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

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 around NSA surveillance 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 of the NSA's programs more broadly. This short briefing paper summarizes a report from the Open Technology Institute analyzing the impact of those programs on the U.S. economy, American foreign policy, and the security of the Internet as a whole. The full paper, "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity" quantifies and categorizes the costs of the NSA surveillance programs since the initial leaks were reported in June 2013.

I. 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... The economic consequences could be staggering."*
> *-Mieke Eoyang and Gabriel Horowitz,* Forbes*, December 2013*

Costs to the Cloud Computing and Web Hosting Industries

Trust in American businesses has decreased 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.[1] Given heightened concern about the NSA's ability to access data stored by U.S. companies, American companies that offer cloud computing and webhosting services are experiencing the most acute economic fallout. Nearly 50 percent of worldwide cloud computing revenue comes from the United States, and the domestic market more than tripled in value from 2008 to 2014.[2] However, within weeks of the first revelation, reports began to emerge that American cloud computing companies like Dropbox and Amazon Web Services were losing business to overseas competitors.[3] The NSA's PRISM program is predicted to cost the cloud computing industry from $22 to $180 billion over the next three years.[4]

Recent reports suggest that those predictions may soon be borne out. A January 2014 survey of 300 British and Canadian businesses found that 25 percent of respondents were moving their data outside of the U.S. and that an overwhelming majority was willing to sacrifice performance in order to ensure data protection.[5] Similarly, a survey of 1000 "ICT decision-makers" from France, Germany, Hong Kong, the UK, and the U.S. conducted 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."[6]

Cost to Overseas Tech Sales

The economic impact of NSA spying does not end with the American cloud computing industry. In the past year, a number of American companies have reported declining sales in overseas markets, loss of customers, and increased competition from non-U.S. services marketing themselves as "secure" alternatives to popular American products. In November 2013, Cisco became one of the first companies to publicly discuss the negative impact of the NSA on its business.[7] Qualcomm, IBM, Microsoft, and Hewlett-Packard have all reported that sales are down in China as a result of the NSA revelations,[8] and industry observers have questioned whether companies like Apple and AT&T will face increased scrutiny in overseas business.[9] Servint, a Virginia-based webhosting company, reported in June 2014 that international

By Danielle Kehl

with Kevin Bankston, Robyn Greene & Robert Morgus

OPEN TECHNOLOGY INSTITUTE

clients have declined by as much as half, dropping from approximately 60 percent of its business to 30 percent since the leaks began.[10]

The NSA disclosures are putting a variety of U.S. companies at a disadvantage. For example, German companies that are increasingly uncomfortable giving business to American firms are excluding American businesses from some requests for proposals.[11] The German government announced in June 2014 that it intends to end its contract with Verizon, which provides Internet service to a number of government departments, in response to that company's cooperation with the NSA.[12] The NSA has also 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.[13] Meanwhile, the marketing of foreign information technology 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 America's tech competitiveness.[14]

SURVEILLANCE COSTS?
According to an April 2014 Harris poll, nearly half of the 2000 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. In particular, 26 percent indicated that they are now doing less online shopping and banking since learning the extent of government surveillance programs.[18]

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. Some companies have tried to regain trust by publicly stating that they are not part of PRISM or other NSA programs, while others that have been directly linked to the NSA programs have publicly criticized the U.S. government's handling of the issue and called for greater transparency.[15] The CEOs of nine major American companies joined together in the "Reform Government Surveillance" campaign advocating for surveillance reform.[16] Other companies have gone one step further, developing new products or taking additional precautions, like encrypting their traffic or offering overseas data storage, to assure customers that their data is safe from the NSA.[17]

II. Economic and Technological Costs of Data Localization and Data Protection Proposals

> *""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 summer of Snowden, but the debate has become significantly more complex in the past year.[19] The NSA disclosures appear to have given ammunition to proponents of greater national control of traffic and network infrastructure, accelerating the number and scope of data localization and national routing proposals intending to limit the amount of global Internet traffic and data that passes through or is stored in the U.S.[20] Now, more than a dozen countries, including Germany, Brazil, and India, have introduced or are actively discussing data localization laws, which would prevent or limit information flows.[21]

In Germany, local leaders and Chancellor Angela Merkel have called for data localization to protect against NSA spying. Deutsche Telekom has promised to keep communications within the country to address the privacy concerns of German users[22] and has been a vocal proponent of a "Schengen routing" network for data traveling between the 26 EU countries of the Schengen Zone.[23] Brazil has proposed that Internet companies like Facebook and Google must set up local data centers in order to bind them by Brazilian privacy laws.[24] And the Indian government has floated a draft policy that 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 the country.[25] Greece, Brunei, and Vietnam have also put forth their

own data sovereignty proposals.[26]

It is unclear how viable these data localization proposals are in the short term, but they have set the stage for serious challenges in the long run. Until now, most foreign countries accepted America's comparative advantage in the technology industry, but the threat of NSA surveillance may be the catalyst that pushes countries to invest heavily in technology sectors that they would otherwise have left to the U.S., including cloud computing and data storage.

Data Protection Proposals and the Cost to European Trade Relations

A number of countries are also proposing stricter domestic privacy regulations in response to NSA snooping. In March 2014, members of the European Parliament passed the Data Protection Regulation and Directive, which imposes strict limitations on the handling of EU citizens' data.[27] The rules, which apply to the processing of EU citizens' data no matter where it is located, require individuals to consent to having their personal data processed, and retain the right to withdraw their consent once given. The deterrent fines are significant: violators face a maximum penalty of up to five percent of revenues, which could translate to billions of dollars for large tech companies.

A resolution from the Civil Liberties, Justice and Home Affairs Committee of the European Parliament also 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.[28] Over 3000 American companies, including Facebook and Google, currently rely on the Safe Harbor framework to process European data without violating the continent's privacy laws.[29] As local and European officials become increasingly concerned that this arrangement makes it easier for U.S. tech companies to sidestep the EU's stricter privacy protections, they appear less inclined to maintain the agreement. These actions are a component of a shift in EU policy away from the favorable digital trade relationship the United States has enjoyed.

Combined Costs of Data Localization and Data Protection

The Information Technology and Innovation Fund predict that data privacy rules and other restrictions could slow the growth of the U.S. technology-services industry by as much as four percent.[30] These challenges could prevent American firms from expanding, or force them to pull out of existing markets, because of the high cost of complying with stricter rules and the need for duplicative server infrastructure in countries with localization requirements.[31] Data localization proposals also threaten 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. Finally, the localization of Internet traffic may 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.

III. Political Costs to U.S. Foreign Policy

> *"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,* CNN*, June 2013*

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

The NSA disclosures have undermined American credibility in the Internet governance debate in the past year. Since 2010, the American government has successfully built a policy and programming agenda promoting an open and free Internet,[32] but the NSA disclosures have led many to question the legitimacy of these efforts in the past year.[33]

NSA surveillance shifted the dynamics of the Internet governance debate and emboldened those who seek to discard existing multistakeholder approaches to Internet governance in favor of a new, government-centric governance system.[34] Concrete evidence of U.S. surveillance hardened the positions of authoritarian governments pushing for greater national control over the Internet and revived proposals from both Russia and Brazil for multilateral management of technical standards and

domain names, whether through the International Telecommunications Union (ITU) or other avenues. Developing countries, many of which traditionally aligned with the U.S. and prioritized access and affordability, have begun to decline U.S. assistance and are "walking straight into the arms of Russia, China, and the ITU."[35] In September 2013, the representative from Pakistan, speaking on behalf of many others at the UN Human Rights Council, explicitly linked the NSA disclosures to the need for Internet governance reform that would give governments a larger role.[36]

Many of the institutions that govern the technical functions of the Internet are connected to the U.S. government or located in the United States, but the disclosures have substantially weakened the U.S.'s status as a neutral steward of the Internet. As a result, in October 2013, heads of a number of key organizations responsible for coordination of the Internet's technical infrastructure issued the Montevideo Statement, which expressed concern over the loss of trust in the U.S. and called for accelerating the globalization of the ICANN and IANA functions allowing equal participation for all stakeholders.[37]

Costs to Internet Freedom Beyond Governance

The loss of trust in the United States as a legitimate advocate for Internet Freedom and the growing perception that the U.S. Internet Freedom agenda is hypocritical has made it harder for civil society around the world to advocate for Internet Freedom within their own governments.[38] For some of these groups, even the appearance of collaboration with or support from the U.S. government can diminish their credibility, making it harder for them to advocate locally for changes that align with U.S. foreign policy interests.[39] For individuals and organizations with U.S. government funded expression activities or projects, the gap in trust is significant as technology supported by or exported from the United States is considered inherently suspect.

The moral high ground that the United States relies upon when publicly pressuring authoritarian countries like China, Russia, and Iran to change their behavior has eroded. The damaged perception of the United States as a leader on Internet Freedom[40] and its diminished ability to legitimately criticize other countries for censorship and surveillance allows foreign leaders to justify and even expand their own efforts. Foreign governments and their populations are now wary not just of the United States government and companies, but of technology more generally.

Broader Foreign Policy Costs

The revelations have also strained bilateral relations with U.S. allies. German Chancellor Angela Merkel refused to visit the United States for months following the revelations, and when she finally agreed to come, the visit was tense and awkward.[41] Brazilian President Dilma Rousseff has also 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 to not attend an October 2013 meeting with President Barack Obama at the White House was a direct response to NSA spying and marked the first time a world leader had turned down a state dinner with the President of the United States.[42]

IV. Costs to Cybersecurity

> *""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 Atlantic*, September 2013*

The bulk of the controversy in the past year has been focused on the NSA's programs to collect phone records and monitor Internet communications, but the NSA is also engaged in a wide variety of conduct that fundamentally threatens the basic security of the Internet.

Compromising Security Standards

The NSA worked covertly to weaken key cryptographic security standards issued by the National Institute of Standards and Technology in 2006, taking advantage of NIST's statutory obligation to consult with the NSA on certain guidelines.[43] The algorithm was included in the

cryptographic libraries of major tech companies[44] for almost a decade due to a government contracting requirement.[45] A few days after the compromised standard was revealed, RSA Security alerted its customers that a cryptography component in several of its products used the specification by default – a default that was set as the result of a $10 million contract with the NSA.[46]

Creating Security Vulnerabilities

The NSA spends $250 million a year to develop relationships with companies in order to weaken standards and build backdoors into their products. The SIGINT Enabling project leverages partnerships with U.S. and foreign IT companies to insert vulnerabilities into commercial encryption systems, IT networks, and communications devices.[47] The NSA also uses its Commercial Solutions center, the program that offers technology companies an opportunity to have their security products assessed and presented to prospective government buyers, to leverage relationships and insert vulnerabilities into those security tools.[48] Additional reports suggest that the NSA worked with Microsoft to circumvent the encryption on popular services including Skype, Outlook, and SkyDrive, and that the agency planted backdoors in foreign-bound Cisco routers without the company's knowledge.[49]

Withholding Security Vulnerabilities

The NSA routinely stockpiles knowledge about security holes (known as zero-days) so that it can later exploit those vulnerabilities, rather than disclosing the flaws to companies so that they can be patched.[50] This leaves companies and ordinary users open to attack not only from the NSA, but also from anyone who discovers the weaknesses. The NSA and related branches of the U.S. intelligence community spend millions of dollars and employ over a thousand researchers looking for such zero-day exploits targeting everything from the commercial software sold by American companies to widely used open-source protocols like OpenSSL.[51] Though the White House claims that there is an existing interagency process designed to facilitate the responsible disclosure of vulnerabilities, it is unclear to what extent the NSA has participated in that process.

Hacking the Internet

When the NSA cannot gain access through other means, the agency relies on a more aggressive set of tools. Much of this is done through an elite group known as the Tailored Access Operations unit, whose employees specialize in Computer Network Exploitation to "subvert endpoint devices" such as computers, routers, phones, servers, and SCADA systems.[52] One tactic for scooping up vast amounts of data is to target networks and network providers, including the undersea fiber optic cables that carry global Internet traffic from one continent to another. The NSA successfully tapped the SEA-ME-WE-4 cable system connecting Europe to the Middle East and North Africa, as well as the fiber optic links connecting Google and Facebook data centers outside of the United States.[53] The Agency also deploys its "QUANTUMTHEORY" toolbox in a variety of ways to insert malware on to target computers.[54] One QUANTUM tactic is to impersonate major companies like LinkedIn and Facebook and redirect traffic to the NSA's own servers to obtain access to sensitive information or insert malware.[55]

For a more in-depth analysis of these costs, see the full paper:

"Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity," *New America's Open Technology Institute*, July 2014, *available at* http://oti.newamerica.net/publications/policy/surveillance_costs_the_nsas_impact_on_the_economy_internet_freedom_cybersecurity.

Recommendations

The U.S. government has already taken limited steps to mitigate this damage and begin the process of rebuilding trust in the United States as a responsible steward of the Internet. However, much more work remains. We recommend that the U.S. government should:

1 Strengthen privacy protections for both Americans and non-Americans, within the U.S. and extraterritorially. The NSA's mass surveillance under to Patriot Act Section 215 and Section 702 of the FISA Amendments Act have had the most immediate impact on consumer trust in the American tech industry. Narrowing the scope of collection under these authorities, as well as limiting the manner in which the collected information is retained, used, and disseminated, will be critical to regaining the trust of governments, companies, and individuals around the world.

2 Provide for increased transparency around government surveillance, both from governments and companies. Increased transparency is critical to rebuilding the trust that has been lost in the wake of the disclosures about the NSA's surveillance activities. In July 2013, a coalition of large Internet companies and advocacy groups came together to call for greater transparency, urging the U.S. government to issue its own transparency reports and to allow companies to disclose as much as possible about the volume and nature of the requests they receive from the NSA.

3 Recommit to the Internet Freedom agenda in a way that directly addresses issues raised by NSA surveillance. The U.S. must move proactively to reestablish the credibility of the Internet Freedom agenda. The State Department and NTIA have taken initial steps to demonstrate goodwill in this area, but it will take a broader effort from across the government to demonstrate that the United States is fully committed to Internet Freedom. That commitment must include clear and continuing support for the evolving multistakeholder system of Internet governance, and direct engagement in international dialogue about how the NSA programs do or do not comport with international human rights and what a human rights-based approach to surveillance in the digital age looks like.

4 Work to restore trust in cryptography standards set by the National Institute of Standards and Technology. 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. Such actions not only weaken everyone's security but also the security standards-setting process itself. Recommendation 29 of the President's Review Group urges the U.S. government to "fully support and not undermine efforts to create encryption standards." NSA's consulting role in NIST's standards process should be clarified and limited to ensure the most secure standards possible.

5 Ensure that the U.S. government does not undermine Internet security by mandating backdoors in products. Recognizing that surveillance backdoors fundamentally threaten the security of our data and our online transactions, the Review Group's Recommendation 29 also urged the U.S. government to make clear that the "NSA will not demand changes in any product by an vendor for the purpose of undermining the security or integrity of the product," even if those changes are intended only to facilitate lawful surveillance. The House of Representatives recently approved an amendment that goes even further, prohibiting the NSA from mandating or requesting the creation of such backdoors.

6 Help eliminate security vulnerabilities, rather than secretly stockpile them. Secret stockpiling of previously unknown flaws irresponsibly leaves users open to attack from anyone who discovers the weakness. Consistent with the Review Group's Recommendation 30, the U.S. government should establish and adhere to a clear policy to disclose vulnerabilities to vendors by default, and only withhold that information in the narrowest circumstances and for the shortest period of time possible—if at all.

7 Develop policy guidance describing the circumstances where it is appropriate for the government to insert malware onto a target's device. The U.S. government should develop clear and specific policies about whether, when, and under what legal standards it is permissible for the government to hack into a target's computer in order to monitor a target's communications or extract information.

8 Separate the offensive and defensive functions of the NSA to minimize conflicts of interest. The NSA's multi-pronged efforts to weaken Internet security to facilitate signals intelligence collection demonstrate the inherent conflict of interest that has resulted from the agency's multiple mandates. In its Recommendation 25, the Review Group recommends that the information assurance mission of the NSA should be assigned to a separate agency. Considering how that role centrally involves the security of domestic and civilian networks, a civilian agency such as the Department of Homeland Security would be most appropriate.

End Notes

1. Barton Gellman & Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *The Washington Post*, June 7, 2013.
2. "Gartner Predict Cloud Computing Spending to Increase by 100% in 2016, Says AppsCare," *PRWeb*, July 19, 2012.
3. David Gilbert, "Companies Turn to Switzerland for Cloud Storage Following NSA Spying Revelations," *International Business Times*.
4. Daniel Castro, "How Much Will PRISM Cost the US Cloud Computing Industry?" *Information Technology and Innovation Foundation*, August 5, 2013; James Staten, "The Cost of PRISM Will Be Larger Than ITIF Projects," *Forrester Research*, August 14, 2013.
5. "NSA Scandal: UK and Canadian Business Weary of Storing Data in the US," Peer 1 Hosting, January 8, 2014.
6. "NSA After-shocks: How Snowden has changed ICT decision-makers' approach to the Cloud," NTT Communications, March 2014.
7. Sean Gallagher, "NSA leaks blamed for Cisco's falling sales overseas," *Ars Technica*, December 10, 2013; Paul Taylor, "Cisco warns emerging market weakness is no blip," *Financial Times*, December 13, 2013.
8. Spencer E. Ante, "Qualcomm CEO Says NSA Fallout Impacting China Business," *The Wall Street Journal*, November 22, 2013. *See also* Eamon Javers, "Is a Snowden effect stalking US telecom sales?" *CNBC*, November 15, 2013.
9. Haydn Shaughnessy, "Will the NSA Hack Wreck Apple's Hopes in China?" *Forbes*, January 7, 2014; Anton Troianovski, Thomas Gryta, and Sam Schechner, "NSA Fallout Thwarts AT&T," *The Wall Street Journal*, October 30, 2013.
10. Julian Hattem, "Tech takes hit from NSA," *The Hill*, June 30, 2014.
11. Claire Cain Miller, "Revelations of NSA Spying Cost US Tech Companies," *The New York Times*, March 21, 2014.
12. Andrea Peterson, "German government to drop Verizon over NSA spying fears," *The Washington Post*, June 26, 2014.
13. Alonso Soto and Brian Winter, "3-Saab wins Brazil jet deal after NSA spying sours Boeing bid," *Reuters*, December 18, 2013.
14. Mark Scott, "European Firms Turn Privacy Into Sales Pitch," *The New York Times*, June 11, 2014.
15. Steven Tisch, "Has the NSA Poisoned the Cloud?" *R Street Policy Study No. 17,* January 2014.
16. *For more information about the Reform Government Surveillance Coalition, see* https://www.reformgovernmentsurveillance.com/. The coalition includes AOL, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo!
17. David E. Sanger and Nicole Perlroth, "Internet Giants Erect Barriers to Spy Agencies," *New York Times*, June 6, 2014.
18. "New Harris Poll Shows NSA Revelations Impact Online Shopping, Banking, and More," *We Live Security*, April 2, 2014; Julian Hattem, "Many say NSA news changed their behavior," *The Hill*, April 2, 2014.
19. Kristina Irion, "Government Cloud Computing and National Data Sovereignty," *Social Science Research Network*, June 2012; 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).
20. Eugene Kaspersky, "What will happen if countries carve up the internet?" *The Guardian*, December 17, 2013, .
21. 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 2014.
22. 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/
23. Hill, "The Growth of Data Localization Post-Snowden," 8.
24. Arnaldo Galvao and Raymond Colitt, "Brazil May Require Google, Facebook to Store Data Locally," *Bloomberg News*, September 16, 2013.
25. Stephen D. Ezell, Robert D. Atkinson, and Michelle Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy," *The Information Technology and Innovation Foundation*, September 25, 2013, 18-9.
26. "Progress on EU data protection reform now irreversible following European Parliament vote," *European Commission*, March 12, 2014.
27. Caroline Kelley, "A Competitive Disadvantage? American Businesses Fear Fallout from Surveillance Leaks," *TIME*, August 1, 2013.
28. "NSA Snooping: MEPs table proposals to protect EU citizens' privacy," *European Parliament*, February 12, 2014.
29. Alex Byers, "Tech Safe Harbor Under Fire in Europe," *POLITICO Morning Tech*, November 6, 2013.
30. Michael Hickens, "American Spying Stymies Tech Firms," *The Wall Street Journal*, February 18, 2014
31. Heather Greenfield, "CCIA Praises Surveillance Reform Plans at Senate Judiciary Hearing," *Computer and Communications Industry Association*, December 11, 2013.
32. Richard Fontaine and Will Rogers, "Internet Freedom: A Foreign Policy Imperative in the Digital Age,"

Center for a New American Security, June 2011, 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.

33. Ben FitzGerald and Robert Butler, "NSA revelations: Fallout can serve our nation," *Reuters*, December 18, 2013.
34. Matthew Shears, "Snowden and the Politics of Internet Governance," *Center for Democracy and Technology*, February 21, 2014.
35. Eli Dourado, "So much for America's internet freedom agenda," *The Guardian*, August 7, 2013.
36. Deborah Brown, "UN Human Rights Council discusses surveillance and other internet issues at 24th session," *Access*, September 16, 2013.
37. "Montevideo Statement on the Future of Internet Cooperation," October 7, 2013.
38. *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. The report describes both the types of work that the State Department supports as well as the countries in which they operate.
39. Sana Saleem, "A year after Snowden revelations, damage persists to freedom of expression in Pakistan," *Committee to Protect Journalists*, June 16, 2014.
40. The U.S. was, for example, named an "Enemy of the Internet" by Reporters Without Borders in 2014. ("USA: NSA symbolises intelligence services' abuses," *Reporters Without Borders*, March 12, 2014.)
41. Mark Landler, "Merkel Signals That Tension Persists Over U.S. Spying," *The New York Times*, May 2, 2014; Paul Lewis, "US and Germany remain frosty amid awkward visit from Merkel," *The Guardian*, May 2, 2014.
42. Heather Arnet, "Why Dilma Cancelled on Obama," *The Daily Beast*, October 23, 2013.
43. James Ball, Bruce Schneier and Glenn Greenwald, "NSA and GCHQ target Tor network that protects anonymity of web users," *The Guardian*, October 4, 2013. 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).
44. Including Microsoft, Cisco and RSA Security amongst others.
45. Larry Greenemeier, "NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard," *Scientific American*, September 18, 2013.
46. Dan Goodin, "Stop using NSA-influenced code in our products, RSA tells customers," *Ars Technica*, September 19, 2013; Joseph Menn, "Exclusive: Secret contract tied NSA and security industry pioneer," *Reuters*, December 20, 2013.
47. "SIGINT Enabling Project," *ProPublica*.
48. James Ball, Julian Borger, and Glenn Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security," *The Guardian*, September 5, 2013.
49. Glenn Greenwald, Ewan MacAskill, Laura Poitras, Spencer Ackerman, and Dominic Rushe, "Microsoft handed the NSA access to encrypted messages," *The Guardian*, July 11, 2013.
50. Bruce Schneier, "Should Hackers Fix Cybersecurity Holes or Exploit Them?" *The Atlantic*, May 19, 2014.
51. Liam Tung, "NSA: Our zero days put you at risk, but we do what we like with them," *ZDNet*, March 13, 2014.
52. Spiegel Staff, "Inside TAO: Documents Reveal Top NSA Hacking Unit," *Der Spiegel*, December 9, 2013
53. *Id.*
54. *Id.*
55. Ryan Gallagher and Glenn Greenwald, "How the NSA Plans to Infect 'Millions' of Computers with Malware," *The Intercept*, March 12, 2014.

About New America's Open Technology Institute

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.

For more information, please visit our website: oti.newamerica.org.