression on the Internet, n.d., http://freedomonline.tn/Fr/themes_11_59 (accessed July 25, 2014).
188. Jillian C. York, "Freedom Online Coalition Takes on Surveillance, PRISM in Tunisia," *PBS*, June 25, 2013, http://www.pbs.org/mediashift/2013/06/freedom-online-coalition-takes-surveillance-prism-tunisia/ (accessed July 25, 2014).
189. Eli Dourado, "So much for America's internet freedom agenda," *The Guardian*, August 7, 2013, http://www.theguardian.com/commentisfree/2013/aug/07/nsa-surveillance-alienating-us-from-world (accessed July 25, 2014).
190. *Id.*
191. Matthew Shears, "Snowden and the Politics of Internet Governance," *Center for Democracy and Technology*, February 21, 2014, https://cdt.org/snowden-and-the-politics-of-internet-governance/ (accessed July 25, 2014).
192. Deborah Brown, "UN Human Rights Council discusses surveillance and other internet issues at 24th session," *Access*, September 16, 2013, https://www.accessnow.org/blog/2013/09/16/un-human-rights-council-discusses-surveillance-and-other-internet-issues-at (accessed July 25, 2014).
193. Taylor *et al.*, "NSA surveillance may cause breakup of the internet, warn experts."
194. Milton Mueller, "Do the NSA Revelations Have Anything to Do With Internet Governance?" *Internet Governance Project*, February 19, 2014, http://www.internetgovernance.org/2014/02/19/do-the-nsa-revelations-have-anything-to-do-with-internet-governance/ (accessed July 25, 2014).
195. "Montevideo Statement on the Future of Internet Cooperation," *Internet Corporation for Assigned Names and Numbers*, October 7, 2013, https://www.icann.org/en/news/announcements/announcement-07oct13-en.htm (accessed July 25, 2014).
196. "Internationalization and Regional Development," *Internet Corporation for Assigned Names and Numbers*, n.d., https://www.icann.org/en/about/planning/strategic-engagement/intreg-development (accessed July 25, 2014).
197. "IANA Functions and Related Root Zone Management Transition Questions and Answers," *National Telecommunications and Information Association*, March 18, 2014, http://www.ntia.doc.gov/other-publication/2014/iana-functions-and-related-root-zone-management-transition-questions-and-answ (accessed July 25, 2014).
198. Natalie Green and Carolina Rossini, "A Real Step? The Future of ICANN and How to Support It." *New America Foundation's Open Technology Institute*, March 21, 2014, http://oti.newamerica.net/blogposts/2014/a_real_step_the_future_of_icann_and_how_to_support_it-105990 (accessed July 25, 2014).
199. Scott Busby, "State Department on Internet Freedom at RightsCon," *Humanrights.gov*, March 4, 2014, http://www.humanrights.gov/2014/03/04/state-department-on-internet-freedom-at-rightscon/ (accessed July 25, 2014).
200. Access Policy Team, "U.S. State Department announces six principles to guide signals intelligence," *Access*, March 4, 2014, https://www.accessnow.org/blog/2014/03/04/dos-odni-announce-six-principles-to-guide-signals-intelligence (accessed July 25, 2014).
201. "International Principles on the Application of Human Rights to Communications Surveillance," *Necessary and Proportionate*, July 10, 2013, https://en.necessaryandproportionate.org/text (accessed July 25, 2014).
202. Carly Nyst, "Sweden's Foreign Minister declares his support for principles to protect privacy in the face of surveillance," *Privacy International*, October 21, 2013, https://www.privacyinternational.org/blog/swedens-foreign-minister-declares-his-support-for-principles-to-protect-privacy-in-the-face-of (accessed July 25, 2014).
203. For more on the work that the U.S. State Department supports to promote Internet Freedom abroad, *see* "Advancing Freedom and Democracy Report," *U.S. Department of State*, 2013, http://www.state.gov/j/drl/rls/afdr/2013/index.htm (accessed July 25, 2014). The report describes both the types of work that the State Department supports as well as the countries in which they operate.
204. Cynthia Wong, "Global internet freedom begins at home," *Index on Censorship*, June 21, 2011, http://www.indexoncensorship.org/2011/06/global-internet-freedom-begins-at-home/ (accessed July 25, 2014).
205. Sana Saleem, "A year after Snowden revelations, damage persists to freedom of expression in Pakistan," *Committee to Protect Journalists*, June 16, 2014, https://www.cpj.org/blog/2014/06/a-year-after-snowden-revelations-damage-persists-t.php (accessed July 25, 2014).
206. *Id.* Sana Saleem is a director of Bolo Bhi, an Internet rights group based in Pakistan. In conversations during the course of research for this paper, numerous other digital rights activists working for organizations located around this world indicated that they faced similar challenges when advocating for Internet Freedom and digital rights in the past year.
207. "USA: NSA symbolises intelligence services' abuses," *Reporters Without Borders*, March 12, 2014, http://12mars.rsf.org/2014-en/2014/03/11/usa-nsa-symbolises-intelligence-services-abuses/ (accessed July 25, 2014). *See* the full "Enemies of the Internet Report" *available at* http://12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf (accessed July 25, 2014).
208. *See, e.g.*, discussion of the "Snowden Effect" in "Global Opposition to U.S. Surveillance and Drones, But Limited Harm to America's Image," *Pew Research Center*, July 14, 2014, http://www.pewglobal.org/files/2014/07/2014-07-14-Balance-of-Power.pdf (accessed July 25, 2014).
209. Wong, "Global internet freedom begins at home." *See also* "Joint Letter from Civil Society Organizations to Foreign Ministers of Freedom Online Coalition Member States," *Open the Government*, April 28, 2014, http://www.openthegovernment.org/node/4436 (accessed July 25, 2014).
210. "Egypt, citing security, wants foreign companies to

help monitor social media," *Reuters*, June 2, 2014, http://uk.reuters.com/article/2014/06/02/uk-egypt-media-idUKKBN0ED1ED20140602 (accessed July 25, 2014); Summer Said, "Egyptians Slam Government Plan to Monitor Social Media," *The Wall Street Journal*, June 3, 2014, http://blogs.wsj.com/middleeast/2014/06/03/egyptians-slam-government-plan-to-monitor-social-media/ (accessed July 25, 2014); "Egypt's plan for mass surveillance of social media an attack on internet privacy and freedom of expression," Amnesty International, June 4, 2014, http://www.amnesty.org/en/news/egypt-s-attack-internet-privacy-tightens-noose-freedom-expression-2014-06-04 (accessed July 25, 2014).

211. Quoted in "#BBCtrending: 'We are being watched' say Egyptians on social media," *BBC News*, June 2, 2014, http://www.bbc.com/news/blogs-trending-27665568 (accessed July 25, 2014).

212. Jayshree Bajoria, "India's Snooping and Snowden," *The Wall Street Journal*, June 5, 2014, http://blogs.wsj.com/indiarealtime/2014/06/05/indias-snooping-and-snowden/ (accessed July 25, 2014).

213. Andy Greenberg, "U.S. Indictment of Chinese Hackers Could Be Awkward for the NSA," *Wired*, May 19, 2014, http://www.wired.com/2014/05/us-indictments-of-chinese-military-hackers-could-be-awkward-for-nsa/ (accessed July 25, 2014). *See also* Michael Kan, "U.S.-China tech exchange shows strain after hacking accusations," *ComputerWorld*, May 23, 2014, http://www.computerworld.com/s/article/9248543/U.S._China_tech_exchange_shows_strains_after_hacking_accusations (accessed July 25, 2014).

214. Ian Bremmer, "Lost Legitimacy: Why governing is harder than ever," *Foreign Affairs*, November 1, 2013, http://www.foreignaffairs.com/articles/140274/ian-bremmer/lost-legitimacy (accessed July 25, 2014).

215. Mascolo and B. Scott, "Lessons from the Summer of Snowden" at 3.

216. Robert Nolan, "5 Undeniable Fallouts from the Edward Snowden Leaks," *US News and World Report*, September 20, 2013, http://www.usnews.com/opinion/blogs/world-report/2013/09/20/brazil-russia-and-the-impact-of-edward-snowden-on-us-foreign-relations (accessed July 25, 2014).

217. Dmitry Minin, "The Strategic Consequences of the Edward Snowden Revelations," *Strategic Culture Foundation*, January 17, 2014, http://www.strategic-culture.org/news/2014/01/17/strategic-consequences-edward-snowdens-revelations-i.html and http://www.strategic-culture.org/news/2014/01/19/the-strategic-consequences-of-edward-snowdens-revelations-ii.html (accessed July 25, 2014).

218. "France, Germany at odds on delaying US trade talks," *The Nation*, July 4, 2013, http://www.nation.com.pk/international/04-Jul-2013/france-germany-at-odds-on-delaying-eu-us-trade-talks (accessed July 25, 2014).

219. David E. Sanger, "US and Germany Fail to Reach a Deal on Spying," *The New York Times*, May 2, 2014, http://www.nytimes.com/2014/05/02/world/europe/us-and-germany-fail-to-reach-a-deal-on-spying.html?ref=todayspaper (accessed July 25, 2014).

220. Mark Landler, "Merkel Signals That Tension Persists Over U.S. Spying," *The New York Times*, May 2, 2014, http://www.nytimes.com/2014/05/03/world/europe/merkel-says-gaps-with-us-over-surveillance-remain.html (accessed July 25, 2014).

221. Paul Lewis, "US and Germany remain frosty amid awkward visit from Merkel," *The Guardian*, May 2, 2014, http://www.theguardian.com/world/2014/may/02/us-germany-frosty-awkward-visit-merkel-nsa (accessed July 25, 2014).

222. Anthony Faiola, "Germany Opens Hearings on U.S. Spying," *The Washington Post*, April 3, 2014, http://www.washingtonpost.com/world/germany-opens-hearings-on-us-spying/2014/04/03/cf58f2d0-b42b-4e59-a403-75f968d6edb0_story.html (accessed July 25, 2014).

223. Heather Arnet, "Why Dilma Cancelled on Obama," *The Daily Beast*, October 23, 2013, http://www.thedailybeast.com/witw/articles/2013/10/23/dilma-rousseff-and-the-state-visit-that-didn-t-happen.html (accessed July 25, 2014).

224. "Statement by the Press Secretary on Postponement of the State Visit of President Dilma Rousseff of Brazil," *The White House*, September 17, 2013, http://www.whitehouse.gov/the-press-office/2013/09/17/statement-press-secretary-postponement-state-visit-president-dilma-rouss (accessed July 25, 2014).

225. Bruce Schneier, "The Only Way to Restore Trust in the NSA," *The Atlantic*, September 4, 2013, http://www.theatlantic.com/politics/archive/2013/09/the-only-way-to-restore-trust-in-the-nsa/279314/ (accessed July 25, 2014).

226. Bruce Schneier, "NSA Secrets Kill our Trust," *CNN*, July 31, 2013, http://www.cnn.com/2013/07/31/opinion/schneier-nsa-trust/index.html (accessed July 25, 2014).

227. Joseph Stiglitz, "In No One We Trust," *The New York Times*, December 21, 2013 http://opinionator.blogs.nytimes.com/2013/12/21/in-no-one-we-trust/?_php=true&_type=blogs&_r=0 (accessed July 25, 2014).

228. *See, e.g.*, Jennifer Golbeck, "Weaving a Web of Trust," *Science* Vol 321: September 19, 2008 (1640).

229. *See, e.g.*, Keith Devlin, "The NSA: A Betrayal of Trust," *Notices of the American Mathematical Society*, June/July 2014, http://www.ams.org/notices/201406/rnoti-p623.pdf at 624-626.

230. *See* "New Harris Poll Shows NSA Revelations Impact Online Shopping, Banking, and More." The Electronic Frontier Foundation's April Glaser writes, "Without trustworthy encryption, safe business transactions are impossible and speech is chilled." (April Glaser, "After NSA Backdoors, Security Experts Leave RSA for a Conference They Can Trust," *Electronic Frontier Foundation*, January 30, 2014, https://www.eff.org/deeplinks/2014/01/after-nsa-backdoors-security-experts-leave-rsa-conference-they-can-trust.). There is already evidence that NSA surveillance may produce a number of chilling effects that influence the way individuals around the world use the Internet. *See, e.g.,* "EFF Files 22 Firsthand Accounts of How NSA Surveillance Chilled the Right to Association," *Electronic Frontier Foundation*, November 6, 2013, https://www.eff.org/press/releases/eff-files-22-firsthand-accounts-how-nsa-surveillance-chilled-right-association (accessed July 25, 2014); "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor," *Pen American Center*, November 12, 2013, http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf; Alex Pasternak, "In Our Own Google Searches, Researchers See a Post-Snowden Chilling Effect," *Motherboard*, May 5, 2014, http://motherboard.vice.com/read/

nsa-chilling-effect (accessed July 25, 2014); April Glaser, "17 Student Groups Pen Open Letters on the Toxicity of Mass Surveillance to Academic Freedom," *Electronic Frontier Foundation*, June 9, 2014, https://www.eff.org/deeplinks/2014/06/students-against-surveillance-17-university-groups-pen-open-letters-toxicity-mass (accessed July 25, 2014).

231. Brendan Sasso, "The NSA Isn't Just Spying On Us, It's Also Undermining Internet Security," *National Journal*, April 29, 2014, http://www.nationaljournal.com/daily/the-nsa-isn-t-just-spying-on-us-it-s-also-undermining-internet-security-20140429 (accessed July 25, 2014).

232. John Markoff, "Electronics Plan Aims to Balance Government Access with Privacy," *The New York Times*, April 16, 1993, http://www.nytimes.com/1993/04/16/us/electronics-plan-aims-to-balance-government-access-with-privacy.html (accessed July 25, 2014). *See also* Steven Levy, "Battle of the Clipper Chip," *The New York Times*, June 12, 2014, http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html (accessed July 25, 2014).

233. *Id.*

234. Daniel Castro, "Guest column: Has the US government learned nothing from the Clipper Chip?" *Fedscoop*, September 11, 2013, http://fedscoop.com/guest-column-has-us-government-learned-nothing/#st-hash.8SkaOHLU.dpuf (accessed July 25, 2014).

235. "By introducing such back doors, the N.S.A. has surreptitiously accomplished what it had failed to do in the open. Two decades ago, officials grew concerned about the spread of strong encryption software like Pretty Good Privacy, designed by a programmer named Phil Zimmermann. The Clinton administration fought back by proposing the Clipper Chip, which would have effectively neutered digital encryption by ensuring that the N.S.A. always had the key... That proposal met a backlash from an unlikely coalition that included political opposites like Senator John Ashcroft, the Missouri Republican, and Senator John Kerry, the Massachusetts Democrat, as well as the televangelist Pat Robertson, Silicon Valley executives and the American Civil Liberties Union. All argued that the Clipper would kill not only the Fourth Amendment, but also America's global technology edge... By 1996, the White House backed down." (Perlroth *et al.*, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web.")

236. Quoted in Perlroth *et al.*, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web."

237. Kevin Poulsen, "New Snowden Leak Reports 'Groundbreaking' NSA Crypto Cracking," *Wired*, August 29, 2013, http://www.wired.com/2013/08/black-budget/ (accessed July 25, 2014).

238. Barton Gellman and Greg Miller, "U.S. spy network's successes, failures and objectives detailed in 'black budget' summary," *The Washington Post*, August 29, 2013, http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html?tid=pm_world_pop (accessed July 25, 2014).

239. "About NIST," *National Institute for Standards and Technology*, last modified July 18, 2013, http://www.nist.gov/public_affairs/nandyou.cfm (accessed July 25, 2014).

240. Quoted in Rachel King, "NSA's Involvement in Standards Setting Erodes Trust," *Wall Street Journal*, October 1, 2013, http://blogs.wsj.com/cio/2013/10/01/nsas-involvement-in-standards-setting-erodes-trust/ (accessed July 25, 2014).

241. James Ball, Julian Border & Glenn Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security" *The Guardian*, September 5, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (accessed July 25, 2014).

242. Perlroth *et al.*, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web."

243. Levy, "Battle of the Clipper Chip." It is important to note that although RSA was founded as an independent company, it was acquired by EMC Corporation in 2006 and now operates as a division within EMC ("EMC Completes RSA Security Acquisition, Announces Acquisition of Network Intelligence," *EMC,* September 18, 2006, http://www.emc.com/about/news/press/us/2006/09182006-4605.htm).

244. Dan Goodin, "Stop using NSA-influenced code in our products, RSA tells customers," *Ars Technica*, September 19, 2013, http://arstechnica.com/security/2013/09/stop-using-nsa-influence-code-in-our-product-rsa-tells-customers/ (accessed July 25, 2014).

245. Danny Yadron, "RSA: Don't Use Encryption Influenced by the NSA," *Wall Street Journal*, September 19, 2013, http://stream.wsj.com/story/latest-headlines/SS-2-63399/SS-2-332655/ (accessed July 25, 2014).

246. Goodin, "Stop using NSA-influenced code in our products, RSA tells customers."

247. Joseph Menn, "Exclusive: Secret contract tied NSA and security industry pioneer," *Reuters*, December 20, 2013, http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220 (accessed July 25, 2014).

248. Matthew Green, "On the NSA," *A Few Thoughts on Cryptographic Engineering*, September 5, 2013, http://blog.cryptographyengineering.com/2013/09/on-nsa.html (accessed July 25, 2014).

249. Sasso, "The NSA Isn't Just Spying On Us, It's Also Undermining Internet Security." As Edward Felten noted in his assessment as part of the report and recommendations in the independent NIST review conducted in the summer of 2014, "The bottom line is that NIST failed to exercise independent judgment but instead deferred extensively to NSA with regard to DUAL_EC. After DUAL_EC was proposed, two major red flags emerged. Either one should have caused NIST to remove DUAL_EC from the standard, but in both cases NIST deferred to NSA requests to keep DUAL_EC." He adds, however, "Although the cryptographic community believes... that at least one NIST standard contained a trapdoor, the community also believes that NIST did not want such a trapdoor and did not knowingly allow it. The community believes that NIST is trying to produce secure standards; and the community is willing to be convinced over time that NIST has taken the necessary steps to protect more effectively against subversion of its standards and processes." (Edward Felten, "NIST Cryptographic Standards and Guidelines Development Process: Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology," *National Institute of Standards and Technology*, July 2014, http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf.)

250. King, "NSA's Involvement in Standards Setting Erodes Trust."
251. Larry Greenemeier, "NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard," *Scientific American*, September 18, 2013, http://www.scientificamerican.com/article/nsa-nist-encryption-scandal/ (accessed July 25, 2014).
252. "Risking It All: Unlocking the Backdoor to the Nation's Cybersecurity," *Institute of Electrical and Electronics Engineers*, 2014 at 6, http://users.ece.cmu.edu/~peha/IEEE_Peha_Camp_Risking_It_All.pdf.
253. *Id.* at 6.
254. "Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology" at 42.
255. Sasso, The NSA Isn't Just Spying On Us, It's Also Undermining Internet Security."
256. "NIST's Cryptographic Material Under Review," *Help Net Security*, May 15, 2014, http://www.net-security.org/secworld.php?id=16861 (accessed July 25, 2014).
257. "Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology." *See also* Joseph Menn, "Experts report potential software 'back door' in U.S. standards," *Reuters*, July 14, 2014, http://www.reuters.com/article/2014/07/15/usa-nsa-software-idUSL2N0PP2BM20140715 (accessed July 25, 2014).
258. "Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology."
259. *Id.* at 69-71.
260. Justin Elliott, "House Committee Puts NSA on Notice Over Encryption Standards," *ProPublica*, May 23, 2014, https://www.propublica.org/article/house-committee-nsa-nist-encryption-standards (accessed July 25, 2014). *See also* Amie Stepanovitch, "Congressional Committee Adopts Amendment to Remove NSA From Crypto Standards Process," *Access*, May 21, 2014, https://www.accessnow.org/blog/2014/05/21/congressional-committee-adopts-amendment-to-remove-nsa-from-crypto-standard (accessed July 25, 2014).
261. Justin Elliott, "House Adopts Amendment to Bar NSA From Meddling With Encryption Standards," *ProPublica*, June 20, 2014, http://www.propublica.org/article/house-adopts-amendment-to-bar-nsa-from-meddling-with-encryption-standards (accessed July 25, 2014).
262. "SIGINT Enabling Project," *ProPublica*, https://www.propublica.org/documents/item/784285-sigint-enabling-project.html (accessed July 25, 2014).
263. *Id.*
264. *Id.*
265. Bruce Schneier, "NSA Surveillance: A Guide to Staying Secure," *The Guardian*, September 6, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance (accessed July 25, 2014).
266. "NSA/CSS Commercial Solutions Center (NCSC)," *National Security Agency Central Security Service*, July 18, 2011, http://www.nsa.gov/business/programs/ncsc.shtml.
267. Ball *et al.*, "Revealed: how US and UK spy agencies defeat internet privacy and security."
268. *Id.*
269. Glenn Greenwald, Ewan MacAskill, Laura Poitras, Spencer Ackerman, and Dominic Rushe, "Microsoft handed the NSA access to encrypted messages," *The Guardian*, July 11, 2013, http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (accessed July 25, 2014).
270. "Statement from Microsoft about response to government demands for customer data," *Microsoft*, July 11, 2013, http://www.microsoft.com/en-us/news/press/2013/jul13/07-11statement.aspx (accessed July 25, 2014). ("To be clear, Microsoft does not provide any government with blanket or direct access to SkyDrive, Outlook.com, Skype or any Microsoft product.") *See also* Doug Aamoth, "Microsoft's Response to NSA Backdoor Allegations: It's Not True. It's Also Complicated. We Can't Explain It, but We Wish We Could," *TIME*, July 12, 2013, http://techland.time.com/2013/07/12/microsofts-response-to-nsa-backdoor-allegations-its-not-true-its-also-complicated-we-cant-explain-it-but-we-wish-we-could/ (accessed July 25, 2014).
271. Don Clark and Danny Yadron, "Greenwald: NSA Plants 'Backdoors' in Foreign-Bound Routers," *Wall Street Journal*, May 12, 2014, http://blogs.wsj.com/digits/2014/05/12/greenwald-nsa-plants-backdoors-in-foreign-bound-routers/ (accessed July 25, 2014).
272. Hesseldahl, "In Letter to Obama, Cisco CEO Complains About NSA Allegations."
273. Mark Chandler, "Internet Security Necessary for Global Technology Economy," *Cisco Blog*, May 13, 2014, http://blogs.cisco.com/news/internet-security-necessary-for-global-technology-economy (accessed July 25, 2014).
274. "SIGINT Enabling Project."
275. Ball *et al.*, "Revealed: how US and UK spy agencies defeat internet privacy and security."
276. Stephanie Pell, "Jonesing for a Privacy Mandate, Getting a Technology Fix – Doctrine to Follow," *Stanford Law School Center for Internet and Society*, May 8, 2013 at 45, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2262397.
277. Statement of Dr. Susan Landau, "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 2," 2011, http://judiciary.house.gov/hearings/pdf/Landau02172011.pdf (accessed July 25, 2014).
278. Pell, "Jonesing for a Privacy Mandate" at 45-46.
279. Perlroth *et al.*, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web."
280. Steven M. Bellovin, Matt Blaze, Sandy Clark & Susan Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," *Northwestern Journal of Technology and Intellectual Property*, April 2014, http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip, at 19-20. *See also* "Risking It All: Unlocking the Backdoor to the Nation's Cybersecurity" at 4-5; Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair," *IEEE SPECTRUM*, July 2007 at 27, http://spectrum.ieee.org/telecom/security/the-athens-affair/0 (which describes how unauthorized actors used built-in lawful intercept capabilities in phone network

equipment to spy on the cell phone call of high Greek officials, including the Prime Minister); Ellen Nakashima, "Chinese hackers who breached Google gained access to sensitive data, U.S. officials say," *The Washington Post*, May 20, 2013 (which describes how Chinese hackers targeted systems used by Google and Microsoft to administer lawful intercepts in order to identify targets of surveillance for counterintelligence purposes).

281. "Risking It All: Unlocking the Backdoor to the Nation's Cybersecurity" at 8.
282. Michael Riley, "NSA Said to Exploit Heartbleed Bug for Intelligence for Years," *Bloomberg*, April 12, 2014, http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html (accessed July 25, 2014).
283. Julian Sanchez, "The NSA's heartbleed problem is the problem with the NSA," *The Guardian*, April 12, 2014, http://www.theguardian.com/commentisfree/2014/apr/12/the-nsas-heartbleed-problem-is-the-problem-with-the-nsa (accessed July 25, 2014).
284. Bruce Schneier, "Should Hackers Fix Cybersecurity Holes or Exploit Them?" *The Atlantic*, May 19, 2014, http://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197/ (accessed July 25, 2014).
285. Spiegel Staff, "Inside TAO: Documents Reveal Top NSA Hacking Unit."
286. Bellovin *et al.*, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet" at 42.
287. Liam Tung, "NSA: Our zero days put you at risk, but we do what we like with them," *ZDNet*, March 13, 2014, http://www.zdnet.com/nsa-our-zero-days-put-you-at-risk-but-we-do-what-we-like-with-them-7000027296/ (accessed July 25, 2014). According to one report from July 2013, "The black market in previously undiscovered vulnerabilities in commercial software is now so established, the average flaw sells for up to $160,000." (Warwick Ashford, "Black market for software security flaws reaches new highs," *Computer Weekly,* July 15, 2013, http://www.computerweekly.com/news/2240188014/Black-market-for-software-security-flaws-reaches-new-highs [accessed July 25, 2014].)
288. Riley, "NSA Said to Exploit Heartbleed Bug for Intelligence for Years."
289. Bellovin *et al.*, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet" at 23.
290. David E. Sanger, "Obama Let N.S.A. Exploit Some Internet Flaws, Officials Say," *The New York Times*, April 12, 2014, http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html (accessed July 25, 2014).
291. *Id.*
292. Bellovin *et al.*, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet" at 52.
293. Jacob Appelbaum, Judith Horchert & Christian Stöcker, "Shopping for Spy Gear: Catalog Advertises NSA Toolbox," *Der Spiegel*, December 29, 2013, http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html (accessed July 25, 2014).
294. Press Release, Office of the Director of National Intelligence Public Affairs Office, "Statement on Bloomberg News story that NSA knew about the 'Heartbleed bug' flaw and regularly used it to gather critical intelligence," April 11, 2014, available at http://icontherecord.tumblr.com/post/82416436703/statement-on-bloomberg-news-story-that-nsa-knew (accessed July 25, 2014).
295. Tung, "NSA: Our zero days put you at risk, but we do what we like with them."
296. "Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command," *Senate Armed Services Committee*, March 11, 2014, http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf (accessed July 25, 2014).
297. Schneier, "Should Hackers Fix Cybersecurity Holes or Exploit Them?"
298. Michael Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities," *The White House Blog*, April 28, 2014, http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities (accessed July 25, 2014).
299. Josh Gerstein, "White House Denies NSA-'Heartbleed' Link," *Politico*, April 11, 2014, http://www.politico.com/story/2014/04/heartbleed-nsa-white-house-105644.html (accessed July 25, 2014).
300. Robyn Greene, "The Cybersecurity Information Sharing Act of 2014: A Major Step Back on Privacy," *New America Foundation's Open Technology Institute*, June 23, 2014, http://oti.newamerica.net/blogposts/2014/the_cybersecurity_information_sharing_act_of_2014_a_major_step_back_on_privacy-115051 (accessed July 25, 2014).
301. "Liberty and Security in a Changing World" at 219.
302. *Id.* at 220.
303. Bellovin *et al.,* "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet" at 52. Although the focus of the paper is on domestic law enforcement and proposals to update the Communications Assistance for Law Enforcement Act (CALEA) to mandate that companies include back-doors for lawful intercept capability, there is significant overlap with what the NSA does. The authors explain, "In considering whether to report a vulnerability, law enforcement should consider how dangerous a particular vulnerability may be. Sometimes this question will be very easy to answer. If the vulnerability is in a network router or switch, its impact is likely to be very large. Indeed, vulnerabilities in network infrastructure are fundamentally a national security risk because network devices are either ISP-grade gear, whose compromise could be used to shut down or tap a large portion of the network; enterprise gear, whose compromise could be used for targeted espionage attacks; or consumer gear, likely to be in wide use and thus the compromise could effect a large population. Without question, such vulnerabilities should be reported to the vendor immediately."
304. Spiegel Staff, "Inside TAO: Documents Reveal Top NSA Hacking Unit."
305. Matthew M. Aid, "Inside the NSA's Ultra-Secret China Hacking Group," *Foreign Policy*, June 10, 2013, http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group (accessed July 25, 2014).
306. Schneier, "NSA Surveillance: A Guide to Staying Secure."

307. Spiegel Staff, "Inside TAO: Documents Reveal Top NSA Hacking Unit."
308. Gellman and Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say."
309. Perlroth *et al.*, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web."
310. James Ball, Bruce Schneier & Glenn Greenwald, "NSA and GCHQ target Tor network that protects anonymity of web users," *The Guardian*, October 4, 2013, http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption (accessed July 25, 2014).
311. "Tor: Overview," *The Tor Project*, n.d., https://www.torproject.org/about/overview.html.en (accessed July 25, 2014).
312. Ball *et al.*, "NSA and GCHQ target Tor network that protects anonymity of web users."
313. Bruce Schneier, "Attacking Tor: how the NSA targets users' online anonymity," *The Guardian*, October 4, 2013, http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity (accessed July 25, 2014).
314. Ball *et al.*, "NSA and GCHQ target Tor network that protects anonymity of web users." On its website, the Tor project lists active sponsors that include the U.S. Department of States Bureau of Democracy, Human Rights, and Labor, the National Science Foundation, and Radio Free Asia (a private non-profit funded by the Broadcasting Board of Governors). ("Tor: Sponsors," *The Tor Project*, n.d. https://www.torproject.org/about/sponsors.html.en.)
315. Spiegel Staff, "Inside TAO: Documents Reveal Top NSA Hacking Unit."
316. *Id.*
317. Ryan Gallagher and Glenn Greenwald, "How the NSA Plans to Infect 'Millions' of Computers with Malware," *The Intercept*, March 12, 2014, https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/ (accessed July 25, 2014).
318. Salvador Rodriguez, "NSA posed as Facebook to infect computers with malware, report says," *Los Angeles Times*, March 12, 2014, http://www.latimes.com/business/technology/la-fi-tn-nsa-posing-facebook-malware-20140312-story.html (accessed July 25, 2014); Cyrus Farivar, "UK spies continue 'quantum insert' attack via LinkedIn, Slashdot pages," *Ars Technica*, November 10, 2013, http://arstechnica.com/tech-policy/2013/11/uk-spies-continue-quantum-insert-attack-via-linkedin-slashdot-pages/ (accessed July 25, 2014); Edward Moyer, "NSA disguised itself as Google to spy, say reports," *CNET*, September 12, 2013, http://www.cnet.com/news/nsa-disguised-itself-as-google-to-spy-say-reports/ (accessed July 25, 2014).
319. Aleksei Oreskovic, "Facebook CEO Zuckerberg phoned Obama to complain about spying," *Reuters*, March 13, 2014, http://www.reuters.com/article/2014/03/13/us-facebook-obama-idUSBREA2C27920140313 (accessed July 25, 2014).
320. Mark Zuckerberg, Facebook post, March 13, 2014, https://www.facebook.com/zuck/posts/10101301165605491 (accessed July 25, 2014).
321. Gallagher and Greenwald, "How the NSA Plans to Infect 'Millions' of Computers with Malware."
322. "Liberty and Security in a Changing World" at 47-8.
323. *Id.* at 48.
324. *Id.* at 155.
325. Tye, "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans." ("A member of the review group confirmed to me that this reference [to "any other authority"] was written deliberately to include Executive Order 12333.")
326. "Liberty and Security in a Changing World" at 29-30.
327. "The Right to Privacy in the Digital Age," *Report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/27/37 at 12, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.
328. S. 1599 and H.R. 3361, USA FREEDOM Act, 113th Congress (2013), as introduced, § 101, at https://beta.congress.gov/113/bills/s1599/BILLS-113s1599is.pdf and https://beta.congress.gov/113/bills/hr3361/BILLS-113hr3361ih.pdf.
329. S. 1599 and H.R. 3361, USA FREEDOM Act, 113th Congress (2013), as introduced, Title III.
330. H.R. 3361, USA FREEDOM Act, 113th Congress (2014), as engrossed in House, https://beta.congress.gov/113/bills/hr3361/BILLS-113hr3361eh.pdf. *See also* Kevin Bankston, "The Weakened USA FREEDOM Act," *New America's Open Technology Institute*, May 21, 2014, http://oti.newamerica.net/blogposts/2014/the_weakened_usa_freedom_act-111071 (accessed July 25, 2014).
331. *See* "'We Need to Know' Coalition Letter," July 18, 2013, available at https://www.cdt.org/files/pdfs/weneedtoknow-transparency-letter.pdf, and "CDT Brings Together Major Internet Companies & Advocates To Demand More Transparency Around Government Surveillance," *Center for Democracy and Technology*, July 17, 2013, https://cdt.org/press/cdt-brings-together-major-internet-companies-advocates-to-demand-more-transparency-around-government-surveillance/ (accessed July 25, 2014).
332. "'We Need to Know' Coalition Letter."
333. "'We Need to Know' Coalition Letter."
334. "Coalition of Major Internet Companies and Advocates Rallies Around Surveillance Transparency Legislation," *Center for Democracy and Technology*, September 29, 2013, https://cdt.org/press/coalition-of-major-internet-companies-and-advocates-rallies-around-surveillance-transparency-legislation/ (accessed July 25, 2014); The Hill Staff, "Tech giants ask Congress to move quickly on NSA transparency bills," *The Hill*, September 30, 2013, http://thehill.com/policy/technology/325477-tech-giants-ask-congress-to-move-quickly-on-nsa-transparency-bills (accessed July 25, 2014).
335. "Liberty and Security in a Changing World" at 26-28.
336. "The Right to Privacy in the Digital Age" at 16. The report emphasizes the "disturbing lack of governmental transparency associated with surveillance policies, laws and practices, which hinders any effort to assess their coherence with international human rights law and to ensure accountability."
337. H.R. 3361, USA FREEDOM Act, 113th Congress (2014), as engrossed in House, https://beta.congress.gov/113/bills/hr3361/BILLS-113hr3361eh.pdf.
338. Mieke Eoyang, "To judge NSA reforms, look to the tech industry," *The Boston Globe,* January 17, 2014, http://www.bostonglobe.com/opinion/2014/01/17/

podium-nsa/yycYzE4ajKl8NGFU1YYEgN/story.html (accessed July 25, 2014).

339. Shears, "Snowden and the Politics of Internet Governance."

340. For more information about the 2014 Internet Governance Forum, which will be held in Turkey in September 2014, *see* http://www.intgovforum.org/cms/. The ITU plenipotentiary meeting will consider the future role of the organization in South Korea in October and November 2014, with information *available at* http://www.itu.int/en/plenipotentiary/2014/Pages/default.aspx. For more on the WSIS+10 review, *see* http://www.internetsociety.org/wsis/isoc-participation-2013-wsis-forum-and-wsis10-review/wsis10-review-phase-ii-2014.

341. Fontaine and Rogers, "Internet Freedom" at 13.

342. At the 2013 Freedom Online Coalition meeting in Tunis, members decided to established "three multistakeholder working groups to strengthen continuous cooperation towards practical outcomes on key issues of concern to Internet freedom and human rights," which are now being developed. For more information, *see* "Freedom Online Coalition: Working Groups," n.d., https://www.freedomonlinecoalition.com/how-we-work/working-groups/.

343. "Remarks by the President of Estonia, Mr Toomas Hendrik Ilves," *Freedom Online Coalition Conference*, April 28, 2014, available at http://www.freedomonline.ee/node/131.

344. Global Network Initiative, "About Us," n.d., https://www.globalnetworkinitiative.org/about/index.php.

345. "Liberty and Security in a Changing World" at 216.

346. *Id.* at 36.

347. *See* assessment of Edward W. Felten in "Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology." Felten writes, "NIST standards provide the greatest benefits to the American people, American industry, and the U.S. government when those standards are adopted widely. If users have confidence in NIST standards, technology vendors are more likely to adopt NIST standards, thereby ensuring that U.S. government agencies, which are required to follow NIST standards, will be able to adopt the most popular technologies and products. A bifurcated world in which the U.S. government uses NIST standards and everyone else uses different standards would be worse for everybody and would prevent government agencies from using Commercial Off-the-Shelf technologies and frustrate interoperation between government and non-government systems" (26). *See also* "Risking It All: Unlocking the Backdoor to the Nation's Cybersecurity" at 5-8.

348. Elliott, "House Committee Puts NSA on Notice Over Encryption Standards."

349. "Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology."

350. Elliott, "House Adopts Amendment to Bar NSA From Meddling With Encryption Standards."

351. The Cryptographic Technology Group, "NIST Cryptographic Standards and Guidelines Development Process (Draft)," *National Institute of Science and Technology Standards*, February 2014, http://csrc.nist.gov/publications/drafts/nistir-7977/nistir_7977_draft.pdf.

352. "NIST Cryptographic Standards and Guidelines Development Process" at 1.

353. "Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology," summarized at 3-4.

354. "Letter In the Matter of NIST Cryptographic Standards and Guidelines Development Process NIST IR 7977 (Draft)," submitted by Access, Advocacy for Principled Action in Government, Competitive Enterprise Institute, Electronic Frontier Foundation, Electronic Privacy Information Center, Fight for the Future, New America Foundation's Open Technology Institute, OpentheGovernment.org, Silent Circle, Student Net Alliance, Sunlight Foundation, TechFreedom, April 18, 2014, available at https://s3.amazonaws.com/access.3cdn.net/73934b6b48cbc48268_oim6bx0jn.pdf (accessed July 25, 2014).

355. "IETF Policy on Wiretapping," *The Internet Society*, May 2000, http://tools.ietf.org/pdf/rfc2804.pdf.

356. Ben Adida, Collin Anderson, Annie I. Anton, Matt Blaze, Roger Dingledine, Edward W. Felten, Matthew D. Green, J. Alex Halderman, David R. Jefferson, Cullen Jennings, Susan Landau, Navroop Mitter, Peter G. Neumann, Eric Rescorla, Fred B. Schneider, Bruce Schneier, Hovav Shacham, Micah Sherr, David Wagner, and Philip Zimmerman, "CALEA II: Risks of Wiretap Modifications to Endpoints," *Center for Democracy and Technology*, May 17, 2013 at 2, https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf.

357. Adida *et al.*, "CALEA II: Risks of Wiretap Modifications to Endpoints" at 7.

358. Declan McCullagh, "FBI: We need wiretap-ready Web sites—now," *CNET*, May 4, 2012, http://www.cnet.com/news/fbi-we-need-wiretap-ready-web-sites-now/ (accessed July 25, 2014); Ellen Nakashima, "Proliferation of new online communications services poses hurdles for law enforcement," *The Washington Post*, July 26, 2014, http://www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2_story.html (accessed July 25, 2014).

359. Bellovin *et al.*, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet" at 17-9.

360. Mike Masnick, "Amendments Offered To NDAA To Try To Stop NSA Surveillance Abuse," *TechDirt*, May 21, 2014, http://www.techdirt.com/articles/20140520/18283127298/amendments-offered-to-ndaa-to-try-to-stop-nsa-surveillance-abuse.shtml (accessed July 25, 2014).

361. Amendment to the Rules Committee Print for H.R. 4435, Offered by Ms. Lofgren of California, May 2014, http://amendments-rules.house.gov/amendments/LOFGRE_056519141329382938.pdf.

362. "OTI Joins With Privacy Groups and Tech Companies To Tell Congress: End the NSA's Backdoor Access to Internet Users' Data," *New America Foundation*, June 18, 2014, http://newamerica.net/node/114440 (accessed July 25, 2014).

363. Ellen Nakashima and Andrea Peterson, "House votes to curb NSA 'backdoor' U.S. data searches," *The Washington Post*, June 20, 2014, http://www.washingtonpost.com/world/national-security/house-votes-to-curb-nsa-backdoor-us-data-searches/2014/06/20/54aacd28-f882-11e3-a3a5-

42be35962a52_story.html (accessed July 25, 2014).

364. Bellovin *et al.*, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet" at 54. They go on to note that disclosing a vulnerability does not prevent intelligence or law enforcement agencies from exploiting that vulnerability until it is patched. Instead, "it will create a situation in which law enforcement is both performing criminal investigations using the wiretaps enabled through exploits, and crime prevention through reporting the exploits to the vendor," which they describe as a "win-win" scenario.

365. "Liberty and Security in a Changing World" at 37.

366. *Id.*

367. 18 U.S.C. §1030(a) (generally prohibiting unauthorized access, or access in excess of authority, to a protected computer); §1030(e)(2)(b): defining a "protected computer" under the law to include "a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States"; §1030(f) ("This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.").

368. Nathan Freed Wessler, "DOJ Proposal on Law Enforcement Hacking Would Undermine Longstanding Check on Government Power," *American Civil Liberties Union's Free Future Blog*, May 9, 2014, https://www.aclu.org/blog/national-security/doj-proposal-law-enforcement-hacking-would-undermine-longstanding-check (accessed July 25, 2014).

369. Jon M. Peha, "The Dangerous Policy of Weakening Security to Facilitate Surveillance," *Social Science Research Network*, Oct. 4, 2013, http://ssrn.com/abstract=2350929.

370. Sanchez, "The NSA's Heartbleed problem is the problem with the NSA."

371. "Liberty and Security in a Changing World" at 189.

372. *Id.* at 34 (Recommendations #23, 24, and 25).

373. *Id.* at 191.

374. *Id.* at 193 ("In an ideal world, IAD could form the core of the cyber capability of DHS."); Schneier, "It's time to break up the NSA."

New America's Open Technology Institute
1899 L Street, NW
Suite 400
Washington DC 20036
Phone 202 986 2700
Fax 202 986 3696

oti.newamerica.org