Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness

BY DANIEL CASTRO AND ALAN MCQUINN | JUNE 2015

The failure of U.S. policymakers to address surveillance concerns over the last few years has buoyed foreign protectionism and hurt American businesses.

Almost two years ago, ITIF described how revelations about pervasive digital surveillance by the U.S. intelligence community could severely harm the competitiveness of the United States if foreign customers turned away from U.S.-made technology and services.[1] Since then, U.S. policymakers have failed to take sufficient action to address these surveillance concerns; in some cases, they have even fanned the flames of discontent by championing weak information security practices.[2] In addition, other countries have used anger over U.S. government surveillance as a cover for implementing a new wave of protectionist policies specifically targeting information technology. The combined result is a set of policies both at home and abroad that sacrifices robust competitiveness of the U.S. tech sector for vague and unconvincing promises of improved national security.

ITIF estimated in 2013 that even a modest drop in the expected foreign market share for cloud computing stemming from concerns about U.S. surveillance could cost the United States between $21.5 billion and $35 billion by 2016.[3] Since then, it has become clear that the U.S. tech industry as a whole, not just the cloud computing sector, has under-performed as a result of the Snowden revelations. Therefore, the economic impact of U.S. surveillance practices will likely far exceed ITIF's initial $35 billion estimate. This report catalogues a wide range of specific examples of the economic harm that has been done to U.S. businesses. In short, foreign customers are shunning U.S. companies. The policy implication of this is clear: Now that Congress has reformed how the National Security Agency (NSA) collects bulk domestic phone records and allowed private firms—rather than the government—to collect and store approved data, it is time to address other controversial digital surveillance activities by the U.S. intelligence community.[4]

The U.S. government's failure to reform many of the NSA's surveillance programs has damaged the competitiveness of the U.S. tech sector and cost it a portion of the global market share.[5] This includes programs such as PRISM—the controversial program authorized by the FISA Amendments Act, which allows for warrantless access to private-user data on popular online services both in the United States and abroad—and Bullrun—the NSA's program to undermine encryption standards both at home and abroad. Foreign companies have seized on these controversial policies to convince their customers that keeping data at home is safer than sending it abroad, and foreign governments have pointed to U.S. surveillance as justification for protectionist policies that require data to be kept within their national borders. In the most extreme cases, such as in China, foreign governments are using fear of digital surveillance to force companies to surrender valuable intellectual property, such as source code.[6]

In the short term, U.S. companies lose out on contracts, and over the long term, other countries create protectionist policies that lock U.S. businesses out of foreign markets. This not only hurts U.S. technology companies, but costs American jobs and weakens the U.S. trade balance. To reverse this trend, ITIF recommends that policymakers:

- Increase transparency about U.S. surveillance activities both at home and abroad.
- Strengthen information security by opposing any government efforts to introduce backdoors in software or weaken encryption.
- Strengthen U.S. mutual legal assistance treaties (MLATs).
- Work to establish international legal standards for government access to data.
- Complete trade agreements like the Trans Pacific Partnership that ban digital protectionism, and pressure nations that seek to erect protectionist barriers to abandon those efforts.

U.S. SURVEILLANCE POWERS COME AT A REAL COST

Since the revelations of PRISM and other digital surveillance programs by Edward Snowden in 2013, a steady stream of troubling details has continued to emerge about online spying by the U.S. intelligence community.[7] These revelations have fundamentally shaken international trust in U.S. tech companies and hurt U.S. business prospects all over the world. In 2014, one survey of businesses in the United Kingdom and Canada found that 25 percent of respondents planned to pull company data out of the United States as a result of the NSA revelations.[8] This survey also found that respondents were thinking differently about the location of their data in a post-PRISM world, with 82 percent citing national laws as their top concern when deciding where to store their data. Several companies have come forward describing the damage that this loss of trust has had on their ability to do business abroad. For example, the software-as-a-service company Birst has found that companies in Europe do not want their data hosted in North America due to concerns about U.S. spying.[9] In order to address these concerns, Birst was forced to partner with a European-based company to access European businesses. In another example, a major German insurance company turned its back on Salesforce—a U.S. cloud computing firm—that was slated to manage its consumer database after the revelations emerged.[10] In

fact, Salesforce faced major short-term sales losses and suffered a $124 million deficit in the fiscal quarter after the NSA revelations.[11]

Salesforce was not the only company to face this challenge, as U.S. firms saw their sales impacted all over the globe. For example, Cisco—a company that makes routers and switches—saw its sales interrupted in Brazil, China, and Russia because of reports that the NSA had secretly inserted backdoor surveillance tools into its routers, servers and networking equipment.[12] During a quarterly earnings call, Cisco CEO John Chambers even cited the NSA as the factor behind steep sales decreases, saying "I do think (the NSA revelation) is a factor in China."[13] These reports damaged the company's international reputation and prompted it to take extra precautions to thwart surreptitious actions by the NSA. The additional costs this involved were passed along to its customers.[14] Other companies have seen declining sales. For example, the Virginia-based web hosting company Servint saw its international clientele shrink from 60 percent of its business to nearly 30 percent as a result of European outrage.[15] Similarly, while mobile device chipmaker Qualcomm expects to see its sales continue to grow in China, its CEO has acknowledged that revelations about U.S. government surveillance are hurting sales and impacting its business in the rapidly growing foreign market.[16] IBM, Microsoft, and Hewlett-Packard also have reported diminished sales in China as a result of the NSA revelations.[17]

Outside the tech sector, other U.S. companies have reported that the U.S. surveillance activities have caused them to lose major contracts to foreign competitors. For example, in December 2013, Boeing lost a contract to Saab AB to replace Brazil's aging fighter jets due to concerns over NSA activities.[18] Foreign governments have also shied away from using U.S. companies to provide IT infrastructure to government entities and sensitive industries. For example, the German government dropped Verizon from providing Internet service to a number of its government departments out of fear that the NSA would be able to spy on its bureaucrats.[19] The government took this action despite a report from the German magazine *Der Spiegel* that suggested a close relationship between the NSA and German intelligence community.[20] In another notable example, some believe that China removed some of the leading U.S. technology brands from its Central Government Procurement Center's (CGPC) approved state purchase list in response to the revelations of widespread U.S. cyberespionage.[21] The Chinese government bodies can only purchase items on this list, which cover smaller-scale purchases of technology equipment. Many U.S. tech companies were dropped from this list, including Cisco (which had 60 products on the CGPC in 2012, but none in 2014), Apple, Intel's McAfee, and Citrix Systems.[22]

At the same time, foreign companies have made the U.S. digital surveillance policy a centerpiece of their own effective marketing strategy. Some European companies have begun to highlight where their digital services are hosted as an alternative to U.S. companies. German cloud companies like Hortnetsecurity bill themselves as "Cloud Services: Made in Germany," while French companies like Cloudwatt have joined the "Sovereign Cloud," a service advertised as resistant to NSA spying.[23] In another example, F-Secure, the European online cloud storage company whose service resembles that of Dropbox, has leveraged government surveillance into a sales pitch. Based out of Finland, F-Secure has made the promise that it will never share an individual's data with other

companies or governments. As a result, F-Secure signed up over one million users within its first 9 months.[24] Similarly, the French telecommunications company Orange has also leveraged the perceived belief that European companies protect privacy better than U.S. alternatives to make deeper inroads into European markets.[25]

U.S. SURVEILLANCE POWERS ARE THE JUSTIFICATION FOR FOREIGN PROTECTIONISM

The ability of companies—both tech and traditional—to easily share data across borders has brought a vast array of benefits to countries, companies, consumers, and economies through increased efficiency, decreased costs, and improved services.[26] And yet nations have continued to erect barriers to cloud computing and cross-border data flows, much to their own detriment.[27] While some defenders of these policies have asserted that they are designed to increase the privacy or security of their citizens' data, it is clear that they are also motivated by misguided self-interest. By creating rules that advantage domestic firms over foreign firms, many countries believe they will build a stronger domestic tech industry or gain short-term economic value, such as jobs in domestic data centers. In reality, these policies unwittingly limit the ability of a country's own firms to innovate by shielding them from international competition.[28] These policies not only limit the number of services that a country's citizens and businesses can enjoy, but also harm that country's productivity and competitiveness.

Some countries used U.S. surveillance laws to justify data protectionism even before Snowden's NSA revelations. For example, when Rackspace built data centers in Australia in 2012, an Australian competitor stirred up fears that the United States would use the Patriot Act to track Australian citizens as a means to force Rackspace out of Australia.[29] In addition, this same Australian company funded a report calling on Australian policymakers to impose additional regulations designed to put foreign cloud computing competitors at a disadvantage.[30] However, since the recent NSA revelations, the use of privacy concerns to justify protectionist barriers has grown significantly.

Amid growing anti-U.S. sentiment, Europe has seen calls for data localization requirements, procurement preferences for European providers, and even a "Schengen area for data"—a system that keeps as much data in Europe as possible—as ways to promote deployment of cloud services entirely focused on the European market.[31] France and Germany have even started to create dedicated national networks: "Schlandnet" for the former and the "Sovereign Cloud" for the latter. [32] The French government has gone so far as to put €150 million ($200 million) into two start-ups, Numergy and Cloudwatt, to create a domestic infrastructure independent of U.S. tech giants.[33] Furthermore, some groups have invoked U.S. cyberespionage to argue that European citizens are not adequately protected and are calling for the removal of the "safe harbor" agreement—an agreement that allows Internet companies to store data outside of the European Union. Yet if this were removed it would cut Europeans off from many major Internet services.[34]

There is also an increasingly distressing trend of countries, such as Australia, China, Russia, and India, passing laws that prevent their citizens' personal information from leaving the country's borders—effectively mandating that cloud computing firms build data centers in

those countries or risk losing access to their markets. For example, in 2014 Russian implemented and Indonesia began considering policies that would require Internet-based companies to set up local data centers.[35] These policies are often a veiled attempt to spur short term economic activity by creating data-center jobs. However, this benefit is often outweighed by the substantial cost of building unnecessary data centers, a cost that is eventually passed along to the country's citizens. Several U.S. tech giants, such Apple and Salesforce, have already started to build their data centers abroad to appease foreign watchdogs and privacy advocates.[36] For example, Amazon started running Internet services and holding data in Germany for its European business partners in an effort to downplay threats of online spying.[37]

Protectionist policies in China have further strained the U.S. tech industry. In January 2015, the Chinese government adopted new regulations that forced companies that sold equipment to Chinese banks to turn over secret source code, submit to aggressive audits, and build encryption keys into their products.[38] While ostensibly an attempt to strengthen cybersecurity in critical Chinese industries, many western tech companies saw these policies as a shot across the bow trying to force them out of China's markets. After all, the Chinese government had already launched a "de-IOE" movement—IOE stands for IBM, Oracle and EMC— to convince its state-owned banks to stop buying from these U.S. tech giants.[39] To be sure, the Chinese government recently halted this policy under U.S. pressure.[40] However, the halted policy can be seen as a part of a larger clash between China and the United States over trade and cybersecurity. Indeed, these proposed barriers were in part a quid pro quo from China, after the United States barred Huawei, a major Chinese computer maker, from selling its products in the United States due to the fear that this equipment had "back doors" for the Chinese government.[41] Since the Snowden revelations essentially gave them cover, Chinese lawmakers have openly called for the use of domestic tech products over foreign goods both to boost the Chinese economy and in response to U.S. surveillance tactics. This system of retaliation has not only led to a degradation of business interests for U.S. tech companies in China, but also disrupted the dialogue between the U.S. government and China on cybersecurity issues.[42]

RECOMMENDATIONS

The free and open Internet that powers the globally networked economy is dependent on the ability of individuals and companies to engage in commerce without geographic restrictions. To turn back the tide of technology protectionism, U.S. trade negotiators will need a stronger hand to play. They cannot go to other nations and tell them to not discriminate against U.S. tech firms if the U.S. intelligence system continues to follow policies that threaten their citizens and businesses. As a result, it is incumbent on the Congress and the Obama administration to take the lead in showing the world the best standards for transparency, cooperation, and accountability.

First, the U.S. government should be forthcoming and transparent about its surveillance practices and clearly inform the public about the data it collects domestically and abroad. The U.S. government should set the gold standard for international transparency requirements, so that it is clear what information both U.S. and non-U.S. companies are disclosing to governments at home and abroad. The U.S. government should then work

with its allies to create an international transparency requirement that illuminates when countries conduct surveillance that accesses foreign companies' information.

Second, the U.S. government should draw a clear line in the sand and declare that the policy of the U.S. government is to strengthen not weaken information security. The U.S. Congress should pass legislation, such as the Secure Data Act introduced by Sen. Wyden (D-OR), banning any government efforts to introduce backdoors in software or weaken encryption.[43] In the short term, President Obama, or his successor, should sign an executive order formalizing this policy as well. In addition, when U.S. government agencies discover vulnerabilities in software or hardware products, they should responsibly notify these companies in a timely manner so that the companies can fix these flaws. The best way to protect U.S. citizens from digital threats is to promote strong cybersecurity practices in the private sector.

Third, the U.S. government should strengthen its mutual legal assistance treaties (MLATs), which allow law enforcement agencies to receive assistance from and provide assistance to their counterparts in other countries. These treaties work through cooperation between both governments, which agree to share information during lawful investigations. Some governments—such as China and the United States—have begun to circumvent the MLAT process to access data stored in other countries because they perceive the process to be too slow.[44] If this becomes the norm for the U.S. government, the end game is clear: significantly fewer foreign businesses, governments, and citizens will do business with U.S. companies. Rather than abandon the MLAT process, the U.S. government should work to improve it and make these requests more transparent. While the U.S. government cannot force other governments to improve their own MLAT process, it can set an example by streamlining its own and asserting that other countries should do the same. The Law Enforcement Access to Data Stored Abroad (LEADS) Act, recently introduced in the Senate by Sens. Orrin Hatch (R-Utah), Chris Coons (D-Del.) and Dean Heller (R-Nev.) and in the House by Reps. Tom Marino (R-Pa.) and Suzan DelBene (D-Wash.), would do just that.[45]

Fourth, the U.S. government should work with its trade partners to establish international legal standards for government access to data. The United States should engage with its trade partners to develop a "Geneva Convention on the Status of Data."[46] This would create a multi-lateral agreement that would establish international rules for transparency, settle questions of jurisdiction, engender cooperation for better coordination of international law enforcement requests, and limit unnecessary access by governments to citizens of other countries. Only by working to establish a global pact on these issues can countries that have previously engaged in mass cyberespionage assure the international community that countries can hold each other accountable in the future.

Finally, while many countries will continue to use U.S. surveillance practices as a pretext to pursue tech-mercantilist measures, the United States should not let these practices go unchallenged. The U.S. government should push back against these barriers by completing trade agreements that eliminate protectionism. The Trans-Pacific Partnership (TPP) may be the first U.S. trade agreement to enshrine such strong free trade provisions for cross-

border data flows. U.S. negotiators should ensure that other agreements, including the Trans-Atlantic Trade and Investment Partnership (T-TIP), and the Trade in Services Agreement (TISA), are equally strong.[47] The United States should build an alliance against bad actors, forcing protectionist countries to the sidelines of the global trade arena if they continue to enact these anti-competitive rules. Furthermore, as the U.S. Congress weighs future trade promotion authority, it should direct U.S. negotiators to include prohibitions against protectionist barriers in all future U.S. trade agreements.

For other nations, especially China, U.S. messages and actions need to be much tougher. If a country resorts to protectionism on the pretext of guarding against U.S. surveillance, but its true end game is to systemically exclude U.S. companies and distort its market for competitive advantage, then the U.S. government should push back aggressively with trade measures that impose significant economic penalties.

CONCLUSION

When historians write about this period in U.S. history it could very well be that one of the themes will be how the United States lost its global technology leadership to other nations. And clearly one of the factors they would point to is the long-standing privileging of U.S. national security interests over U.S. industrial and commercial interests when it comes to U.S. foreign policy.

This has occurred over the last few years as the U.S. government has done relatively little to address the rising commercial challenge to U.S. technology companies, all the while putting intelligence gathering first and foremost. Indeed, policy decisions by the U.S. intelligence community have reverberated throughout the global economy. If the U.S. tech industry is to remain the leader in the global marketplace, then the U.S. government will need to set a new course that balances economic interests with national security interests. The cost of inaction is not only short-term economic losses for U.S. companies, but a wave of protectionist policies that will systematically weaken U.S. technology competiveness in years to come, with impacts on economic growth, jobs, trade balance, and national security through a weakened industrial base. Only by taking decisive steps to reform its digital surveillance activities will the U.S. government enable its tech industry to effectively compete in the global market.

ENDNOTES

1. Daniel Castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry," *Information Technology and Innovation Foundation*, August 2013, http://www2.itif.org/2013-cloud-computing-costs.pdf.
2. Alex Hern, "FBI anti-terror official calls on tech firms to 'prevent encryption above all else,'" *The Guardian*, June 5, 2015, http://www.theguardian.com/technology/2015/jun/05/fbi-anti-terror-tech-firms-encryption.
3. Daniel Castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry," *Information Technology and Innovation Foundation*.
4. Lily Newman, "Senate Approved USA Freedom Act, Which Ends NSA Bulk Surveillance," *Slate*, June 2, 2015, http://www.slate.com/blogs/future_tense/2015/06/02/senate_approves_usa_freedom_act.html; Susan Molinari, "Congress takes a significant step to reform government surveillance," *Google*, June 2, 2015, http://googlepublicpolicy.blogspot.com/.
5. Dara Lind, "Everyone's heard of the Patriot Act. Here's what it actually does," *Vox*, June 2, 2015, http://www.vox.com/2015/6/2/8701499/patriot-act-explain; Kim Zetter, "NSA's Decade-Long Plan to Undermine Encryption Includes Backdoors, Stolen Keys, Manipulating Standards," *Wired*, November 5, 2013, http://www.wired.com/2013/09/nsa-backdoored-and-stole-keys/.
6. "China puts cybersecurity squeeze on US technology companies," *The Guardian*, January 29, 2015, http://www.theguardian.com/technology/2015/jan/29/china-puts-cybersecurity-squeeze-on-us-technology-companies.
7. Salvador Rodriguez, "NSA 'Equation' Fallout: Experts Say Damage To US Tech Firms Could Top $180B," *International Business Times*, February 15, 2015, http://www.ibtimes.com/nsa-equation-fallout-experts-say-damage-us-tech-firms-could-top-180b-1819264; Charlie Savage, Julia Angwin, Jeff Larson, and Henrik Moltke, "Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at U.S. Border," *New York Times*, June 4, 2015, http://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-spying-at-us-border.html.
8. "NSA Scandal: UK and Canadian Businesses Wary of Storing Data in the U.S." *PEER 1 Hosting*, January 8, 2014, http://www.peer1.com/news-update/nsa-scandal-uk-and-canadian-businesses-wary-storing-data-in-us.
9. Derek du Preez, "Birst partners with AWS in Ireland in direct response to NSA concerns," *Diginomica*, August 28, 2014, http://diginomica.com/2014/08/28/birst-partners-aws-ireland-direct-response-nsa-concerns/.
10. Timothy Stenovec, "NSA Spying Has Tech Companies Worried About Their Most Precious Thing," *Huffington Post*, December 09, 2013, http://www.huffingtonpost.com/2013/12/09/nsa-tech-companies_n_4415258.html.
11. Andrew Mouton, "Salesforce loses money, but masters art of distraction," *USA Today*, December 2, 2013, http://www.usatoday.com/story/tech/2013/12/02/salesforce-earnings/3803095/.
12. Aarti Shahani, "A Year After Snowden, U.S. Tech Losing Trust Overseas," *National Public Radio*, June 5, 2014, http://www.npr.org/sections/alltechconsidered/2014/06/05/318770896/a-year-after-snowden-u-s-tech-losing-trust-overseas.
13. Sean Gallagher, "NSA leaks blamed for Cisco's falling sales overseas (updated)," *Arstechnica*, December 10, 2013, http://arstechnica.com/information-technology/2013/12/nsa-leaks-blamed-for-ciscos-falling-sales-overseas/.
14. Jeremy Kirk, "To avoid NSA, Cisco delivers gear to strange addresses," *Computerworld*, March 19, 2015, http://www.computerworld.com/article/2899341/to-avoid-nsa-cisco-delivers-gear-to-strange-addresses.html.
15. Julian Hattem, "Tech takes hit from NSA," *The Hill*, June 30, 2014, http://thehill.com/policy/technology/210880-tech-takes-hit-from-nsa.
16. Spencer Ante, "Qualcomm CEO Says NSA Fallout Impacting China Business," *Wall Street Journal*, November 22, 2013, http://www.wsj.com/articles/SB10001424052702304337404579214353783842062.
17. Danielle Kehl et al., "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity," *New America Foundation*, July 2014, https://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf.

18. Alonso Soto and Brian Winter, "UPDATE 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.
19. Andrea Peterson, "German government to drop Verizon over NSA spying fears," *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/.
20. Spiegel Staff, "Spying Together: Germany's Deep Cooperation with the NSA," *Spiegel Online*, June 18, 2014, http://www.spiegel.de/international/germany/the-german-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445.html.
21. Paul Carsten, "China drops leading tech brands for certain state purchases," *Reuters*, February 27, 2015, http://www.reuters.com/article/2015/02/27/us-china-tech-exclusive-idUSKBN0LV08720150227.
22. Ibid.
23. Leila Abboud and Paul Sandle, "Analysis: European cloud computing firms see silver lining in PRISM scandal," *Reuters*, June 17, 2013, http://www.reuters.com/article/2013/06/17/us-cloud-europe-spying-analysis-idUSBRE95G0FK20130617; Mitch Wagner, "Cloudwatt Builds Snoop Proof Cloud," *Light Reading*, July 31, 2014, http://www.lightreading.com/carrier-sdn/cloudwatt-builds-snoop-proof-cloud/d/d-id/710181.
24. Mark Scott, "European Firms Turn Privacy into Sales Pitch," *New York Times*, June 11, 2014, http://bits.blogs.nytimes.com/2014/06/11/european-firms-turn-privacy-into-sales-pitch.
25. Ibid.
26. Daniel Castro and Alan McQuinn, "Cross Border Data Flows Enable Growth in All Industries," *Information Technology and Innovation Foundation*, February 2015, http://www2.itif.org/2015-cross-border-data-flows.pdf.
27. Stephen Ezell, Robert Atkinson, and Michelle Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy," *Information Technology and Innovation Foundation*, September 2013, http://www2.itif.org/2013-localization-barriers-to-trade.pdf.
28. Ibid.
29. Daniel Castro and Alan McQuinn, "Data sovereignty or data protectionism?" *Computerworld Australia*, May 15, 2015, http://www.computerworld.com.au/article/575087/data-sovereignty-data-protectionism/.
30. The report notes: ""The United States Patriot Act brazenly declares the US Government's right to access anything it wants from any cloud infrastructure over which it can claim jurisdiction. That creates a demand for cloud computing services that are not subject to such capricious hazards…the Australian government should regulate the cloud so that we're a preferred provider for firms, governments and other users offshore." See "The potential for cloud computing services in Australia," *Lateral Economics*, October 2011, http://lateraleconomics.com.au/wp-content/uploads/2014/02/The-potential-for-cloud-computing-services-in-Australia.pdf.
31. Jeanette Seiffert, "Weighing a Schengen zone for Europe's Internet data," *Deutsche Welle*, February 2, 2014, http://www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482.
32. Ibid.
33. Leila Abboud and Paul Sandle, "Analysis: European cloud computing firms see silver lining in PRISM scandal," *Reuters*.
34. Duncan Robinson and Murad Ahmed, "US Tech giants face fresh fight with Europe over privacy," *Financial Times*, March 24, 2015, http://www.ft.com/cms/s/0/44c71248-d22c-11e4-ae91-00144feab7de.html#axzz3bpHsBNwU.
35. Michelle Wein, "The Worst Innovation Mercantilist Policies of 2014," *Information Technology and Innovation Foundation*, December 2014, http://www2.itif.org/2014-worst-mercantilist-fourteen.pdf.
36. Paul McDougall, "Why Are Apple, Amazon Data Center Jobs Going to Europe? Blame the NSA," *International Business Times*, February 26, 2015, http://www.ibtimes.com/why-are-apple-amazon-data-center-jobs-going-europe-blame-nsa-1829260.
37. Murad Ahmed, "Amazon to open German data centres to soothe European concerns," *Financial Times*, October 23, 2014, http://www.ft.com/intl/cms/s/0/56181a6e-5a96-11e4-b449-00144feab7de.html#axzz3bvD1OxId.

38. Paul Mozur, "New Rules in China Upset Western Tech Companies," *New York Times*, January 28, 2015, http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html.
39. Li Xiaoxiao et al., "China pulling the plug on IBM, Oracle, others," *Market Watch*, June 26, 2014, http://www.marketwatch.com/story/china-pulling-the-plug-on-ibm-oracle-others-2014-06-26.
40. Paul Mozur and Jane Perlez, "China Halts New Policy on Tech for Banks," *New York Times*, April 16, 2015, http://www.nytimes.com/2015/04/17/business/international/china-suspends-rules-on-tech-companies-serving-banks.html?_r=0.
41. Paul Mozur, "New Rules in China Upset Western Tech Companies," *New York Times*.
42. Ibid.
43. Daniel Castro, "Why FBI Is Wrong on Encryption Workaround," *InformationWeek*, December 3, 2014, http://www.informationweek.com/strategic-cio/digital-business/why-fbi-is-wrong-on-encryption-workaround/a/d-id/1317824; Daniel Castro, "Has the US government learned nothing from the Clipper Chip?" *FedScoop*, September 11, 2013, http://fedscoop.com/guest-column-has-us-government-learned-nothing/.
44. U.S. law enforcement agencies have attempted to circumvent established law enforcement information sharing treaties at the expense of U.S. economic interests. For example, in 2013, the U.S. government chose not to use its established information sharing treaty with Ireland to request access to data stored abroad about a suspect. Instead, it served Microsoft with a search warrant, demanding that the company turn over data stored in a data center in Dublin, Ireland. See Daniel Castro and Alan McQuinn, "Cross-Border Digital Searches: An Innovation-Friendly Approach," *Information Week*, November 5, 2014, http://www.informationweek.com/strategic-cio/digital-business/cross-border-digital-searches-an-innovation-friendly-approach/a/d-id/1306989.
45. Alan McQuinn, "The LEADS Act presents a path forward for cross-border digital searches," *Innovation Files*, September 22, 2014, http://www.innovationfiles.org/the-leads-act-presents-a-path-forward-for-cross-border-digital-searches/.
46. Daniel Castro, "The False Promise of Data Nationalism," *Information Technology and Innovation Foundation*, December 2013, http://www2.itif.org/2013-false-promise-data-nationalism.pdf.
47. Daniel Castro and Alan McQuinn, "Cross Border Data Flows Enable Growth in All Industries," *Information Technology and Innovation Foundation*.

ACKNOWLEDGMENTS

The authors wish to thank the following individuals for providing input to this report: Rob Atkinson, Randolph Court, and Sue Wunder. Any errors or omissions are the authors' alone.

ABOUT THE AUTHOR

Daniel Castro is the vice president of the Information Technology and Innovation Foundation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

Alan McQuinn is a research assistant with the Information Technology and Innovation Foundation. Prior to joining ITIF, Mr. McQuinn was a telecommunications fellow for Congresswoman Anna Eshoo and an intern for the Federal Communications Commission in the Office of Legislative Affairs. He got his B.S. in Political Communications and Public Relations from the University of Texas at Austin.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

FOR MORE INFORMATION, VISIT US AT WWW.ITIF.ORG.