ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of

Robert D. Atkinson, Ph.D.

Founder and President

Information Technology and Innovation Foundation

Before the

Committee on Ways and Means

Trade Subcommittee

Hearing on

"Expanding U.S. Digital Trade and Eliminating Barriers to Digital Exports"

July 13, 2016

1100 Longworth House Office Building

Washington, DC

The Information Technology and Innovation Foundation (ITIF) appreciates the House Ways and Means Trade Subcommittee's invitation to testify regarding the importance of digital trade to the U.S. and global economy and the need to secure trade rules that ensure both fair competition in global digital trade and the seamless movement of data and information across international borders.

ITIF is a nonpartisan 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.

Data and Digital Trade as the Key Drivers of the Modern Global Economy

Data and digitalization are increasingly the driving forces of innovation and growth in the modern global economy. For example, TEKES (Finland's Technology and Innovation Agency) recently estimated that, by 2025, fully half of all value generated in the global economy will be created digitally. Similarly, a report released in March 2016 by the McKinsey Global Institute finds that the global value of international data flows in 2015—$2.8 trillion—exceeded the value of global merchandise trade for the first time.[1] The McKinsey report further estimates that almost one-quarter, or 22 percent, of global economic output can be attributed directly to the digital economy and notes that the application of digital technologies—such as cloud computing, data analytics, and the Internet of Things—will increase global GDP by $2 trillion by 2020.[2] And, as ITIF has shown, a wide array of industries, from manufacturing to mining to retail and financial services, depend on cross-border data flows.[3]

The contribution of digital technologies to the modern global economy is an extension of the role of information technology (IT) on growth. For example, 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.[4] And the McKinsey Global Institute has estimated that, for 13 of the world's largest economies between 2007 and 2011, the Internet alone accounted for 21 percent of aggregate GDP growth.[5]

The United States holds a distinct leadership role in the fast-growing data economy owing to its role as a pioneering innovator and early adopter of IT, coupled with an Internet regulatory regime, particularly a light touch for privacy, which enables innovation. As of 2010, U.S. firms held a 26 percent share of the global IT industry and were the world's largest producers of IT goods and services.[6] Of the top 20 enterprise cloud computing service providers in the world, 17 are headquartered in the United States.[7] Of the top 10 Internet firms, 7 are headquartered in the United States.[8] The digitally enabled services that these firms provide 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.[9] The United States exports over $162 billion worth of digital services to Europe annually.

Moreover, it is increasingly the case that many of the benefits from information technology come from creating value and insights from data, often in real-time. Virtually every sector of the U.S. economy benefits from the data revolution; the applications for data processing and analytics are quite large. And this value will only increase as the public and private sectors alike become more data-driven.[10] 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.[11] In the United States, the use of big data in health care can save $450 billion per year.[12] Industry forecasters estimate that, by 2025, the Internet of Things will have an economic impact of up to $11.1 trillion per year.[13] And for the global public sector, the Internet of Things is expected to create $4.6 trillion in value by 2022.[14] Even Europe could grow more quickly if it more fully embraced data and the digital revolution.[15]

Why Free Trade in Data is Vital

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 Organization for Economic Cooperation and Development (OECD) noted 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 centers 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 labor 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.[16]

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.[17] This is why—absent policy-created "data protectionism"—digital trade and cross-border data flows are expected to continue to grow much faster than the overall rate of global trade.

As a result, the ability to move data across borders has become 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."[18] In fact, fully half of all global trade in services now depends on access to cross-border data flows.[19] And, as noted, 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.[20]

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).[21] The ITC further estimates that digital trade increased average wages and helped create 2.4 million American 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 estimates that decreasing barriers to cross-border data flows would increase U.S. GDP by 0.1 to 0.3 percent.[22] 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 (SMEs), 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.

Free trade in data is important not just to technology firms, but also to traditional industries, such as automobile manufacturers, mining companies, banks, airlines, hospitals, and grocery store chains—all of which depend upon 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 erstwhile U.S.-EU Safe Harbor Agreement, 51 percent did 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.[23] 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.[24]

There are numerous examples of U.S. firms, large and small alike, 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.[25] 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 that Ford serves as customers' "data steward." For internal purposes, performance data is de-identified and analyzed to track potential performance and warranty issues.[26] Ford uses a U.S. cloud service provider to host this data.[27]

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.[28]

When nations impose restrictions on data flows, the U.S. economy is harmed in at least three ways. First, policies such as requiring localization of data or computing infrastructure will move activity from the United States to these nations, reducing jobs and investment here and raising costs for U.S. firms. Second, cross-border data restrictions will increase costs and limit innovation for U.S. firms. Third, 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, domestic-serving 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 overall 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.[29] 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.[30] Another study of U.S. multinational corporation services firms found that affiliate sales abroad increase U.S. employment by promoting intra-firm exports from parent firms to foreign affiliates.[31] In short, when U.S. multinationals firms, regardless of size, 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, management, and engineering, computer science, and technical jobs. And this matters because, as ITIF has shown, IT workers earned 74 percent more than the average American 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.[32] Finally, digital trade does not just benefit large companies such as Amazon, Ford, GE, IBM, or P&G. Small- and medium-sized U.S. enterprises account for one-quarter of digital trade sales and fully one-third of digital trade purchases.[33]

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 individuals 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 motorists' vehicles.

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, Illinois, 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.[34] For example, a Boeing 737 engine produces 20 terabytes of data per hour.[35] 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.[36] 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.[37] Likewise, when General Electric (GE) Aircraft Engines develops engine maintenance and service plans for its airline customers, it customizes the entire package based upon data showing the individual service history (e.g., hours flown, weather conditions flown in, etc.) of each of the jet engines in the airline customers' entire fleet.

Another reason the digital trade linkage between products and services is so important is that the increasing phenomenon of "servicization" means that products are increasingly being sold as services. For example, GE no longer sells individual radiological equipment (e.g., MRI or X-Ray machines) to hospitals; rather it sells radiological services, whereby GE takes over for example a hospital's entire suite of radiological assets, installing the devices with remote-monitoring capabilities that allow GE to know if they are operating and functioning properly or to diagnose various failure models. In other words, GE is selling its products as a package of bundled services, with the quality of GE's service offering being dependent on the digital data stream produced by its devices. (In a like manner, GE's Aircraft Engines division no longer sells airlines individual jet engines; it sells them "guaranteed thrust." And Johnson Controls no longer sells individual heating or air conditioning units; it sells to customers a service—"chilled air.") The point is that these "servicized" business models account for an increasingly large share of the economy—and digital trade—and they depend upon the free flow of unfettered data across borders; any trade restrictions that impede the free flow of such information imperil these digital-data-predicated business models.

The free flow of data will also enhance overall "data innovation," which is playing 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 a country.[38] 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."[39] 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 or illegal drugs 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.

The Barriers to Global Digital Trade

Data for legal goods and service will naturally flow across borders when it needs to, unless nations erect digital barriers that impede it. Unfortunately, despite the vast benefits to companies, workers, consumers, and economies that arise from the ability to easily share data across borders, dozens of countries—both developed and developing alike—have erected a wide slate of barriers to digital trade.[40] The nations that have enacted such barriers proffer three main types of "justifications" for these policies: privacy and security concerns, national security and law enforcement concerns, and aspirations for domestic economic growth. In almost all cases, though, more than one motivation plays a role. But as the following discussion elaborates, none of these justifications validate the digital trade barriers all too many countries are increasingly erecting.

First, some nations have raised privacy concerns, contending that data, if transferred overseas, is somehow inherently less secure. But as ITIF has demonstrated in a detailed report, *The False Promise of Data Nationalism*, 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 commercial privacy protections.[41] For example, Europe's concerns about data trade stem in large part from its desire to protect citizens' privacy. However, effectively addressing privacy concerns should be the easiest of the three motivations to address. As long as the company involved has legal nexus in a nation, it is subject to the privacy and cybersecurity laws and regulations of that nation—moving data overseas, or storing it elsewhere, does not give the company a free pass to ignore a nation's (or European Union's) laws. 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 elsewhere) or on a third-party cloud server in another nation.[42]

The focus of discussions on cross-border data flows should be on the actual issue (e.g. privacy or cybersecurity), rather than the geographic location of the data. The new Privacy Shield agreement between the United States and the European Union attempts to address this. The Privacy Shield agreement shows that while the United States and Europe have different laws and values with regard to privacy, these can be addressed in a manner that that does not restrict or block data flows. One of the reasons why the Privacy Shield negotiations have become so heated is that there are misconceptions about how each respective side treats privacy. Too many Americans believe European Union (EU) privacy rules exclude even the most basic uses of data for commercial purposes and innovation, while too many Europeans believe that the United

States is a "wild west" in terms 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. Moreover, as ITIF has written, as long as U.S. firms have physical nexus in Europe, European privacy law continues to apply for European data U.S. firms collect, regardless of where they store that data.[43]

Second, some governments require data to stay in-country due to concerns over the ability of governments to get access to data. This appears to be a motivation for many non-democratic governments, such as China and Russia, which require 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 have 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 subsequently.

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.[44] Many nations that invoke privacy and security concerns as a justification to impede cross-border data flows are often simply commandeering these issues as a smokescreen for naked data protectionism. And all too often countries do so spurred on by domestic IT companies seeking an unfair leg up over foreign competitors. For example, Australian businesses have trumped up privacy and security fears to promote protectionist policies that spare them from having to compete with U.S. (and other foreign) technology 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 Australian market.[45] 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.[46]

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 pure digital protectionism.[47] For example, Germany has started to create a dedicated national network, called "Schlandnet."[48] And Deutsche Telecom has pushed 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 up a domestic cloud infrastructure ("*le cloud souverain*") that is independent of U.S. technology companies.[49] French Digital Economy Minister Fleur Pellerin has explained that France's goal is to locate data servers and centers in French national territory and to "build a France of digital sovereignty."[50]

Examples of countries enacting barriers to cross-border data flows are rife:

- **Australia** requires that local data centers be used as part of e-health record systems.[51] The purported rationale is to protect Australians' privacy and security. However, as noted, 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.

- **China**, not surprisingly, given its history of rampant "innovation mercantilism," has implemented a wide array of protectionist measures on data. To start with, it has long limited data "imports." For example, China's 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. As the United States Trade Representative's Office recently noted, China's "outright blocking of websites appears to have worsened over the past year [2015]."[52]

  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 movement of data.[53] 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 telecommunications companies and other providers of "critical information infrastructure" to store data on Chinese servers and to provide encryption keys to government authorities.[54] 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.

- **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.[55]

- Many are concerned that **Europe** will introduce data protectionist policies as part of its Digital Single Market, General Data Protection Regulation (GDPR), and European Cloud initiatives.[56] The GDPR proclaims data privacy to be a fundamental human right; introduces a "right to be forgotten," which Europe is attempting to apply to the whole of the global Internet; and proposes significant fines—as high as €100 million or up to 5 percent of an enterprise's annual revenue—for firms found to be in violation of European data protection laws.

  Certain EU Member States have instituted measures that require news aggregators, which provide snippets of text from other news sources, to remunerate those other sources for use of the snippets. These measures serve as an arbitrary tax on firms that help drive traffic to publishing sites. After Germany implemented such measures, some aggregators dropped links to sites seeking compensation

for use of the indexed extracts and related links, causing many publishers to opt out of requiring such payments. In late 2014, Spain passed a similar measure which made such payments mandatory.[57]

In short, all too often European digital trade policies are animated by a desire to impede the competitiveness of American digital or information technology-based enterprises competing in European markets. As Juliette Garside divulged the sentiment in 2014 in *The Guardian*, writing that, "Brussels and Berlin are mobilizing to defend…the digital environment of Europe's inhabitants; their enemies are the Silicon Valley corporations that seek to dominate it."[58] Such thinking, too prevalent in Europe, hinders digital trade, to the harm of both Europe's and America's economy alike.

- **India** has considered a measure that would require companies to locate part of their information and communications technology infrastructure within the country to provide investigative agencies with ready access to encrypted data on their servers.[59] 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 further mandate that all data related to communication between two users in India should remain within the country.[60]

- 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.[61] The Technology and Information Ministry is now implementing this regulation under the country's Electronic Information and Transactions Law.[62] The Indonesian government may pursue regulation or national legislation on personal data protection in 2016, either of which could further define requirements for data localization.[63]

- In 2010, **Malaysia** passed the Personal Data Protection Act, which requires data about Malaysians to be stored on local servers.[64]

- In 2010, **New Zealand's** tax collection agency, the Commissioner of Inland Revenue, issued guidance that electronic business and tax records must only be stored in New Zealand.[65]

- In 2014, **Nigeria** put into effect the "Guidelines for Nigerian Content Development in Information and Communications Technology." Several of the provisions regard restrictions on cross-border data flows and mandate that all subscriber, government, and consumer data be stored locally.[66]

- In **Russia**, amendments to the Personal Data Law mandate that data operators which collect personal data about Russian citizens must "record, systematize, accumulate, store, amend, update and retrieve" data using databases physically located in Russia.[67] 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.

- 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.[68] The Act also requires "data subjects" to be informed about whom 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.

- **Turkey** passed a law in 2014 mandating that companies process all digital payments inside its borders. This regulation caused PayPal to suspend its Turkish operations on May 31, 2016 after the country's financial regulators rejected its license applications—on the grounds that PayPal did not keep its IT systems in Turkey.[69]

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

- In **Vietnam**, a Decree on Information Technology Services requires digital service providers or websites to locate at least one server within Vietnam.[70] 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. Vietnam is also establishing a national payments gateway that discriminates against foreign electronic payment services—favoring a new local firm called "NAPAS"—in direct contravention of its Trans-Pacific Partnership (TPP) commitments.

The examples above show that digital trade barriers vary in terms of scope and scale, but while some are blanket policies that affect all data or e-commerce, there are a few specific sectors and processes that are the specific target, such as cloud computing and electronic payment processing.

Cloud computing services are often a specific target of data localization policies as countries think that this will lead to the development of local data centers. These countries think that data localization is a quick way to bring economic activity within their borders, but in reality, such policies cause more harm than good. The supposed benefits of data localization policies are misunderstood. As data centers become more automated, the number of jobs associated with each facility, especially for technical staff, decrease. While data centers contain expensive hardware and create some temporary construction jobs, they employ relatively few full-time staff to operate the equipment, especially as cloud-based technologies have increased automation in data centers.[71] The short-term benefit of these jobs is outweighed by the substantial costs to build unnecessary data centers, a cost which is ultimately passed on to business and consumer customers.

Barriers to cross-border data transfers for cloud computing add significant costs for local companies. Studies show that local companies would need to pay 30 to 60 percent more for their cloud computing needs when they are compelled to use local vendors and as opposed to global best-of-breed providers. For example, it is estimated that businesses that move their cloud computing outside of the European Union, in the event of a "European Cloud," could save more than 36 percent.[72] India, Indonesia, and Russia have no cloud computing providers from key global data centers, thereby forcing local companies to build their own or use

cloud providers that are not the most efficient or secure. Cross-border data flow restrictions go against the very distributed design of the Internet and do not achieve the goals often cited for such misguided policies.

Electronic payment services are also often targeted by data localization and other regulations in a way that effectively acts as a barrier to digital trade, often enacted to favor a local firm. Such services, through credit card companies (such as Visa and MasterCard) or online providers (such as PayPal), are critical enablers of the global digital economy and are closely tied to trade flows. Such cross-border transactions are growing rapidly as technology, consumer preferences, and services continues to change and as more people in more countries, especially emerging economies, gain access to the Internet and online e-commerce platforms.

As global electronic payment services grow, more countries are trying to capture this activity for local firms by introducing protectionist policies. In 2010, the United States won a legal case against China at the World Trade Organization for measures it had introduced that discriminated against foreign payment providers—a critical win given the large and growing role of the Chinese market for these services. Recognizing the rise of these measures, the TPP's financial services chapter explicitly prohibits member countries from introducing measures that act as a barrier to the cross-border delivery of electronic payment card services. Despite this provision, it is disappointing to learn that Vietnam—despite this being raised as an issue by the United States Trade Representative—is pursuing measures that directly contravene this provision by enacting a barrier that favors a new local firm over foreign service providers.

The Trans-Pacific Partnership (TPP)—Breaking Down and Protecting Against Digital Trade Barriers

The TPP's e-commerce chapter takes a number of positive steps in pushing back against barriers to digital trade. The TPP is the first trade agreement to include provisions that prohibit barriers to cross-border data flows and forced data localization, thus outlawing the practice of requiring companies to store data or setup computing facilities within a country's borders as a condition of competing in domestic markets. These updated rules are sorely needed as current World Trade Organization (WTO) rules were largely codified in the 1990s when the Internet as we know it barely existed, as did even the concept of digital protectionism. As demonstrated by the examples above, the failure of these rules to adapt to modern trade has allowed countries to introduce a range of barriers to cross-border data flows.

The TPP's e-commerce chapter recognizes the vital importance of digital trade to the modern global economy. The e-commerce chapter addresses a range of issues that enable digital trade, including provisions that:

- Prohibit countries from imposing customs duties on electronic transmissions and digital goods;
- Prohibit countries from discriminating against digital products as compared to tangible goods and services;
- Prohibit requirements that force suppliers to share valuable software source code with foreign governments or commercial rivals as a condition of entry;

- Facilitate the recognition and use of electronic authentication and signatures;
- Ensure countries have measures against unsolicited emails (spam); and
- Ensure that countries have laws and regulations that protect consumers from fraudulent and deceptive activities and protect personal information online, and sets up a mechanism for countries to cooperate on a range of e-commerce related issues.

The TPP's primary contribution to developing a modern set of rules for digital trade is its provisions addressing localization. The TPP's key provisions prohibit countries from enacting barriers to cross-border data flows or from enacting requirements that companies must use local (or locate their own) computing facilities within a country as a condition of doing business in that country.[73] These provisions are indeed groundbreaking, as before there were no rules in place that protected and enabled cross-border data flows. These rules also go a long way to setting a new norm for the global digital economy, as TPP member countries are home to close to 600 million Internet users, or almost one in every five global Internet users. The TPP's impact on global e-commerce and data flows will only grow if more countries join the agreement—as will happen if Indonesia, the Philippines, South Korea, Thailand, and others follow through on their expression of interest in joining the TPP—or if these provisions are adopted in other trade agreements.

However, how effective these rules will be in removing existing—and preventing future—barriers to digital trade depends in part on how TPP members interpret, enact, and enforce these rules, especially the exceptions to each of these provisions. The provisions prohibiting barriers to cross-border data flows and forced localization each contain an exception that nothing in these provisions "shall prevent a party from adopting or maintaining measures inconsistent [with the prohibition] to achieve a legitimate public policy objective." In terms of what is a legitimate public policy, the TPP refers to current World Trade Organization exemptions for public morals, public order, and privacy.[74] Such provisions would clearly be legitimate, for example, in the case of blocking child pornography; they would not be if a government refused to allow insurance companies to locate their data on servers in another nation. The lack of legal jurisprudence (e.g., countries challenging digital trade barriers in a legal dispute at the WTO) on these exceptions makes it unclear whether barriers to data flows enacted due to privacy and cybersecurity concerns are technically allowed or not.

This raises the prospect that TPP member countries' existing barriers to cross-border data flows, such as for privacy reasons (such as in Australia, Canada, and Malaysia) or national security reasons (such as Vietnam), may be allowed to remain in place (or even be potentially copied by other TPP members). The TPP includes language that tries to limit the potential for such exceptions to be misused by stating that any rule that contravenes these prohibitions "is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade" or "does not impose restrictions…greater than are required to achieve the objective." However, the effectiveness of these limitations will likely depend in part upon implementation, and potentially, enforcement through the TPP's dispute resolution mechanism to

determine whether such barriers to data flows are indeed an unjustifiable trade barrier and/or unnecessarily restrictive.

The TPP's much-improved framework for digital trade and data flows was let down in one key area—financial data. The United States undermined its own interests in the TPP by pushing for the financial sector to be exempted from the agreement's prohibitions on measures that would force data to be stored within a country's geographic borders. This rule, made at the insistence of U.S. financial regulators, unfortunately undermined the United States' natural position as a leader of the global digital economy and as an advocate for the free flow of data.

As ITIF argued in its report, *Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements*, the TPP's special treatment of financial data was unnecessary and redundant, given financial regulatory reforms introduced after the global financial crisis (in the Dodd-Frank Wall Street and Reform and Consumer Protection Act) and existing trade provisions that provide an exemption for prudential regulation.[75] This special treatment of financial data was also dangerous as it created a pernicious loophole that could be misused for protectionist purposes by other countries, such as China, India, or Russia. Allowing forced local storage for financial data on regulatory grounds could have been the start of a slippery slope that allowed these countries and others to force local data storage for other types of data, such as health and education, based on broadly and poorly defined "regulatory" concerns.

Making a special case out of financial data would be highly problematic. Giving countries a free pass to require certain data to be stored inside their borders would raise costs for U.S. financial services firms, and the firms would likely pass those costs on to the businesses and customers they serve. The special carve out also validates the false impression that moving data across borders is somehow inherently riskier than storing it locally, which would embolden data mercantilists and undermine U.S. efforts to push back against such measures.

Thankfully, the Obama administration has recognized that this provision needs fixing. Reports on the outlines of this fix indicate it will go a long way toward removing this loophole. The fix sets out specific steps to facilitate regulatory access to financial data among TPP member countries, and in doing so, makes any potential localization a truly final resort, while ensuring that countries remain committed to not enacting policies that require data localization or other barriers to data flows.[76] As ITIF has argued, in an ideal world this provision would be dropped completely from the TPP and any other future U.S. trade agreements.[77] However, given the position of financial regulators, the fix seems to find a middle ground for facilitating data flows and legitimate government access to data.

Looking Ahead—Building on TPP in TiSA and T-TIP

The last few months have seen mixed progress on establishing movement toward free trade in data. 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. However, the United States' recent success in negotiating the TPP, the Umbrella Agreement with the European Union (which enables sharing of law enforcement data), and the Privacy Shield (which manages privacy related data issues) shows that success is possible. Another productive step has been congressional passage of the U.S. Judicial Redress Act (since incorporated as part of the Privacy Shield), which grants EU citizens standing to sue the U.S. government concerning its collection of EU data.

Nevertheless, a key challenge to achieving strong outcomes on data flows in 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. As noted, the exemptions under existing international agreements, such as the WTO's General Agreement on the Trade in Services (GATS), are widely referenced and used in bilateral and regional trade agreements, but are vaguely defined and untested by legal challenges, thereby providing a loophole for data protectionism. The United States should use trade agreements and other international mechanisms to push for greater information sharing and cooperation on the legitimate and practical concerns involved in improving a country's cybersecurity and privacy protections. This reduces a country's ability to misuse concerns over these issues as a guise to enact data protectionist policies. As with the TPP, this involves cooperation on a wide range of issues such as protecting personal information, protecting consumers online, cybersecurity, and government access to online information. Directly addressing these legitimate concerns will allow stronger rules on cross-border data flows and localization.

The Trade in Services Agreement (TiSA) is the United States' most immediate opportunity to build on the TPP. A high-standard TiSA agreement would effectively set a new global norm for rules that support and protect the free flow of data. This is because TiSA has a large and diverse membership of developed and developing countries—it includes 15 non-TPP members, including the European Union, Colombia, Pakistan, South Korea, Taiwan, and Turkey. TiSA countries represent 75 percent of the world's $44 trillion services market.

As ITIF argues in *Crafting an Innovation-Enabling Trade in Services Agreement*, for TiSA to build and improve upon the TPP's efforts to address data localization it needs to explicitly cut the false link between geography and data policies concerning privacy and cybersecurity.[78] This should be a key litmus test to evaluate any final agreement. The United States should not budge from its commitment to use TiSA to enact strong rules to protect data flows, especially as more countries are likely to sign onto TiSA after it is completed. TiSA member countries are already discussing how the agreement can be expanded from a plurilateral agreement outside the WTO (which it is now) into a multilateral agreement under the WTO. Such an expansion means the rules in TiSA would formally become the core of the international trading system for services and data.

Holding firm to this commitment is important because as much as TiSA's membership is notable for whom is involved, it is equally important to recognize which countries are not—data mercantilists such as China, India, Indonesia, and Russia. An upfront commitment for these countries to join TiSA should for be for them to remove data localization measures, practices and other barriers to cross-border data flows.

The United States has another significant opportunity to shape the rules governing digital trade in its critical negotiations for a Transatlantic Trade and Investment Partnership (T-TIP) with the European Union. U.S. trade negotiators must insist that strong cross-border data provisions be included. 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.

Unfortunately, the prospects for T-TIP to set new standards for unimpeded digital trade and data flows are not looking sanguine. First, the United Kingdom's decision to leave the European Union will likely delay further negotiations as European Union countries re-evaluate their positions in T-TIP (minus the United Kingdom) as the United Kingdom and the European Union try to figure out how to reconfigure arrangements for trade, political, and other issues. Second, T-TIP negotiations over digital trade and data flows have lagged other issues, as the European Union has proven unwilling to discuss these issues until the transatlantic data transfer agreement, the Privacy Shield, is in place.[79] While the European Union's efforts to negotiate and implement the Privacy Shield agreement are commendable, they should not hold back efforts to create a broader framework to support digital trade and the free flow of data. Thankfully, the European Union recently announced that Privacy Shield should be implemented shortly, so hopefully T-TIP negotiations can catch up after this happens.[80] Finally, when negotiations do start in earnest, they are likely to be challenging as a growing range of EU policymakers are turning against trade and are attached to the notion that data needs to be stored locally for it to be secured or for privacy to be maintained. All these factors, when taken together, pose a great threat to T-TIP which, to be effective, needs to include data localization measures.

The challenge now for forward-looking policymakers will be to approve TPP, focus on TiSA and T-TIP, and look beyond them. The United States 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. 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 concern over government "snooping" as an excuse to restrict cross-border data flows, even if they have signed a trade agreement covering the issue.

To address this, the United States and European Union should collaborate toward 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.

The United States could also strengthen its MLAT regime by having the government expedite and simplify the MLAT process through a variety of measures such as increased funding for the Department of Justice's Office of International Affairs and the introduction of standardized, online requests. It could also allow countries with high human rights standards to join the eventual U.S.-UK MLAT agreement.

At the same time U.S. policymakers should insist that other nations not use variations in privacy laws as a justification for limiting free trade in data, whether policymakers 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 (for data privacy policies) 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 as 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. When firms using the Internet cannot use data effectively because of draconian privacy rules, the result, as studies have shown, is less revenue, meaning a less robust Internet ecosystem.[81] In fact, in looking at the impacts of the European Union's previous (2002) Privacy and Electronic Communications Directive (PECD), Avi Goldfarb and Catherine Tucker found that they resulted in an average reduction in the effectiveness of online ads of approximately 65 percent.[82] The authors write "the empirical findings of this paper suggest that even moderate privacy regulation does reduce the effectiveness of online advertising, that these costs are not borne equally by all websites, and that the costs should be weighed against the benefits to consumers." If European advertisers reduced their spending on online advertising in line with the reduction in effectiveness resulting from stricter privacy regulations, "revenue for online display advertising could fall by more than half from $8 billion to $2.8 billion." And without that revenue it has been more difficult for European Internet firms to thrive. And now many U.S. privacy advocates are using this breakdown to push their innovation-restricting policy agenda to impose European-style privacy regulations onto the United States. But as noted above, it is a "red herring" to assert that the only way to protect the commercial privacy and security of a nation's citizens' data is to restrict the export of that data. Companies simply cannot escape legal responsibilities for data by moving it outside of a nation. Moreover, the United States should not allow other nations to dictate U.S. laws and regulations about the Internet when doing so

will have no effect on trade—doing so would set a dangerous precedent for other policy issues, such as freedom of expression.[83]

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 G20 countries increasingly consider digital trade issues, another step the United States should take is to work to obtain G20 leaders' endorsement of the OECD Internet policymaking principles, which include allowing cross-border information flows and respecting human rights, as well as endorsement of interoperable privacy protection, such as APEC's privacy framework.[84]

Conclusion

In conclusion, data is the lifeblood of the modern global economy. The TPP represents the best opportunity to establish high-standard rules that will permit digital trade to flourish to the maximum possible extent—and ensure that U.S. enterprises, many of which have pioneered the creation and innovative use of the Internet and other digital technologies, can enjoy more open access to partners' markets and be able to seamlessly move data across international borders. If the TPP is not adopted the global digital economy will be put at risk, because a significant opportunity will be lost to put an affirmative stake in the ground demonstrating that localization barriers to digital trade are unacceptable in the modern global economy. The United States should view the TPP as a building block toward stronger and more comprehensive rules for digital trade and data flows in TiSA, T-TIP, and elsewhere. The United States should use these trade agreements 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. James Manyika et al, "Digital Globalization: The New Era of Global Flows" (McKinsey Global Institute, March 2016), http://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi%20digital%20globalization%20executive%20summary.ashx.
2. Ibid.
3. 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?_ga=1.174884642.1240521073.1404749065.
4. Robert D. Atkinson, Stephen Ezell, Scott Andes, and Daniel Castro, "The Internet Economy 25 Years After .com" (Information Technology and Innovation Foundation), March 5, 2010), https://itif.org/publications/2010/03/15/internet-economy-25-years-after-com.
5. 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/.

6. 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.
7. International Trade Administration (ITA), "2015 Top Market Report Cloud Computing" (ITA, July 2015), http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf.
8. 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.
9. Ezell, "Digital Trade Act of 2013 Instrumental to Protecting and Empowering the Global Digital Economy."
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. Paul MacDonnell and Daniel Castro, "Europe Should Embrace the Data Revolution" (Information Technology and Innovation Foundation, February 2016), http://www2.datainnovation.org/2016-europe-embrace-data-revolution.pdf.
16. 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.
17. 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
18. OECD, "Data-driven Innovation, Big Data for Growth and Well-being," 109.
19. 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./.
20. Ezell, "Digital Trade Act of 2013 Instrumental to Protecting and Empowering the Global Digital Economy."
21. U.S. International Trade Commission (ITC), *Digital Trade in the U.S. and Global Economies, Part 2*, (U.S. ITC, August 2014), http://www.usitc.gov/publications/332/pub4485.pdf.
22. Ibid.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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/.
28. Business Roundtable, "Putting Data to Work" (Business Roundtable, 2015), http://businessroundtable.org/sites/default/files/reports/BRT%20PuttingDataToWork.pdf.
29. 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.
30. 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.

31. 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.
32. 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.
33. U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*.
34. 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.
35. 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.
36. Maggiore, "Remote Management of Real-Time Airplane Data."
37. 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.
38. 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.
39. Ibid.
40. 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.
41. Daniel Castro, "The False Promise of Data Nationalism" (ITIF, December 2013), http://www2.itif.org/2013-false-promise-datanationalism.pdf.
42. Stephen Ezell, "Why Privacy Alarmists Are Wrong About Data Rules In Big Trade Deals," *The 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.
43. *International Data Flows: Promoting Digital Trade in the 21st Century* (2015), (written testimony of Robert D. Atkinson, ITIF), http://www2.itif.org/2015-atkinson-international-data-flows.pdf?_ga=1.4629043.1886866732.1462063876.
44. 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-mercantilistindex.pdf.
45. 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/.
46. 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
47. 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.
48. Ibid.
49. 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.
50. Anupam Chandler and Uyen Le, "Breaking the Web: Data Localization vs. the Global Internet," UC Davis Legal Studies Research Paper No. 378, (July 5, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858.
51. 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.

52. United States Trade Representative' Office (USTR), "Fact Sheet: Key Barriers to Digital Trade," (accessed July 10, 2016), https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2016/march/fact-sheet-key-barriers-digital-trade#.
53. Atkinson, Ezell, and Wein, "Localization Barriers to Trade: Threat to the Global Economy."
54. 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.
55. "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.
56. "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.
57. USTR, "Fact Sheet: Key Barriers to Digital Trade."
58. Juliette Garside, "From Google to Amazon: EU goes to war against power of US digital giants," *The Guardian*, July 2014, https://www.theguardian.com/technology/2014/jul/06/google-amazon-europe-goes-to-war-power-digital-giants.
59. Business Roundtable, "Promoting Economic Growth through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements" (Business Roundtable, June 2012), http://businessroundtable.org/uploads/studies-reports/downloads/Global_IT_Policy_Paper_final.pdf.
60. 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-protectinternet-users/article5685794.ece.
61. 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.
62. 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-theireconomic-recovery/.
63. USTR, "Fact Sheet: Key Barriers to Digital Trade."
64. Anupam Chander and Uyen Le, "Data Nationalism," Emory Law Journal No. 64:677 (2015), http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.
65. New Zealand Inland Revenue Service, "Revenue Alert RA 10/02," http://www.ird.govt.nz/technical-tax/revenue-alerts/revenue-alert-ra1002.html.
66. 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%2 0on%2012062014.pdf.
67. "Russia's Personal Data Localization Law Goes Into Effect," Duane Morris.
68. Chandler and Le, "Breaking the Web: Data Localization vs. the Global Internet."
69. David Meyer, "Here's Why PayPal Is About to Suspend Operations in Turkey," *Fortune*, May 31, 2016, http://fortune.com/2016/05/31/paypal-turkey-suspension/.
70. Chander and Le, "Data Nationalism."
71. Michael Rosenwald, "Cloud centers bring high-tech flash but not many jobs to beaten-down towns," Washington Post, November 24, 2011, http://www.washingtonpost.com/business/economy/cloud-centersbring-high-tech-flash-but-not-many-jobs-to-beaten-down-towns/2011/11/08/gIQAccTQtN_story.html; Henry Blodget, "Apple's Huge New Data Center In North Carolina Created Only 50 Jobs," Business Insider, November 28, 2011, http://www.businessinsider.com/apple-new-data-center-north-carolinacreated-50-jobs-2011-11; Darrell Etherington, "Apple To Build A $2 Billion Data Command Center In Arizona," TechCrunch, February 2, 2015, http://techcrunch.com/2015/02/02/apple-to-build-a-2-billiondata-command-center-in-arizona/; Rich Miller, "The Economics of Data Center Staffing," Data Center Knowledge, January 18, 2008, http://www.datacenterknowledge.com/archives/2008/01/18/the-economicsof-data-center-staffing/
72. Brendan O'Connor, "Quantifying the Cost of Forced Localization" (company report, Leviathan Security Group) http://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization

73. The Trans-Pacific Partnerships Trade Agreement, Chapter 14 E-Commerce, Articles 14.11 and 14.13.
74. "General Agreement on Trade in Services," World Trade Organization, accessed July 8, 2016, https://www.wto.org/english/res_e/booksp_e/analytic_index_e/gats_02_e.htm.
75. Nigel Cory and Robert Atkinson, "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements" (Information Technology and Innovation Foundation, April 2016), http://www2.itif.org/2016-financial-data-trade-deals.pdf.
76. Nigel Cory, "The TPP's Financial Data Carve Out—USTR Closes a Loophole for Digital Protectionists," Innovation Files, July 7, 2016, http://www.innovationfiles.org/the-tpps-financial-data-carve-out-ustr-closes-a-loophole-for-digital-protectionists/.
77. Cory and Atkinson, "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements."
78. Nigel Cory and Stephen Ezell, "Crafting an Innovation-Enabling Trade in Services Agreement" (Information Technology and Innovation Foundation, June 2016), http://www2.itif.org/2016-tisa-services.pdf.
79. "O'Sullivan: No Work on TTIP Digital Chapters Until Privacy Shield In Place, *Inside U.S. Trade*, May 17, 2016, http://insidetrade.com/daily-news/o%E2%80%99sullivan-no-work-ttip-digital-chapters-until-privacy-shield-place.
80. Julia Fioretti, "EU-U.S. commercial data transfer pact clears final hurdle," *Reuters*, July 8, 2016, http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN0ZO0SH.
81. Catherine Tucker, "Empirical Research on the Economic Effect of Privacy Regulation," *Journal on Telecommunications and High Technology Law* 10 (2012): 265, http://cetucker.scripts.mit.edu/docs/law_summary_2011.pdf
82. Avi Goldfarb and Catherine Tucker, "Privacy Regulation and Online Advertising," http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259/
83. 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.
84. Ibid. and Asia-Pacific Economic Cooperation (APEC), *APEC Privacy Framework* (Singapore, APEC, 2005), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx