ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of

Robert D. Atkinson, Ph.D.

Founder and President

The Information Technology and Innovation Foundation

on

"International Data Flows: Promoting Digital Trade in the 21st Century"

Before the

House Judiciary Committee

Subcommittee on Courts, Intellectual Property, and the Internet

November 3, 2015

Good afternoon Chairman Issa, Ranking Member Nadler, and members of the Subcommittee; thank you for inviting me to share the views of the Information Technology and Innovation Foundation (ITIF) on the path to promoting digital trade in the 21st century.

The Information Technology and Innovation Foundation is a non-partisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity internationally, in Washington, and in the states. Recognizing the vital role of technology in ensuring prosperity, ITIF focuses on innovation, productivity, and digital economy issues. We have long been involved in the digital trade debate, advocating for policies which support the free flow of data across borders as essential to global trade and commerce and I very much appreciate the opportunity to comment on this issue today.

Since 1944, when the Bretton Woods Conference established the framework for the post-war global economy, there has been a strong, shared consensus that as long as governments do not engage in mercantilist policies, global trade will improve economic welfare. In the manufacturing-based economy of that time, this consensus mainly applied to trade in goods. But as services trade grew, so too did the shared commitment to free trade in services. Now, with the rise of the data economy, it has become clear that free trade in data is just as important to maximizing both U.S. and global welfare as free trade in goods and services, if not more so. The United States holds a distinct leadership role in the data economy because it has been a pioneering innovator and early adopter of information technology, so ensuring that there is global free trade in data will be an especially important driver of U.S. economic competitiveness, job creation, wage growth, and consumer benefits.

However, global free trade in data is under serious threat. Many nations, for a variety of motivations—some related to privacy and security concerns, many related to naked protectionism—are putting in place policies to balkanize the data economy by limiting cross-border data flows. Even here in the United States, some privacy advocates and opponents of trade are decrying the proposed Trans-Pacific Partnership (TPP) for (rightly) including strong and enforceable provisions against data protectionism.

My testimony will first review why free trade in data is so important to the U.S. economy. I will then document the sizeable and growing threat to free trade in data and explore the different motivations of countries involved. Finally, I will discuss where we stand in terms of progress (e.g., TPP) and setbacks (e.g., the recent decision by the European Court of Justice to reject the longstanding U.S.-EU Safe Harbor Agreement) and propose a number of steps Congress and the administration can take to advance free trade in data.

In short, the task now is for policymakers to continue building on the progress in TPP—next in the context of the Transatlantic Trade and Investment Partnership (T-TIP) and the Trade in Services Agreement (TiSA)—while at the same time alleviating tensions in the law enforcement and national security arena by embracing needed reforms.

Why Data Innovation Is Important

In a growing digital economy, the ability of organizations to collect, analyze, and act on data represents an increasingly important driver of innovation and growth. To start with, the Internet broadly, and data specifically, are key drivers of growth. The McKinsey Global Institute estimates that for 13 of the world's largest economies between 2007 and 2011, the Internet alone accounted for 21 percent of aggregate GDP growth.[1] ITIF has estimated that, all by itself, the commercial activity that is concentrated under the Internet's ".com" top-level domain will contribute $3.8 trillion annually to the global economy by 2020.[2]

Moreover, it is increasingly the case that many of the benefits from information technology come from creating value and insights from data. Virtually every sector of the U.S. economy benefits from the data revolution; the applications for data processing and analytics are so vast that it is difficult to grasp the magnitude of the potential benefits. And this value will only increase as the public and private sectors alike become more data-driven.[3] For example, the McKinsey Global Institute estimates that making open data available for public use, particularly government data, would unlock up to $5 trillion in global economic value annually across just seven sectors, ranging from education to consumer finance.[4] In the United States, the use of big data in health care can save $450 billion per year.[5] Industry forecasters estimate that, by 2025, the Internet of Things will have an economic impact of up to $11.1 trillion per year.[6] And for the global public sector, the Internet of Things is expected to create $4.6 trillion in value by 2022.[7] According to a study by the Lisbon Council and the Progressive Policy Institute, if six of Europe's largest economies (France, Germany, Italy, Spain, Sweden, and the United Kingdom) could raise their "digital density" (the amount of data used per capita) to U.S. levels, those countries could generate an additional €460 billion in economic output per year; a 4 percent increase in their GDP.[8]

Why Free Trade in Data Is Important

A key reality of the global digital economy is that a significant share of data needs to move across borders. It is not unusual, for example, for Internet traffic to go through multiple different intermediaries in multiple nations. To paraphrase cyberspace advocate John Perry Barlow, who once said "information wants to be free," today, "information wants to be global." As the OECD notes in a recent report on the data economy:

> The data ecosystem involves cross-border data flows due to the activities of key global actors and the global distribution of technologies and resources used for value creation. In particular, ICT infrastructures used to perform data analytics, including the data centres and software, will rarely be restricted to a single country, but will be distributed around the globe to take advantage of several factors; these can include local work load, the environment (e.g., temperature and sun light), and skills and labour supply (and costs). Moreover, many data-driven services developed by entrepreneurs "stand on the shoulders of giants" who have made their innovative services (including their data) available via application programming interfaces (APIs), many of which are located in foreign countries.[9]

Indeed, the growing extent and value of cross-border data flows is reflected in the fact that the data-carrying capacity of transatlantic submarine cables rose at an average annual rate of 19 percent between 2008 and 2012.[10]

This is why—absent policy-created "data protectionism"—digital trade and cross-border data flows are expected to grow much faster than the overall rate of global trade. Indeed, Finland's national innovation organization, TEKES, estimates that by 2025, half of all value created in the global economy will be created digitally.[11]

As a result, the ability to move data across borders is a critical component of value creation for organizations in the United States and other countries around the world. As the OECD states, "the free flow of information and data is not only a condition for information and knowledge exchange, but a vital condition for the globally distributed data ecosystem as it enables access to global value chains and markets."[12] Fully half of all global trade in services now depends on access to cross-border data flows.[13] And digitally enabled services have become a key growth engine for the U.S. economy, with exports reaching $356 billion in 2011, up from $282 billion just four years earlier.[14]

This is why the U.S. International Trade Commission (ITC) estimates that digital trade increased annual U.S. GDP by between $517 and $710 billion in 2011 (3.4 to 4.8 percent).[15] The ITC further estimates that digital trade increased average wages and helped create 2.4 million jobs in 2011. U.S. firms in digitally intensive industries sold $935.2 billion in products and services online in 2012, including $222.9 billion in exports. Similarly, based on 2014 estimates, the U.S. International Trade Commission estimated that decreasing barriers to cross-border data flows would increase U.S. GDP by 0.1 to 0.3 percent.[16] And even though the ITC's analysis shows important benefits from digital trade, those benefits are likely understated. This is because the report limited its analysis to "digitally intensive" sectors, which means that its numbers exclude contributions from firms in industries that only use digital trade as a smaller part of their business.

The ITC also found digital trade to be crucial for digitally intensive small and medium-sized enterprises, which sold $227 billion in products and services online in 2012. Indeed, small firms in a wide array of sectors depend on digital trade. For example, in the $120 billion U.S. app industry, small companies and startups account for 82 percent of the top-grossing applications. Consumers throughout the world use these apps and any interruption in cross-border data flows will negatively affect both firms' revenues and customers' experiences.

One reason digital trade is so important to the U.S. economy is that U.S. information technology companies lead the world. As of 2010, U.S. firms held a 26 percent share of the global information technology (IT) industry and were the world's largest producers of IT goods and services.[17] Of the top 20 enterprise cloud computing service providers in the world, 17 are headquartered in the U.S.[18] Of the top 10 Internet firms, seven are U.S.-headquartered.[19]

But as important as free trade in data is to U.S. tech firms, it is even more important to traditional industries, such as automobile manufacturers, mining companies, banks, hospitals, and grocery store chains—all of which depend on the ability to move data across borders or analyze it in real-time as a fundamental enabler of their supply chains, operations, value propositions, and business models. Indeed, among the thousands of U.S. firms that have operated under the U.S.-EU Safe Harbor Agreement, 51 percent do so in order to process data on European employees—for example, transferring the personnel files of overseas workers to the United States for human resource purposes—and most of these firms are in traditional industries.[20] In fact, the McKinsey Global Institute estimates that about 75 percent of the value added by data flows on the Internet accrues to "traditional" industries, especially via increases in global growth.[21]

There are numerous examples of U.S. firms benefiting from cross-border data flows. For example, Ford Motor Company gathers data from over four million cars with in-car sensors and remote applications management software.[22] All data is analyzed in real-time, giving engineers valuable information to identify and solve issues, know how the car responds in different road and weather conditions, and be aware of any other forces affecting the vehicle. This data is returned back to the factory for real-time analysis and then returned to the driver via a mobile app. Like other car companies, Ford believes the data belongs to the owner and they are its "data steward." For internal purposes, performance data is de-identified and analyzed to track potential performance and warranty issues.[23] Ford uses a U.S. cloud service provider to host this data.[24]

Likewise, Caterpillar, a leading manufacturer of machinery and engines used in industries, established its fleet management solution to increase its customers' performance and cut costs. Sensor-enabled machines transmit performance and terrain information to Caterpillar's Data Innovation Lab in Champaign, Illinois where data can be analyzed, enabling Caterpillar and its customers to remotely monitor assets across their fleets in real time. This also enables Caterpillar and its customers to diagnose the cause of performance issues when things go wrong. For example, truck data at one worksite showed Caterpillar that some operators were not using the correct brake procedures on a haul road with a very steep incline. Retraining the operators saved the customer about $12,000 on the project, and company-wide driver incidents decreased by 75 percent. Cross-border data flow restrictions could limit Caterpillar's ability to offer these services in certain markets, such as those that prevent the movement of GPS data across borders.[25]

When nations impose restrictions on data flows, the U.S. economy is harmed in at least two ways. First, requiring localization of data and servers will move activity from the United States to these nations, reducing jobs and investment here and raising costs for U.S. firms. Second, if the restrictions preclude U.S. firms from participating in foreign markets, then U.S. firms will lose global market share to competitors that are based in those protected markets.

Some advocates assert that the U.S. economy can thrive simply by having a healthy small business sector and that policymakers can and should be indifferent to the competitive fate of U.S. multinational corporations. But this is profoundly wrong. Losing global market share because of digital protectionism—regardless of whether it is in information industries or "traditional"

industries—harms not just U.S. multinationals, but also the U.S. economy and U.S. workers. A large body of scholarly literature proves this point. Dartmouth's Matthew J. Slaughter finds that employment and capital investment in U.S. parents and foreign affiliates rise simultaneously.[26] In a study of U.S. manufacturing multinationals, Desai et al., find that a 10 percent greater foreign investment is associated with 2.6 percent greater domestic investment.[27] Another study of U.S. multinational corporation services firms found that affiliate sales abroad increases U.S. employment by promoting intra-firm exports from parent firms to foreign affiliates.[28] In short, when U.S. multinationals are able to expand market share overseas, it creates real economic benefits and jobs here at home. These jobs run the gamut, including sales, marketing, and management—particularly engineering, computer science, and technical jobs. And this matters because, as ITIF has shown, IT workers earned 74 percent more than the average worker in 2011 ($78,584 versus $45,230). In 2011, the IT industry contributed about $650 billion to the U.S. economy, or 4.3 percent of GDP, up from 3.4 percent in the early 1990s.[29]

Finally, digital trade is not just benefiting large companies like Amazon and Ford. Small and medium-sized U.S. enterprises make up one-quarter of digital trade sales and fully one-third of digital trade purchases.[30]

Free trade in data is important not just for businesses and their workers, but for all Americans. Imagine if data had a much harder time crossing borders. Americans traveling overseas would not be able to use their credit cards or cell phones, because both require cross-border data flows. In fact, without cross-border data flows, people would not be able to fly overseas at all, because airlines need to transmit data on passenger manifests and flight operations and governments need to transfer passport data on passengers. People would have a hard time shipping packages overseas. If they get sick while traveling, there would be no way to access their medical records, much less receive remote medical expertise or diagnostic tests, if medical data are not allowed to cross borders. Without data flows, officials can't pre-position travelers' personal information to speed customs and border crossings. And companies would not be able to provide international service or warranty protection over the productive life of a product. For example, it would disrupt the increasingly common practice in which automakers remotely upgrade the software in people's cars.

By contrast, the free flow of data can improve the quality of goods and services, including public goods. For example, cross-border data flows can be an essential component of pandemic disease management and control. The free flow of data is also a key to providing remote diagnostics with medical imaging systems, as there can be personally identifiable information in these systems. Likewise, farmers can remotely receive personalized weather feeds that are based on big data analytics (e.g., a mash up of data on weather forecast and history, soil moisture, soil content, river flows, etc.), but this requires data to be able to flow across national borders.

As a case study, consider how cross-border data flows can impact quality and safety in the airline industry. Aircraft manufacturer Boeing, headquartered in Chicago, relies heavily on data transmitted from planes operating around the world to improve safety and reduce flight delays and cancellations. Boeing has created a system called Airplane Health Management that processes the large amounts of

data that its airplanes generate and transmit in real time while they are in flight.[31] For example, a Boeing 737 engine produces 20 terabytes of data per hour.[32] Commercial airlines that operate Boeing aircraft, such as United Airlines, can monitor this data in real time and proactively dispatch maintenance crews to await an airplane's arrival and quickly address any problems that may have arisen during a flight.[33] Since the very purpose of airplanes is to traverse borders, the success of such a system hinges on Boeing's ability to quickly and easily transmit data from its planes to its airline customers across the globe.[34]

The free flow of data will also enhance overall "data innovation," which will play a key role in improving the lives of Americans. A case in point is medical research. Diseases do not stop at national borders, and the data that are needed to help find cures need to cross borders, too. Powerful data analytics applied to bigger global data sets can help speed the development of cures. (Organizations can "de-identify" data so that they do not release personally identifiable information.) The rarer the disease, the more important it is to collect data on a global basis, since data from individual countries may not create a large enough database to reveal patterns. Unnecessary restrictions on data flows will make it harder for health care providers to save lives.

Finally, it is important to note that support for free trade in data does not have to mean support for the free flow of all data, regardless of its legal status. Just as it is not a violation of free trade principles to block trade in banned products, such as elephant ivory or rhinoceros products, it is also not a violation of free trade principles to oppose digital trade in illegal digital goods, such as child pornography, email spam, Internet malware, and pirated digital content. Numerous countries, including the United Kingdom, Denmark, Greece, Italy, Portugal, and Singapore, have blocked websites that trade in pirated digital content (either using their domain name or network address), thereby preventing that data from flowing into the country.[35] In fact, according to the International Federation of the Phonographic Industry, the global trade association for the music industry, "[Internet service providers] in 19 countries have been ordered to block access to more than 480 copyright infringing websites."[36] This is clearly not digital protectionism. Rather, it is indicative of how the global trading system was intended to work, enabling trade in legal goods, services, and data, and prohibiting trade in illegal goods, services, and data. Moreover, just as taking a stand against trade in products like ivory does not weaken America's intellectual leadership in promoting free trade, taking a stand against trade in illegal digital goods will not weaken our case in promoting free trade in data.

Barriers to Digital Trade

Data will naturally flow across borders when it needs to, unless nations erect digital barriers. Such barriers involve legal requirements on companies to either store and process data locally or to use only local data servers as a condition for providing certain digital services. These non-tariff barriers undermine the benefits of digital trade and make it difficult for U.S. firms to compete with local ones. Troublingly, an increasing number of nations are erecting digital trade barriers.

- In 2014, **Nigeria** put into effect the "Guidelines for Nigerian Content Development in Information and Communications Technology (ICT)."[37] Several of the provisions regard restrictions on cross-border data flows and mandate that all subscriber, government, and consumer data be stored locally.[38]

- **Turkey** passed a law in 2014 mandating that companies process all digital payments inside its borders.

- Two Canadian provinces, **British Columbia** and **Nova Scotia**, have implemented laws mandating that personal data held by public bodies such as schools, hospitals, and public agencies must be stored and accessed only in Canada unless certain conditions are fulfilled.[39]

- **Greece** introduced data localization requirements in February 2011 through a law that states, "Data generated and stored on physical media, which are located within the Greek territory, shall be retained within the Greek territory." The European Commission criticized the law as being inconsistent with the E.U. single market, but it remains in effect.[40]

- **Venezuela** has passed regulations requiring that IT infrastructure for payment processing be located domestically.

- **Malaysia** has passed a local data server requirement, but has not yet implemented it.[41]

- **Australia** requires that local data centers be used as part of e-health record systems.[42] The rationale is to protect Australians' privacy and security. However, as discussed below, mandates on where data is stored do not improve privacy or security. Nevertheless, Australian IT companies have used this fear to promote protectionist policies that spare them from having to compete with U.S. technology companies.

- In 2014, **Indonesia** began considering a "Draft Regulation with Technical Guidelines for Data Centres" that would require Internet-based companies, such as Google and Facebook, to set up local data storage centers.[43] The Technology and Information Ministry is now implementing this regulation under the country's Electronic Information and Transactions (ITE) Law.[44]

- In **Russia**, amendments to the Personal Data Law mandate that data operators that collect personal data about Russian citizens must "record, systematize, accumulate, store, amend, update and retrieve" data using databases physically located in Russia.[45] This personal data may be transferred out, but only after it is first stored in Russia. Even the guidelines for this law, which went into effect in September 2015, acknowledge that there are significant ramifications for foreign companies due to this law.

- Many are also concerned that **Europe** will introduce data protectionist policies as part of its Digital Single Market, General Data Protection Regulation, and European Cloud initiatives.[46]

- In **Vietnam**, a Decree on Information Technology Services requires digital service providers or websites to locate at least one server within Vietnam. Vietnam had also put forth a draft IT Services Decree that would include additional data localization requirements as well as restrictions on cross-border data flows.

- **India** has considered a measure that would require companies to locate part of their ICT infrastructure within the country to provide investigative agencies with ready access to encrypted data on their servers.[47] In February 2014 the Indian National Security Council proposed a policy that would institute data localization by requiring all email providers to setup local servers for their India operations and mandating that all data related to communication between two users in India should remain within the country.[48]

- In **South Korea**, the Personal Information Protection Act requires companies to obtain consent from "data subjects" (i.e., the individuals associated with particular datasets) prior to exporting that data.[49] The act also requires "data subjects" to be informed who receives their data, the recipient's purpose for having that information, the period that information will be retained, and the specific personal information to be provided. This is clearly a substantial burden on companies trying to send their data across borders.

- Not surprisingly, given its history of rampant "innovation mercantilism," **China** is putting in place a wide array of protectionist measures on data. To start with, it has long limited data "imports." For example, the Ministry of Public Security runs the Golden Shield program (commonly referred to as the "Great Firewall of China"), which restricts access to certain websites and services, particularly ones that are critical of the Chinese Communist Party. But more importantly from a trade perspective, China has made a number of moves in the wake of the Snowden revelations to restrict the cross-border transfer of data.[50] For example, Chinese law prohibits institutions from analyzing, processing, or storing off-shore personal financial, credit, or health information of Chinese citizens. A recent set of draft administrative regulations for the insurance industry included localization requirements, both for data centers and cross-border data flows. Furthermore, China's Counter-Terrorism Law requires Internet and telecommunication companies and other providers of "critical information infrastructure" to store data on Chinese servers and to provide encryption keys to government authorities.[51] Any movement of data offshore must undergo a "security assessment." And China's draft cybersecurity law would require IT hardware to be located in China. China's policy framework to develop a domestic cloud computing capability also refers to the importance of regulating cross-border data flows.

Countries' Motivations for Limiting Free Trade in Data

Despite the vast benefits to companies, workers, consumers, and economies that arise from the ability to easily share data across borders, dozens of countries—in every stage of development—have erected barriers to digital free trade.[52] There are three main motivations for this: privacy and security concerns, national security and law enforcement concerns, and aspirations for economic growth. In almost all cases, though, more than one motivation plays a role.

For example, Europe's concerns about data trade stem in large part from its desire to protect citizens' privacy (although as noted below there are some in Europe who want to use these concerns as a justification for data protectionism in an effort to grow Europe's IT sector). As discussed below, effectively addressing privacy concerns should be the easiest of the three motivations to address. First, as ITIF has shown, requiring data not to leave a nation does little to increase privacy.[53] As long as the company involved has legal nexus in a European nation, it is subject to EU laws and regulations; moving data outside the EU does not give the company a free pass to ignore EU law. Moreover, the EU and the United States have long had a workable Safe Harbor agreement to address precisely these kinds of privacy concerns. And the European Court of Justice overturned the Safe Harbor not because of privacy concerns, but because of concerns about governmental access.

If privacy were the only motivation for Europe to restrict transatlantic data flows, then there should be no reason why Europe and America cannot work out a mutually agreeable solution. To be sure, compared to the United States, Europe has different laws and values with regard to privacy. But there are misconceptions about this on both sides of the Atlantic. Too many Americans believe EU privacy rules exclude even the most basic uses of data for commercial purposes and innovation, and too many Europeans believe that the United States is a "wild west" of data privacy. In fact, both sides share similar values with regard to privacy, the rule of law, and government access to data, and both benefit enormously from globalization and data innovation.

A second motivation for governments to require data to stay in country concerns the ability of governments to get access to data. This appears to be a motivation for many non-democratic governments, such as Russia and China, requiring that data be stored inside their borders. There is no question that localization policies such as these give government security services easier access to data. However, those nations do not need to mandate localization for their governments to legal access to data. They are still able to compel companies doing business in their markets to turn over data even if it is stored outside their nation. In truth, even this is not enough for some governments; they want the power to collect data without the knowledge of the company involved, and that is easier if the data are stored locally. For democratic nations that abide by the rule of law, there is no need for mandating data be stored domestically as long as there is a well-functioning and robust system of mutual legal assistance treaties (MLATs) in place as described below.

Finally, a number of countries see "data mercantilism" as a path to economic growth, because they believe (incorrectly) that if they restrict data flows they will gain a net economic advantage from data-related jobs.[54] And all too often they are spurred on by domestic IT companies seeking an unfair leg up over foreign competitors. For example, Australian businesses have used privacy and

security fears to promote protectionist policies that spare them from having to compete with U.S. tech companies. When Rackspace, a Texas-based cloud computing firm, built its first data center in Australia, MacTel—a domestic competitor—tried to stoke fears of U.S. surveillance efforts under the Patriot Act to push Rackspace out of the market.[55] In fact, 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.[56]

Similarly, some calls in Europe for data localization requirements and procurement preferences for European providers, and even for a so-called "Schengen area for data"—a system that would keep as much data in Europe as possible—appear to be motivated by digital protectionism.[57] For example, Germany has started to create a dedicated national network, called "Schlandnet."[58] And Deutsche Telecom is pushing the European Commission to adopt rules making it harder for U.S. cloud providers to operate in Europe in order for them to gain market share. Similarly, the French government has gone so far as to put €150 million into two start-ups, Numergy and Cloudwatt, to build domestic cloud infrastructure that is independent of U.S. tech companies.[59] French Digital Economy Minister Fleur Pellerin explains that France's goal is to locate data servers and centers in French national territory and to "build a France of digital sovereignty."[60]

But any economic benefits for countries from digital protectionism are far outweighed by the costs. Such requirements raise ICT costs not only by forcing companies to locate servers in locations that may not be the most cost-effective; they also force companies to operate at sub-optimal economies of scale. Barriers to cross-border data transfer for cloud computing add significant costs for local companies. Studies show that local companies would need to pay 30 percent to 60 percent more for their computing needs.[61] Businesses that move their cloud computing outside the European Union could save more than 36 percent because they could use global best in class providers.[62]

These increased costs are eventually passed along to data users, including businesses. As ITIF has shown, elasticity is quite high with information and communications technologies—ranging from 1 to 3—meaning that for every 1 percent increase in ICT costs, there is a 1 percent to 3 percent reduction in ICT consumption.[63]

Barriers to cross-border data flows can also stop research and development between a company and a foreign partner as they are not able to share all the data relevant to developing new services or processes.[64] For example, companies may not be able to use cloud computing to connect different research and development units. These barriers may force multinational companies to use second-best research partners. All of these factors hinder innovation.

This is why a 2013 report by the European Center for International Political Economy (ECIPE) estimated that if cross-border data flows were seriously disrupted, the negative impact on EU GDP would be between 0.8 percent and 1.3 percent.[65] This study also showed that the negative economic impact of recently proposed or enacted cross-border data flow restrictions would be substantial in a number of other nations, including Brazil, China, India, Indonesia, South Korea, and Vietnam. Likewise, a study into the impact of Russia's data localization laws shows an estimated economic loss

of 0.27 percent of GDP, equivalent to $5.7 billion, and a 1.4 percent decrease in investment.[66] But despite these costs, many nations persist in data protectionism.

Costs to the U.S. Economy of Foreign Digital Protectionism

As described above, the U.S. economy and U.S. workers benefit from cross-border data flows, in part because the United States is the global leader in the data economy. Foreign restrictions will impose costs on U.S. companies in a wide variety of industries. But particularly damaging are the costs to U.S. IT companies. One reason is that a number of nations have used the Snowden revelations as an excuse to impose protectionist data policies that will disproportionally hurt U.S. tech firms. 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 National Security Agency (NSA) revelations.[67] As a result, U.S. tech firms have seen losses across the world. For example, the U.S. cloud company Salesforce faced major short-term sales losses and suffered a $124 million deficit following the initial NSA revelations.[68] Cisco also 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.[69] These reports damaged the company's international reputation and prompted it to take extra precautions to thwart surreptitious actions by the NSA.[70] IBM, Microsoft, and Hewlett-Packard also have reported diminished sales in China as a result of the NSA revelations.[71]

In 2013, ITIF estimated that if concerns about U.S. surveillance practices caused even a modest drop in the expected foreign market share for cloud computing services, it could cost U.S. technology companies between $21.5 billion and $35 billion by 2016.[72] It has since become clear that not just the cloud computing sector but the entire U.S. tech industry has underperformed as a result of the Snowden revelations. Therefore, the economic impact of from the Snowden revelations will likely far exceed ITIF's initial $35 billion estimate.[73] Indeed, other estimates have put the figure somewhere around $47 billion.[74] As noted above, these costs are borne by U.S. workers and the U.S. economy overall, not just by tech company shareholders.

Where Are We Now?

The last few months have seen mixed progress on establishing movement toward free trade in data. On the one hand, the proposed TransPacific Partnership significantly advances the cause. But on the other, the European Court of Justice's invalidation of the U.S.-EU Safe Harbor agreement is a significant setback.

The digital trade provision in the Trade Promotion Authority Bill rightly puts the issue of cross-border data flows at the top of U.S. trade negotiators' agenda.[75] Reflected in the U.S. Trade Representative's top priorities for digital trade, which it refers to as the "Digital Dozen," these disciplines are necessary elements for trade agreements to promote an open Internet and an Internet-enabled economy.[76]

The TPP's e-commerce chapter is reported to contain rules explicitly prohibiting restrictions on cross-border data flows and data localization requirements. Ideally, the TPP should expand and strengthen the trade rules achieved under the e-commerce chapter of the Korea-United States FTA (KORUS), which included an agreement that both countries "shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[77] There has also been progress through the Asia Pacific Economic Community (APEC) process. In November 2011, APEC Leaders issued a directive to implement the APEC Cross Border Privacy Rules System (CBPR). The CBPR system balances the flow of information and data across borders while at the same time providing effective protection for personal information. The system is one by which the privacy policies and practices of companies operating in the APEC region are assessed and certified by a third-party verifier (known as an "Accountability Agent") and follows a set of commonly agreed upon rules, based on the APEC Privacy Framework. The Privacy Recognition for Processors (PRP) was recently endorsed by APEC in January 2015 and will be operationalized in the coming months. The PRP is designed to help personal information processors assist controllers in complying with relevant privacy obligations, and helps controllers identify qualified and accountable processors.

At the same time, when the European Court of Justice decided in early October 2015 to allow the High Court of Ireland to invalidate the U.S.-EU Safe Harbor agreement, it signaled that the Snowden revelations had called into question the mutual understanding that both parties share the basic goal of protecting their citizens' privacy in a digital world, even though they go about it differently—the EU, by adhering to comprehensive legislation, and the United States by taking a sector-by-sector approach that relies on a mix of legislation, regulation, and self-policing. Europeans have become wary because their laws provide a fundamental right to privacy, and they now believe that they are not getting an equivalent level of protection from the United States government. There is now a real risk of contagion as other nations look at the EU decision and decide – for privacy or protectionist motivations – to restrict data flows between the U.S. and their nation. Indeed, reportedly, Israel has also ruled that it would now not recognize that data transferred from Israel to the United States was covered under the EU-US Safe Harbor, as it previously had.[78]

But while European citizens and policymakers are understandably concerned about government access to their citizens' data, abruptly revoking the Safe Harbor agreement was the wrong way to address those concerns. It is disrupting not just to the thousands of U.S. and European companies that currently depend on the Safe Harbor to do business across the Atlantic, but also to the broader digital economy. Policymakers in the United States and EU should instead work together to swiftly implement an interim agreement so the court's ruling does not continue to adversely affect transatlantic digital commerce. At stake is the future viability of the world's most important economic relationship: If it is to continue flourishing in the age of digital commerce, then both sides must make accommodations.

Policy Steps to Enable Digital Free Trade

In many nations, trade negotiators are working to build an international consensus and enforceable regime for the free flow of data across borders. However, at the same time, law enforcement and intelligence communities are seeking to preserve or extend their access to data. These two goals are in fundamental tension and unless nations can put in place a reasonable and consistent framework to govern lawful government access to data, nations will be more likely to restrict cross-border data flows and trade, commerce, law enforcement, and intelligence gathering will all suffer. Indeed, the turbulence in the system now underscores the urgency of addressing these issues, both in terms of advancing new trade regimes to establish enforceable rules for free trade in data and in crafting international standards for government access to data.

The first step in shaping this new system will be to ensure that the U.S. government works to embed strong cross-border data flow protections in new trade agreements. The Obama administration has worked to enshrine strong and enforceable cross-border digital trade provisions in the TPP. But that agreement only applies to 12 nations. So the United States now needs to champion a Trade in Services Agreement (TiSA) that builds upon this language and to persuade as many nations as possible to sign on. TiSA currently covers 23 countries that represent 75 percent of the world's $44 trillion services market.

As the United States moves forward with Europe to negotiate the Transatlantic Trade and Investment Partnership, it will be important for U.S. trade negotiators to insist that strong cross-border provisions be included. Indeed, if the T-TIP is truly going to be a "21st century trade agreement," it must give data flows the same level of consideration it would have given manufacturing in a 20th century agreement.

But because data is so critical to the modern global economy, the United States and European Union should push further to protect the free and unfettered movement of data across the globe—for example by championing a "Data Services Agreement" at the World Trade Organization, which would commit participating countries to protect cross-border data flows and prevent signatory countries from creating barriers to them. It would be akin to the Information Technology Agreement (ITA)—which 54 countries commendably agreed to expand with 201 new product lines earlier this year—for cross-border data flows.

A key challenge to achieving a strong outcome in negotiations on upcoming trade agreements will be ensuring that privacy and national security exemptions are specific and narrow enough to ensure that members are not able to use these as an excuse for digital protectionism. These exemptions under existing international agreements, such as the General Agreement on the Trade in Services (GATS), are so vaguely defined and poorly enforced as to provide a huge loophole for data protectionism. Both issues are obviously legitimate public policy objectives for members and are common exemptions in trade agreements, but the challenge for negotiators is to ensure that the various parts of an agreement (such as on protecting personal information) are strong enough as to allow a stronger regime on cross-border data flows and localization.

In addition, those who argue that free trade provisions for data abrogate national privacy rules, and therefore should not be included in trade agreements, overlook the reality that data does not need to be stored locally to be secure or to maintain privacy protections, as ITIF has shown in a detailed report, *The False Promise of Data Nationalism*.[79]

With regard to privacy, it is important to understand that entities with legal nexus in another nation must adhere to the privacy laws that nation imposes when they leverage consumers' data in the course of their business activities; thus, where that data is stored is immaterial. It is either in compliance with the privacy laws and regulations of that nation, or it is not. For example, foreign companies operating in America must comply with the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA), which regulates U.S. citizens' privacy rights for health data, or the Gramm-Leach-Bliley rules regulating the privacy of financial data, whether they store a customer's data on their own server in the United States or on a third-party cloud server in another nation.[80] Likewise, there is no benefit to data security by mandating local data storage. Just as with privacy, companies cannot avoid a nation's data security requirements by simply storing data in another nation.

At the same time the United States pushes for stronger, broader, and more enforceable trade regimes on cross-border data protection, it must also lead on reform of government access to data. Otherwise, many nations will likely use the concern of government "snooping" as an excuse to restrict cross-border data flows, even if they have signed a trade agreement covering the issue.

In the pre-Internet era, with Westphalian borders, it was much easier to define a U.S. person versus a non-U.S. person. But when data can be generated, stored, and accessed from anywhere in the world, this old territory-based system is in need of significant modernization. If, for example, the U.S. government asserts that it has authority to compel U.S. technology companies to turn over data on a non-U.S. person that is stored overseas, then the end result will either be that countries will prohibit data from being stored with U.S. technology companies, or that market forces will lead in this direction, as domestic IT companies will market themselves as "NSA-proof." In either case, the U.S. intelligence community will have less access and U.S. technology companies will lose global market share, costing jobs here at home.[81]

To start with and to address European concerns about privacy protections for their citizens' data, the U.S. Senate should follow the House of Representatives' lead and pass the Judicial Redress Act, which would allow non-U.S. citizens in select nations to bring civil actions against the U.S. government if it violates the Privacy Act. Congress also should reform the Foreign Intelligence Surveillance Act to improve oversight, transparency, and accountability whenever the government gets a warrant to collect private data for national security purposes.

The United States should also take the lead in strengthening the Mutual Legal Assistance Treaty (MLAT) process so that, where appropriate, law enforcement can gain access to data overseas.

MLATs are agreements designed for law enforcement agencies to receive and provide assistance to their counterparts in other countries. The United States has MLATs with 64 nations.[82] Despite these arrangements, U.S. law enforcement agencies have complained that MLATs involve a "slow and cumbersome" process.[83] The best option for addressing these challenges is to strengthen the MLAT process so that it is not, as the government argues, too slow, and so that companies cannot take actions to make it difficult for government investigators to gain lawful access to data. The U.S. government should take the lead in creating a timely and efficient international framework for allowing governments to request access to data stored abroad. This framework would help meet the needs of law enforcement agencies operating in a digital world and keep the U.S. tech sector competitive globally by making border distinctions inconsequential for legitimate law enforcement requests. In addition, one immediate step in this direction is to bring the MLAT process into the digital age by creating a streamlined, online docketing system for all MLAT requests.[84]

To build on that, the United States and European Union should also lead in creating a "Geneva Convention on the Status of Data," as ITIF writes in *The False Promise of Data Nationalism.* The purpose of such a convention would be to resolve international questions of jurisdiction and transparency regarding the exchange of information. This would allow for the development of global rules on data sharing and ensure that legitimate concerns regarding privacy and cybersecurity are taken into account as cross-border data flows increase.

This multilateral agreement would establish specific rules for government transparency, create better cooperation for legitimate government data requests, and limit unnecessary access to data on foreign citizens. It would also settle questions of jurisdiction when companies encounter conflicting rules, assist nations in reassuring individuals at home and abroad that the era of mass electronic surveillance unencumbered by effective judicial oversight is at an end, and better hold nations accountable for respecting basic civil liberties. And just as the principles of the Geneva Convention are taught to soldiers in basic training, the principles of a Geneva Convention for Data should be taught to network administrators and IT professionals worldwide, thereby ensuring that the ethics of the agreement are embedded at all levels of industry and government.

Also, it is important for government to not oppose strong encryption to ensure consumers have access to secure technologies without government backdoors. FBI director James Comey reignited a long-running controversy recently when he argued that the encryption U.S. technology companies such as Apple and Google use on their devices could impede law enforcement's ability "to prosecute crime and prevent terrorism."[85] Comey wants U.S. tech companies to design a way for law enforcement officials to access the data stored on those devices. In addition to raising the obvious privacy and government overreach issues, this proposal would also weaken the security and global competitiveness of U.S. tech products.

It is understandable that law enforcement agencies, accustomed to a world where they can open mail and monitor phone calls easily, are nervous about unbreakable encryption. However, these agencies must accept the premise that some communication networks, especially those used by the most elite

criminals and terrorists, will inevitability "go dark."[86] If the U.S. government insists on backdoors in domestic products, those criminals and terrorists intent on avoiding surveillance will simply use devices made in countries that allow less vulnerable encryption. Rather than fight the tide of progress, law enforcement officials should work to find viable alternatives, such as analysis of other data sources and metadata, to solve and prevent crimes.

Europe has reforms to make, too, including fully embracing its planned digital single market. Individual members of the EU should not be able to set their own privacy rules or other digital policies, nor should they be able to overrule laws and regulations established at the European level, because that would fragment the digital marketplace and raise costs for consumers and businesses, as is happening now with the rejection of the safe harbor. More broadly, the purpose of establishing a digital single market cannot be to create a "fortress Europe" where European technology companies have an unfair leg up on foreign competitors. It should instead be the first step toward a more seamlessly integrated transatlantic market.

If the United States and Europe do not come together to resolve their differences on these data privacy and security issues, then both sides will suffer. U.S. companies need to be able to store and process European data in the United States, and vice versa, or it will harm all sorts of technology users, including small businesses and consumers. The better alternative is to build a durable privacy framework that provides the necessary safeguards and instills the requisite trust and confidence to drive long-term growth on both sides of the transatlantic digital economy.

Most urgently, now that the United States and Europe have settled the Umbrella Agreement for exchanging data related to criminal activities, policymakers should also finish the process of creating a Safe Harbor 2.0 with terms that give comfort to all parties. In particular, the updated agreement should reflect the EU request that a national security exception is used only to the extent that it is strictly necessary and proportionate for a given incident.

At the same time U.S. policy makers should insist that other nations not use variations in privacy laws as a justification for limiting free trade in data, whether policy makers in these nations are doing so out of a sincere concern for privacy or whether they are using privacy as a guise for data protectionism. If the EU precedent stands only one of two outcomes are possible. The first is that all nations will have to put in place domestic privacy rules as strict as Europe's, or in fact, as strict the nation with the strictest rules in the world. Otherwise, the nation with the strictest rules will simply say that data cannot leave its nation. To be sure, this is an outcome that most U.S. privacy advocates relish, for they have long advocated that the United States adopt EU-style privacy laws, ignoring the real economic and innovation costs that would come from doing so. And now they are using this breakdown to push their innovation-restricting policy agenda. But as noted above, it is a "red herring" to assert that the only way to protect commercial privacy and security of a nation's citizens' data is to restrict the export of that data. Moreover, the United States should not allow other nations to dictate U.S. laws and regulations about the Internet—doing so sets a dangerous precedent for other policy issues such as freedom of expression. The second possible outcome is that nations will

effectively levy a privacy tariff" on all companies in nations that do not adopt their rules, as they will have to use more complex and costly arrangements to transfer data across borders. Neither solution is acceptable in a global economy.

As such, if European policy makers are not willing to expeditiously come to a new agreement that allows data to flow relatively easily across the Atlantic, the United States Trade Representative should consider filing a WTO case against Europe. Striking down the Safe Harbor agreement protection was not only arbitrary and capricious but wrong. Europe has invalidated the Safe Harbor agreement with the United States on the grounds that EU citizen data is not safe from government access, but it still maintains that other nations with similar laws and practices provide adequate protection. Moreover, if anything, EU citizen data is safer from government access in the United States than it is in nations like Argentina and Israel, yet European privacy authorities and courts have not revoked data sharing agreements with either of those nations.

In conclusion, we need to protect the ability of individuals and companies to engage in data-driven commerce without geographic restrictions. Companies are using data in creative and wondrous ways to create new value for the global economy. Policymakers must be equally visionary in shaping rules that protect citizens' rights to privacy, without unduly encumbering data's catalytic economic growth and innovation potential. America's ability to grow its economy and jobs will depend on it.

Thank you again for this opportunity to appear before you today.

Endnotes

1. Stephen Ezell, "Digital Trade Act of 2013 Instrumental to Protecting and Empowering the Global Digital Economy," *Innovation Files*, December 12, 2013, http://www.innovationfiles.org/digital-trade-act-of-2013-instrumental-to-protecting-and-empowering-the-global-digital-economy/.
2. Robert D. Atkinson, Stephen Ezell, Scott Andes, and Daniel Castro, "The Internet Economy 25 Years After .com," (Information Technology and Innovation Foundation [ITIF]), March 5, 2010), https://itif.org/publications/2010/03/15/internet-economy-25-years-after-com.
3. Daniel Castro and Travis Korte, "Data Innovation 101: An Introduction to the Technologies and Policies Supporting Data-Driven Innovation" (Center for Data Innovation, November 4, 2013), http://www2.datainnovation.org/2013-data-innovation-101.pdf.
4. James Manyika et al., "Open data: Unlocking innovation and performance with liquid information" (McKinsey Global Institute, October 2013), http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information.
5. Peter Groves et al., "The big-data revolution in US health care: Accelerating value and innovation" (McKinsey & Company, April 2013), http://www.mckinsey.com/insights/health_systems_and_services/the_big-data_revolution_in_us_health_care.
6. James Manyika et al., "Unlocking the potential of the Internet of Things" (McKinsey Global Institute, June 2015), http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world.
7. Joseph Bradley et al., "Internet of Everything: A $4.6 Trillion Public-Sector Opportunity" (Cisco, 2013), http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf.
8. Paul Hofheinz and Michael Mandel, "Uncovering the Hidden Value of Digital Trade" (The Lisbon Council/Progressive Policy Institute, 2015), http://www.lisboncouncil.net/publication/publication/127-uncovering-the-hidden-value-of-digital-trade-towards-a-21st-century-agenda-of-transatlantic-prosperity.html.
9. Organization for Economic Cooperation and Development (OECD), "Data-driven Innovation, Big Data for Growth and Well—being," (OECD, October 2014), 73, http://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf.
10. Michael Mandel, "Data, Trade, and Growth" (Progressive Policy Institute, April 2014), http://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel_Data-Trade-and-Growth.pdf.
11. Ministry of Employment and the Economy, Industrial Competitiveness Approach (Helsinki: Ministry of Employment and the Economy, March 2013), 28.
12. OECD, "Data-driven Innovation, Big Data for Growth and Well—being," 109.
13. Stephen Ezell, "Data a Key Driver of Transatlantic Economic Growth," *Innovation Files*, July 23, 2015, http://www.innovationfiles.org/data-a-key-driver-of-transatlantic-economic-growth./.
14. Stephen Ezell, "Digital Trade Act of 2013 Instrumental to Protecting and Empowering the Global Digital Economy," *Innovation Files*, December 12, 2013, http://www.innovationfiles.org/digital-trade-act-of-2013-instrumental-to-protecting-and-empowering-the-global-digital-economy/.
15. *Digital Trade in the U.S. and Global Economies, Part 2*, United States International Trade Commission, August 2014, http://www.usitc.gov/publications/332/pub4485.pdf.
16. Ibid.
17. National Science Board (NSB), *Science and Engineering Indicators 2012*, (NSB, 2012), appendix table 6-13, Value added of ICT industries, by region/country/economy: 1990–2010.
18. International Trade Administration (ITA), *2015 Top Market Report Cloud Computing* (ITA, July 2015), http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf.
19. Shobhit Seth, "World's Top 10 Internet Companies," *Investopedia*, March 4, 2015, http://www.investopedia.com/articles/personal-finance/030415/worlds-top-10-internet-companies.asp.
20. European Commission, "Communications from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbor From the Perspective of EU Citizens and Companies Established in the EU," (European Commission, November 27, 2013), http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.
21. Matthieu Pélissié du Rausas et al., "Internet matters: The Net's sweeping impact on growth, jobs, and prosperity," (McKinsey Global Institute, May 2011), http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.
22. Mark van Rijmenam, "Ford Drives In The Right Direction With Big Data," *Datafloq*, July 5, 2015, https://datafloq.com/read/ford-drives-direction-big-data/434.
23. Doug Henschen, "Microsoft Azure Drives Ford Hybrid-Cloud Plan," InformationWeek, March 18, 2015, http://www.informationweek.com/strategic-cio/digital-business/microsoft-azure-drives-ford-hybrid-cloud-plan/d/d-id/1319533.
24. Jason Hiner, "How Ford reimagined IT from the inside-out to power its turnaround," *TechRepublic*, July 9, 2012, http://www.techrepublic.com/blog/tech-sanity-check/how-ford-reimagined-it-from-the-inside-out-to-power-its-turnaround/.

25. Business Roundtable, "Putting Data to Work" (Business Roundtable, 2015), http://businessroundtable.org/sites/default/files/reports/BRT%20PuttingDataToWork.pdf.
26. Matthew J. Slaughter, "How U.S. Multinational Companies Strengthen the U.S. Economy" (The United States Council Foundation, Spring 2009), http://www.uscib.org/docs/foundation_multinationals.pdf.
27. Mihir A. Desai, C. Fritz Foley, and James R. Hines Jr., "Domestic Effects of the Foreign Activities on U.S. Multinationals" *National Bureau of Economic Research* (May 2008), http://www.people.hbs.edu/ffoley/fdidomestic.pdf.
28. Jitao Tang and Rosanne Altshuler, "The spillover effects of outward foreign direct investment on home countries: evidence from the United States" (Oxford University Centre for Business Taxation, January 2015), http://www.sbs.ox.ac.uk/sites/default/files/Business_Taxation/Docs/Publications/Working_Papers/Series_15/WP1503.pdf.
29. U.S. Bureau of Economic Analysis, GDP-by-Industry Accounts (value added by industry, accessed December 12, 2012), http://www.bea.gov/iTable/index_industry.cfm; Robert J. Shapiro and Aparna Mathur, "The Contributions of Information and Communication Technologies To American Growth, Productivity, Jobs and Prosperity," (Sonecon, September 2011), http://www.sonecon.com/docs/studies/Report_on_ICT_and_Innovation-Shapiro-Mathur-September8-2011-1.pdf.
30. U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*.
31. John Maggiore, "Remote Management of Real-Time Airplane Data" (Boeing, 2007), http://www.boeing.com/commercial/aeromagazine/articles/qtr_3_07/AERO_Q307_article4.pdf.
32. Maggiore, "Remote Management of Real-Time Airplane Data"; Paul Mathai, "Big Data: Catalyzing Performance in Manufacturing" (Wipro, 2011), http://www.wipro.com/documents/Big%20Data.pdf.
33. Maggiore, "Remote Management of Real-Time Airplane Data."
34. Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries" (ITIF, February 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf?_ga=1.174884642.1240521073.1404749065.
35. The International Federation of the Phonographic Industry (IFPI), *Digital Music Report 2015, Charting the Path to Sustainable Growth* (IFPI, April 27, 2015), http://www.ifpi.org/downloads/Digital-Music-Report-2015.pdf.
36. Ibid.
37. Nigeria Federal Ministry of Communication Technology, *Guidelines for Nigerian Content Development in Information and Communications Technology (ICT)*, (Nigeria Federal Ministry of Communication Technology, 2013), http://www.nitda.gov.ng/documents/Guidelines%20on%20Nigerian%20Content%20Developmenet%20in%20ICT%20updated%20on%2012062014.pdf.
38. Ibid.
39. "No Transfer, No Trade" (Kommerskollegium (Swedish National Board of Trade, January 2014), 35, http://www.kommers.se/Documents/dokumentarkiv/publikationer/2014/No_Transfer_No_Trade_webb.pdf.
40. Business Roundtable, "Promoting Economic Growth through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements" (Business Roundtable, June 2012), 5, http://businessroundtable.org/uploads/studies-reports/downloads/Global_IT_Policy_Paper_final.pdf .
41. Ibid.
42. James Stamps and Martha Lawless, *Digital Trade in the U.S. and Global Economies, Part 1* (U.S. International Trade Commission, July, 2013), http://www.usitc.gov/publications/332/pub4415.pdf.
43. Matthias Bauer, Hosuk Lee-Makiyama, Erik can der Marel, and Bert Verschelde, "The Costs of Data Localization: Friendly Fire on Economic Recovery" (European Centre for International Political Economy, March 2014), http://www.ecipe.org/media/publication_pdfs/OCC32014__1.pdf.
44. Eli Sugarman, "How Emerging Markets' Internet Policies Are Undermining Their Economic Recovery," *Forbes*, February 12, 2014, http://www.forbes.com/sites/elisugarman/2014/02/12/how-emerging-markets-internet-policies-are-undermining-their-economic-recovery/.
45. "Russia's Personal Data Localization Law Goes Into Effect" (Duane Morris, October 16, 2015), http://www.duanemorris.com/alerts/russia_personal_data_localization_law_goes_into_effect_1015.html?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.
46. Nigel Cory, "The Architect of Europe's Digital Single Market Leaves Important Questions Unanswered on U.S. Visit," *Innovation Files,* October 2, 2015, http://www.innovationfiles.org/the-architect-of-europes-digital-single-market-leaves-important-questions-unanswered-on-u-s-visit/.
47. Business Roundtable, "Promoting Economic Growth through Smart Global Information Technology Policy."
48. Thomas K. Thomas, "National Security Council proposes 3-pronged plan to protect Internet users," *The Hindu Business Line*, February 13, 2014, http://www.thehindubusinessline.com/info-tech/national-securitycouncil-proposes-3pronged-plan-to-protect-internet-users/article5685794.ece.

49. Nnupam Chandler and Uyen Le, "Breaking the Web: Data Localization vs. the Global Internet" *Emory Law Journal* (April 2014), 40, http://papers.ssrn.com/sol3/papers.cfm.
50. Robert Atkinson, Stephen Ezell, and Michelle Wein, "Localization Barriers to Trade: Threat to the Global Economy" (ITIF, September, 2013), http://www2.itif.org/2013-localization-barriers-to-trade.pdf.
51. AmCham China, "Protecting Data Flows in the US-China Bilateral Investment Treaty" (AmCham China 2015 Policy Spotlight Series, April, 2015), http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization.
52. Ezell, Atkinson, and Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy."
53. Daniel Castro, "The False Promise of Data Nationalism" (ITIF, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.
54. For more information on mercantilism, see Michelle Wein, Stephen Ezell, and Robert Atkinson, "The Global Mercantilist Index: A New Approach to Ranking Nations' Trade Policies" (ITIF, October 2014), http://www2.itif.org/2014-general-mercantilist-index.pdf.
55. Adam Bender, "Patriot Act could apply to Rackspace data in Australia: Privacy advocates," *Computerworld*, August 27, 2012, http://www.computerworld.com.au/article/434683/patriot_act_could_apply_rackspace_data_australia_privacy_advocates/.
56. 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: Lateral Economics, "The potential for cloud computing services in Australia" (Lateral Economics, October 2011), http://www.lateraleconomics.com.au/outputs/The%20potential%20for%20cloud%20computing%20services%20in%20Australia.pdf
57. 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.
58. Ibid.
59. 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.
60. Chandler and Le, "Breaking the Web: Data Localization vs. the Global Internet."
61. Leviathan Security Group, "Quantifying the Cost of Forced Localization" (Leviathan Security Group, 2015), https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.
62. Ibid., 10.
63. Robert D. Atkinson and Ben Miller, "Digital Drag: Ranking 125 Nations by Taxes and Tariffs on ICT Goods and Services," (ITIF, October 2014), http://www2.itif.org/2014-ict-taxes-tariffs.pdf?_ga=1.3078388.571485694.1368547120.
64. Kommerskollegium, "No Transfer, No Trade."
65. Bauer et al., "The Costs of Data Localization: Friendly Fire on Economic Recovery."
66. Matthias Bauer, Hosuk Lee-Makiyama, Erik can der Marel, and Bert Verschelde, "Data Localisation in Russia: A Self-imposed Sanction" (European Centre for International Political Economy, June 2015), (http://www.ecipe.org/app/uploads/2015/06/Policy-Brief-062015_Fixed.pdf.
67. "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.
68. 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/.
69. 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-stech-losing-trust-overseas.
70. 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-strangeaddresses.html.
71. 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.
72. Daniel Castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry," (ITIF, August 2013), http://www2.itif.org/2013-cloud-computingcosts.pdf.
73. Daniel Castro and Alan McQuinn, "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness," (ITIF, June 2015), http://www2.itif.org/2015-beyond-usa-freedom-act.pdf?_ga=1.110906501.1240521073.1404749065.
74. Ed Ferrara and James Staten with Andrew Bartels, Glenn O'Donnell, and Josh Blackborow, "Government Spying Will Cost US Vendors Fewer Billions Than Initial Estimates," *Forrester*, April 1, 2015, https://www.forrester.com/Government+Spying+Will+Cost+US+Vendors+Fewer+Billions+Than+Initial+Estimates/fulltext/-/E-res122149.

75. Ian Fergusson, *Trade Promotion Authority (TPA) and the Role of Congress in Trade Policy* (U.S. Congressional Research Service, June 15, 2015), https://fas.org/sgp/crs/misc/RL33743.pdf.
76. United States Trade Representative's Office (USTR), "The Digital Dozen"(USTR, May 1, 2015), https://ustr.gov/sites/default/files/USTR-The_Digital_Dozen.pdf.
77. United States Trade Representative's Office, "United States – South Korea Free Trade Agreement – Chapter Fifteen – Electronic Commerce" (USTR), accessed October 29, 2015, https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf.
78. Francoise Gilbert, "Israel Revokes Acceptance of Safe Harbor," http://www.francoisegilbert.com/2015/10/israel-revokes-is-acceptance-of-safe-harbor/.
79. Emma Woollacott, "Leaked TISA Documents Reveal Privacy Threat," *Forbes*, June 4, 2015, http://www.forbes.com/sites/emmawoollacott/2015/06/04/leaked-tisa-documents-reveal-privacy-threat; Castro, "The False Promise of Data Nationalism."
80. Stephen Ezell, "Why Privacy Alarmists Are Wrong About Data Rules in Big Trade Deals," *Christian Science Monitor*, July 15, 2015, http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0715/Opinion-Why-privacy-alarmists-are-wrong-about-data-rules-in-big-trade-deals.
81. Daniel Castro, "Cross-Border Digital Searches: An Innovation-Friendly Approach," *InformationWeek*, September 5, 2014, http://www.informationweek.com/strategic-cio/digital-business/cross-border-digital-searches-an-innovation-friendly-approach/a/d-id/1306989.
82. U.S. Department of State, *2015 International Narcotics Control Strategy Report, Bureau of International Narcotics Control Strategy Report* (U.S. Department of State, 2015), http://www.state.gov/j/inl/rls/nrcrpt/2015/vol2/239045.htm.
83. Preet Bharara and Lorin Reisner, "Government's Memorandum of Law in Opposition to Microsoft's Motion," *Washington Post*, April 20, 2014, accessed October 30, 2015, http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/06/10/National-Security/Graphics/Government%27s Memorandum of Law in Opposition to Motion to Vacate (doc 97....pdf.
84. This is a key provision in the Law Enforcement Access to Data Stored Abroad Act (LEADS Act) currently before Congress.
85. David Sanger and Matt Apuzzo, "James Comey, F.B.I. Director, Hints at Action as Cellphone Data Is Locked," *New York Times*, October 16, 2014, http://www.nytimes.com/2014/10/17/us/politics/fbi-director-in-policy-speech-calls- dark-devices-hindrance-to-crime-solving.html?_r=0; Craig Timberg, "Newest Androids will join IPhones in offering default encryption, blocking police," *Washington Post*, September 18, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.
86. Valerie Caproni, "Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security," (Federal Bureau of Investigations, February 17, 2011), http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies.