Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?

BY NIGEL CORY | MAY 2017

Data needs to flow to maximize value, which means policies that limit such flows across borders will reduce economic growth and social value.

Data is the lifeblood of the modern global economy. Digital trade and cross-border data flows are expected to continue to grow faster than the overall rate of global trade. Businesses use data to create value, and many can only maximize that value when data can flow freely across borders, yet a growing number of countries are enacting barriers that make it more expensive and time consuming, if not illegal, to transfer data overseas. Some nations base their decisions to erect such barriers on the mistaken rationale that it will mitigate privacy and cybersecurity concerns; others do so for purely mercantilist reasons. Yet, whatever the motivation, as this report demonstrates, the costs of these policies are significant, not just for the global economy, but for the nations that "shoot themselves in the foot" by using these policies.

The increased digitalization of organizations, driven by the rapid adoption of technologies such as cloud computing and data analytics, has increased the importance of data as an input to commerce, impacting not just information industries, but traditional industries as well. The use of data analytics in virtually all industries has streamlined business practices and increased efficiency, but also made the movement of data more important.[1] Organizations increasingly rely on data for a number of purposes, including to monitor production systems, manage global workforces, monitor supply chains, and support products in the field in real time. Companies collect and analyze personal data to better understand customers' preferences and willingness to pay, and adapt their products and services accordingly. It is a simple fact that international trade involving consumers cannot

take place without collecting and sending personal data across borders—such as names, addresses, billing information, etc.[2]

Despite the significant benefits to companies, consumers, and national economies that arise from the ability of organizations to easily share data across borders, dozens of countries—across every stage of development—have erected barriers to cross-border data flows, such as data-residency requirements that confine data within a country's borders, a concept known as "data localization."[3] Data localization can be explicitly required by law or is the de facto result of a culmination of other restrictive policies that make it unfeasible to transfer data, such as requiring companies to store a copy of the data locally, requiring companies to process data locally, and mandating individual or government consent for data transfers. These policies represent a new barrier to global digital trade. Cutting off data flows or making such flows harder or more expensive puts foreign firms at a disadvantage.[4] This is especially the case for small and solely Internet-based firms and platforms that do not have the resources to deal with burdensome restrictions in every country in which they may have customers. In essence, these tactics constitute "data protectionism" because they keep foreign competitors out of domestic markets.

This report first analyzes the privacy and security "justifications" nations offer for enacting barriers to data flows, concluding that, while such policies may be well intentioned, these rationales are generally not valid. (A forthcoming Information Technology and Innovation Foundation report will focus on a third motivation—to enable surveillance and government access for law enforcement—and will explain how governments need to develop a revised framework to help them determine jurisdiction over data while also facilitating cooperation among governments.) The report then examines the economic rationales countries provide to justify their data-localization policies, explaining the shortcomings in those arguments and noting that such policies impose large costs on countries' own economies. The report then proceeds to review the emerging body of research that estimates the cost of barriers to data flows in terms of lost trade and investment opportunities, higher information technology (IT) costs, reduced competitiveness, and lower economic productivity and GDP growth. These studies show that data localization and other barriers to data flows impose significant costs: reducing U.S. GDP by 0.1-0.36 percent; causing prices for some cloud services in Brazil and the European Union to increase 10.5 to 54 percent; and reducing GDP by 0.7 to 1.7 percent in Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam, which have all either proposed or enacted data localization policies.

Finally, the report offers recommendations for policymakers in both the United States and other countries.

The Trump administration should:

- Negotiate trade agreements that prohibit and eliminate digital barriers.
- Develop better measures of the digital economy and trade.

- Expand the focus on digital economy and trade issues.
- Initiate enforcement cases against countries, such as China, that have enacted digital-protectionism policies.
- Propose and negotiate a "data-services agreement" to address digital trade barriers.
- Propose and negotiate a "Geneva convention on the status of data" to establish international legal standards for government access to data, to improve mutual legal-assistance processes, and to decide on a framework to manage questions on data-related jurisdiction issues.

Dozens of countries—across every stage of development—have erected barriers to cross-border data flows.

For policymakers in other countries:

- Recognize the critical role of data flows and prohibit data-localization policies.
- Promote international interoperability in privacy and data protection.
- Encourage international organizations, such as the World Trade Organization and the Organization for Economic Cooperation and Development, to focus on digital trade barriers.

RATIONALES FOR DATA LOCALIZATION AND OTHER BARRIERS TO DATA FLOWS

Policymakers often offer one of the following motivations when introducing policies that restrict cross-border data flows: privacy and cybersecurity, or economic mercantilism. In pursuing these goals, some countries simply apply a blanket ban on data transfers. Others only apply restrictions to certain types of data. But, in all cases, the result is harmful to global trade and economic growth as well as to the host country's own economy. As the current list of data-localization policies shows (see a full list in appendix A), a growing number of countries have enacted barriers to data flows.

Privacy and Cybersecurity Rationales

Many policymakers reflexively and mistakenly believe that data is more private and secure when it is stored within a country's borders. This misunderstanding lies at the core of many data-localization policies. However, in most instances, data-localization mandates do not increase commercial privacy nor data security.[5] This is a key point that few policymakers have fully grasped.

Most companies doing business in a nation—all domestic companies and most foreign—have "legal nexus," which puts the company in that country's jurisdiction. For example, a global bank or manufacturer that has branches or plants in a nation is subject to that nation's privacy and security laws and regulations. As such, the bank must comply with those rules whether it stores the data in the host country, in the home country of the

foreign company, or even in a third country. Companies simply cannot escape from complying with a nation's laws by transferring data overseas.

But what about companies without legal nexus (i.e., the firm has no physical presence, business activity, nor marketing directed toward a specific foreign country)? For example, the citizens of nation A might visit the website of a small company located in nation B, which has different privacy and security laws. This company did not have a legal nexus in country A, so it cannot be expected to abide by the laws there. In this case, the only way nation A's laws can be enforced—whether or not they require data localization—is if they simply cut off their citizens' access to all foreign websites. This is not the case for most businesses involved in foreign digital trade, as they have legal nexus, but it highlights the fallacy of countries trying to enact policies that cannot be contained in-country, but affect the entire Internet.

Policymakers focusing on geography to solve privacy and cybersecurity concerns are missing the point. Consumers and business can rely on contracts or laws to limit voluntary disclosures to ensure that data stored abroad receives the same level of protection as data stored at home. In the case of inadvertent disclosures of data (e.g., security breaches), to the extent nations have security laws and regulations, again a company operating in the nation is subject to those laws, regardless of where the data are stored. Moreover, security breaches can happen no matter where data are stored—data centers everywhere are exposed to similar risks. Such disclosures are the result of security failures, such as hackers breaking into a corporate network to steal data, government agencies tapping into telecommunications links, or employees mistakenly posting sensitive data in a public forum. What is important is that the company involved (either a company with its own networks or a third-party cloud provider) be dedicated to implementing the most advanced methods to prevent such attacks. The location of these systems has no effect on security.

Moreover, policymakers misunderstand that the confidentiality of data does not generally depend on which country the information is stored in, only on the measures used to store it securely. A secure server in Colombia is no different from a secure server in Brazil. Data security depends on the technical, physical, and administrative controls implemented by the service provider, which can be strong or weak, regardless of where the data is stored. For example, in a practice that protects both data privacy and security, some cloud-computing companies have upgraded security controls, so that customers retain the keys used to encrypt data before it is uploaded, thereby preventing third parties, including the cloud companies themselves, from accessing their data.[6] While cloud computing does not guarantee security, and organizations should investigate the terms of service and security practices of any service provider, cloud computing will likely lead to better overall security because implementing a robust security program requires resources and expertise, which is what many small and mid-sized organizations lack, but large-scale cloud-computing providers can offer.

Regardless of these realities, many countries have enacted rules to limit the movement of data outside their nation. While countries with explicit local data-storage requirements get the most attention, some nations have made their privacy requirements so restrictive that companies have to keep data local, such as policies that require consent for any data transfers. For example, South Korea's Personal Information Protection Act targets data leaving the country and requires companies to obtain consent from "data subjects" (i.e., the individuals associated with particular datasets) prior to exporting that data, as well as details about who receives the data, the purpose, the period the data will be retained, and the specific personal information provided.[7] (See appendix A.) Again, as noted above, this law has no actual positive effect on privacy; its only effect is a mercantilist one to substitute domestic production for foreign.

Economic Development—"Digital Mercantilism"

With modern technology, it is nonsensical to think that companies should be forced to move people to the data, and not the other way around.

Some countries believe data localization offers a quick way to force high-tech economic activity to take place within their borders—a new form of "digital mercantilism"—similar to how countries use local content requirements and tariffs to protect local manufacturing operations.[8] Given that traditional trade-protectionism tools, such as tariffs, do not work as readily on digital economic activity, countries pursuing digital mercantilism are reverting to "behind-the-border" regulations and technical requirements, such as data localization. These barriers represent the most significant issue for digital trade.

Some policymakers believe that, if they restrict data flows, their countries will gain a net economic advantage from companies that will be forced to relocate data-related jobs to their nations.[9] These supposed benefits of data-localization policies are misunderstood. Data centers have become more automated, meaning that the number of jobs associated with each facility, especially for technical staff, has decreased. While data centers contain expensive hardware (which is usually imported) and create some temporary construction jobs, they employ relatively few full-time staff.[10] For example, in 2011, a $1 billion data center built by Apple in North Carolina created only 50 full-time jobs and another 250 support jobs in the local community in areas such as security and maintenance. Similarly, a new Microsoft data center in Virginia was expected to create at most several dozen permanent jobs. As this report shows below, the economic benefit from these jobs is outweighed by the increased costs of data processing following on these policies.

THE EXTENT AND IMPACT OF DIGITAL TRADE BARRIERS ON U.S. FIRMS

In 2014, the United States International Trade Commission (ITC) released a survey showing the pervasive and extensive impact that digital trade barriers have on U.S. firms. The survey asked whether companies in seven digitally intensive sectors (such as digital communications and content) faced localization and data-privacy and protection requirements, and asked them to rank these along a scale of one (not an obstacle) to five (a very substantial obstacle). Eighty-two percent of large firms and 52 percent of small and medium-sized enterprises (SMEs) in the digital-communications sector reported facing localization barriers to digital trade. The severity of these barriers varied: 34 percent of large firms in digital communications faced localization requirements; 27 percent of content firms considered localization barriers as "substantial or very substantial"; and 20 percent of large retail firms and 19 percent of large financial firms considered them "substantial or very substantial." Large firms in digital communications and SMEs in finance had the highest percentage viewing localization and data privacy and protection requirements as "substantial or very substantial." In general, firms reported that data-localization requirements are expensive, time-consuming, and disruptive, while observing that these requirements do not improve data security, which is often the officially stated purpose of this type of measure.[11]

THE COSTS OF BARRIERS TO CROSS-BORDER DATA FLOWS

Barriers to data flows affect a growing share of economic activity, as data is important to an increasing array of industries, including more "traditional" ones.[12] For example, in the United States, digitally enabled services grew from $282.1 billion in 2007 to $356.1 billion in 2011.[13] Globally, McKinsey analysis finds that, over the past decade, data flows have increased world GDP by 10.1 percent.[14] This section analyzes how barriers to data flows affect firm competitiveness as well as economic productivity and innovation.

Barriers to Data Flows Undermine Firm Competitiveness and Economic Productivity

Maximizing the value of data requires it to move. Innovation and economic growth are increasingly driven by how firms collect, transfer, analyze, and act on data. 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.

At the firm level, barriers to data flows make firms less competitive, as a company will be forced to spend more than necessary on IT services. Companies will likely have to pay more for data-storage services, especially those in smaller countries (which will not naturally be home to a data center). Such barriers also prevent companies from transferring data that's needed for day-to-day activities, such as for human resources, which means companies may have to pay for duplicative services. Likewise, companies may be compelled to spend more on compliance activities, such as hiring a data-protection officer, or putting

in place software and systems to get individuals' or the government's approval to transfer data. These additional costs are either borne by the customer or the firm, which undermines the firm's competitiveness (especially for foreign firms who are at some disadvantage vis-a-vis domestic firms) by cutting into profit margins.

This economic impact ripples throughout an economy as barriers to data flows affect data processing and Internet services—or any service that depends on the use of data for delivery, which in today's economy is most. For example, if Brazil had proceeded with its proposed data-localization plan, it would have forced companies to pay an average of 54 percent more for some cloud-computing services.[15] As the studies in this report show, these additional costs detract from firm and industry competitiveness as well as a country's economy more broadly. The opportunity cost is that the resources could otherwise go toward hiring new employees or buying new equipment.

Barriers to Cross-Border Data Flows Undermine Innovation and Access to Innovative Services

Countries that enact barriers to data flows make it harder and more expensive for their companies to benefit from the ideas, research, technologies, and best practices that accompany data flows.

Organizations use data to create better insights, which, in turn, lead to innovation. Businesses use data to enhance research and development, develop new products and services, create new production or delivery processes, improve marketing, and establish new organizational and management approaches.[16] Countries that enact barriers to data flows make it harder and more expensive for their companies to gain exposure and to benefit from the ideas, research, technologies, and best practices that accompany data flows and the innovative new goods and services that rely on data. Countries that artificially prop up domestic businesses with such digital-protectionist policies—which disadvantage foreign firms—set them up to fail because they will always be less competitive and innovative than those companies in global markets that operate without similar protection.

Barriers to data flows also mean delays and higher costs in the development of new and innovative goods, as companies may be unable to use their preferred research partners and are forced to use second choice partners (if they do so at all). Data-localization policies undermine the ability of companies, such as Procter & Gamble (P&G), that use new and innovative global "open-innovation" platforms to facilitate collaboration among firms, universities, and other research organizations to drive their own innovation.[17]

Likewise, these barriers can impede important medical research. Compared with other categories of data, health data is much less "liquid" and is therefore underutilized due to the barriers put around it.[18] This has consequences. For example, disease does not stop at national borders, meaning that data needed to find cures need to cross borders, too. Powerful data analytics applied to bigger global datasets can help speed the development of cures. The rarer the disease, the more important it is to build bigger datasets. By erecting barriers to the exchange of medical information, even anonymous data, countries' protectionist policies harm not only their own citizens, but also people around the world, all of whom benefit from advances in such medical research.

Countries enacting barriers to data flows not only undermine innovation, but prevent their citizens from accessing innovative services. For example, barriers to the exchange of personal medical data, such as those in Australia, Canada, China, and Russia, could prevent these counties' citizens from accessing the latest technological advances. For example, companies such as Hermes and Alliance Medical provide outsourced analysis of MRI scans, thereby decreasing health-care costs and time demands on doctors. Likewise, such health-data restrictions prevent IBM Watson—which combines a supercomputer, artificial intelligence (AI), and sophisticated analytical software—from using patient data for newer, quicker, and better health diagnosis.[19] Given that each of Watson's AI applications—such as for health, weather forecasts, or others—require customized hardware to match the application, it is unrealistic to assume that IBM would build such data centers in each and every country that enacts barriers to health data. Instead, citizens in these countries are likely to miss out on access to the latest and most-sophisticated medical services.

CALCULATING THE COSTS OF DATA LOCALIZATION

A growing body of research has examined not only the relationship between cross-border data flows and economic growth but the economic costs engendered by limiting cross-border data flows. This section summarizes the key studies that have estimated the economic cost of data localization.

United States International Trade Commission: The Impact of Foreign Digital Trade Barriers on the U.S. Economy

A 2014 International Trade Commission (ITC) study showed that barriers to digital trade and data flows imposed costs on U.S. firms and the U.S. economy. The ITC study analyzed the impact of barriers to digital trade and data flows on three levels of the U.S. economy: the firm level, through 10 case studies of U.S. companies involved in digital trade; the industry level, through a survey of U.S. businesses in seven digitally intensive industries; and at the economy level, through a computable general equilibrium and econometric model.[20]

The ITC study estimated that removing foreign digital trade barriers would increase U.S. GDP by $16.7 to $41.4 billion (0.1 to 0.3 percent) and wages by 0.7 to 1.4 percent in the seven digitally intensive sectors.[21] The econometric model used surveys of U.S. firms in these sectors to identify barriers to digital trade and to rank countries that enact these barriers in order to help the model estimate the impact removing these barriers would have on these sectors and the overall U.S. economy.[22] For example, large firms noted that China was largely closed to digital trade and that the removal of these digital trade barriers could have a substantial positive effect on sales abroad, which would indirectly increase U.S. economic activity.

Leviathan Security Group: The Costs of Cutting Access to Global Cloud Services

A 2015 Leviathan (an information security company) study shows that local companies could have to pay significantly more for cloud services in Brazil and Europe if data-localization policies had cut them off from the most cost-competitive global cloud

providers.[23] How much more depends on whether the country/region is home to a local data center from one of these seven providers and how competitive (price wise) this local provider is in comparison to global competitors. The study looks at the change in per-hour costs for cloud services if data-localization policies forced local companies to use the local cloud services from one of the seven major providers covered in the study. The study considered like-for-like services (focusing on memory allocated to services, with 1GB, 2GB, 4GB, 8GB, 16GB, and 32GB server categories) from global leaders in public infrastructure-as-a-service cloud companies: Amazon Web Services, DigitalOcean, Google Compute Engine, HP Public Cloud, Linode, Microsoft Azure, and Rackspace.[24]

The Leviathan study found that cutting off access to global leaders in cloud-computing services—through localization—would force local companies in Brazil and the European Union to pay 10.5 to 62.5 percent more for some cloud-computing services.

Leviathan's study was not able to calculate the cost of data localization in other countries that have enacted or considered data-localization policies, such as Canada, Russia, Indonesia, and India, as these countries do not have data centers from any of the major cloud providers covered in the study. This shouldn't be surprising given the distributed nature of the Internet: At the time of the study (2015), the seven companies in this study had data centers in just 12 countries: Australia, Belgium, Brazil, China, Germany, Ireland, Japan, the Netherlands, Singapore, Taiwan, the United Kingdom, and the United States.[25]

At the heart of this study is a fact that some policymakers refuse to accept—that for global cloud companies, it makes no sense to have duplicative cloud-computing facilities in every country. This study shows how forcing firms to use only local data centers is much more expensive compared with permitting them to use the lowest-cost cloud-computing service—wherever the data center for that service is located. The study found that the cost of cloud services can increase substantially, depending on the availability of alternative services. The study shows that:

- If Brazil had enacted data localization as part of its "Internet Bill of Rights" in 2014, companies would have had to pay an average of 54 percent more to use cloud services (of all categories) from local cloud providers compared with the lowest worldwide price. For example, for 1GB equivalent services Brazilian customers would have had to pay 37.5 percent more, while for 2GB services the increase would be 62.5 percent.
- At the time of the study, some of the world's lowest-cost data centers were in the European Union, but others were more expensive. If the European Union enacted data localization, companies would not have to pay any more for 1GB and 2GB services, but would have had to pay up to 36 percent more to use 4GB and higher services.
- Furthermore, if data localization were used to create a "Schengen" cloud in Europe (thereby excluding Ireland and the United Kingdom), companies would not have to pay more for some services (such as 1GB and 2 GB), but would face cost increases of 10.5 percent for 4GB and above services.[26]

CIGI and Gotham House: Estimating the Economic Impact of Data Regulations

A 2016 Center for International Governance Innovation (CIGI) and Chatham House study shows that restrictive data regulations, including forced data localization, increase prices and decrease productivity across a range of economies. The report's econometric study analyzes the negative impact data-protection measures have on 10 downstream sectors (i.e., the users of data or data-related services) and the impact this has on the broader economy in Brazil, China, the European Union, India, Indonesia, Russia, South Korea, and Vietnam.[27]

The study first identifies and combines common data regulations to use as a proxy, such as full/partial data localization; strict consent for collection, storage, and dissemination of personal data; and user rights of review of stored information. It then estimates the industry impact by calculating the data intensity of downstream sectors, such as telecommunications and information services.[28] It uses these two measures—data regulations and industry-data intensity—to form a joint indicator for a regression analysis to estimate the economy-wide impact via the change in total factor productivity (TFP).[29]

The study uses this indictor as a counterfactual to assess the economic impact of actual or proposed data regulations, including localization, in Brazil, China, the European Union, India, Indonesia, Russia, South Korea, and Vietnam.[30] As part of this, the study develops a weighted index to compare the severity of data-regulation barriers in each country. It is unsurprising that Russia (4.82) and China (3.88) score the highest (out of a one to six scale, six being the worst) because of their explicit data-localization measures. Indonesia (2.42), India (2.36), and Vietnam (2.19) are not far behind, due to a mix of data localization and other measures. However, it is important to point out that the European Union (3.18) is not far behind China and Russia, due to the indirect impact that restrictive data regulations have on data flows.[31]

The regressions show that data localization and commonly used barriers to data flows decreased TFP, such that a one-standard-deviation change in the joint indicator decreased TFP by 3.9 percent. In the final stage, the study's econometric modeling shows that the lost TFP in downstream sectors, especially in the services sector, reduced GDP by 0.10 percent in Brazil, 0.55 percent for China, 0.48 percent in the European Union, and 0.58 percent in South Korea.[32]

European Center for International Political Economy

The European Center for International Political Economy (ECIPE) has conducted several econometric studies about the costs of data localization and data regulations in the European Union, Russia, Brazil, China, India, Indonesia, South Korea, and Vietnam.

The Costs of Data Localization: Friendly Fire on Economic Recovery

A 2014 ECIPE study estimated the economic costs related to proposed or enacted data-localization requirements and related data-privacy and security laws in Brazil, China, the European Union, India, Indonesia, South Korea, and Vietnam.[33] The study aimed to analyze the impacts on exports, GDP, and consumer welfare (lost consumption due to

higher prices and displaced domestic demand). ECIPE estimates that policies that increase data-processing costs negatively impact economic growth through higher prices on data services.

The study examines the effects of the recently proposed or enacted legislation in the seven countries. Some countries have economy-wide localization policies (such as China and Vietnam), while others only have localization measures for specific sectors (such as South Korea, for financial services). Beyond data localization, the study also considers other common regulatory requirements for data protection that increase compliance costs, such as strict consent requirements for data use and transfers, a right for users to review personal data, strict requirements to notify authorities of data breaches, appointing a data-privacy officer, sanctions for noncompliance, and the requirement to provide government access to a business or its customers' data.[34]

The CIGI/Chatham House study shows that data localization and other data regulations in Brazil, China, the European Union, India, Indonesia, Russia, South Korea, and Vietnam significantly decreased total factor productivity.

The study's econometric model uses regulatory and cost indices to analyze the productivity, price, and investment "shocks" from data restrictions and data-localization policies. The model accounts for different levels of data intensity in different sectors to estimate the productivity impact.[35] The study uses two scenarios: The first sets a benchmark by examining data-protection regulations in each country, which is built upon in the second scenario by adding data-localization policies. The model assigns weights to the measures to account for different levels of restrictiveness.

The results are significant and negative:

- The impact of proposed or enacted data restrictions on GDP is substantial in all seven countries: Brazil (-0.2 percent), China (-1.1 percent), EU (-0.4 percent), India (-0.1 percent), Indonesia (-0.5 percent), Korea (-0.4 percent), and Vietnam (-1.7 percent).
- If these countries also introduced economy-wide data localization requirements, GDP losses would be even higher: Brazil (-0.8 percent), the EU (-1.1 percent), India (-0.8 percent), Indonesia (-0.7 percent), and Korea (-1.1 percent).
- The impact on domestic investments is considerable: Brazil (-4.2 percent), China (-1.8 percent), the EU (-3.9 percent), India (-1.4 percent), Indonesia (-2.3 percent), Korea (-0.5 percent), and Vietnam (-3.1 percent). If these countries also introduced economy-wide data localization, the impact increases for most countries: Brazil (-5.4 percent), the EU (-5.1 percent), India (-1.9 percent), Indonesia (-12.6 percent), South Korea (-3.6 percent), and Vietnam (-3.1 percent).
- Exports from China and Indonesia decrease by -1.7 percent due to loss of competitiveness.
- If these countries enacted economy-wide data localization, the study estimates that higher prices and displaced domestic demand will lead to consumer welfare losses of: $15 billion for Brazil, $63 billion for China, $193 billion for the EU, $14.5 billion for India, $3.7 billion for Indonesia, $15.9 billion for South Korea, and

$1.5 billion for Vietnam. For India, the loss per worker is equivalent to 11 percent of the average monthly salary, almost 13 percent in China, and around 20 percent in South Korea and Brazil.

The Economic Importance of Getting Data Protection Right

A 2013 ECIPE study into the European Union's plan to harmonize data-protection rules—the General Data Protection Regulation (GDPR)—shows that it is likely to have a detrimental impact on the EU economy and hurt domestic firms much more than foreign exporters (i.e., the benefits of intra-EU harmonization are overshadowed by the impact of lost productivity).[36] The GDPR replaces the current patchwork of national rules in EU member states and enables companies to deal only with the data-protection authority (DPA) in the EU country of their head office. This study looked at the impact the GDPR has on trade and cross-border transactions, and by consequence, the effect on EU GDP as well as its consumers and producers.[37] While many changes have happened since this study (e.g., regarding the GDPR and how U.S.-EU data flows are managed), it is still useful in pointing out the cross-border impact that data regulations have on an economy and the potential impact should data flows between the European Union and the rest of the world be disrupted.

The study assesses the GDPR's economic impact in two scenarios. The first looks at how the GDPR affects prices and competitiveness within the EU (focusing on services) and the impact on EU-U.S. services trade.[38] The second scenario builds on the first by removing the potential use of binding corporate rules (BCRs) and model contracts clauses (MCC) (two key tools companies use to manage data transfers between overseas-based subsidiaries), meaning that data flows are largely cut off between the EU and non-EU countries.[39]

Key results:

- Scenario one: EU service exports to the United States decrease by 6.7 percent due to a loss of competitiveness. U.S. service exports to the EU decrease by 0.2 to 0.5 percent. The negative impact likely represents SMEs that are displaced from the market due to increased trade barriers, as they have little means to establish subsidiaries inside the EU or use costly BCRs or MCCs. Furthermore, U.S. service exports to the EU decrease by 16.6 percent to 24 percent, while exports from other countries to the EU fall by up to 80 percent.
- Scenario two: The GDPR decreases EU GDP by 0.8 percent to 1.3 percent, partly as foreign companies have to establish a local business (including data storage facilities) to comply with GDPR requirements to handle EU citizens' data. EU manufacturing exports to the United States are estimated to decrease by up to 11 percent, depending on the industry (as goods exports are highly dependent on the efficient provision of services). On a consumer-welfare basis, the study estimates that the GDPR leads to a loss of $102 billion to $170 billion, which is equal to $1,353 for each household of four people.

An Economic Assessment of Data-Localization Measures in EU Member States

A 2016 ECIPE study shows that data localization diminishes productivity and that this impact far outweighs whatever marginal gains the domestic ICT sector might gain from such digital protectionism.[40] This econometric study focuses on EU data-localization measures to estimate the economic impact if these were removed or if they grew into full data-localization measures between EU members.[41]

The study uses 22 measures where EU member countries impose direct restrictions on the transfer of data to other EU members. These measures are used to estimate "best-case" and "worst-case" scenarios—in the best-case "liberalization" situation where actual data-localizing measures in the EU are removed (considering the price and productivity impact), and a worst-case "ratchet" situation that looks at the economy-wide cost (in terms of lost productivity) if all cross-border data flows within the EU were restricted.

ECIPE: The impact of proposed or enacted data restrictions on GDP is substantial: Brazil (-0.2 percent), China (-1.1 percent), the EU (-0.4 percent), India (-0.1 percent), Indonesia (-0.5 percent), Korea (-0.4 percent), and Vietnam (-1.7 percent).

The best-case scenario estimates that the removal of existing data-localization policies would increase the GDP of individual EU member economies by 0.05 percent in the United Kingdom and Sweden, 0.06 percent in Finland, 0.07 percent in Germany, 0.18 percent in Belgium, and 1.1 percent in Luxembourg. In a situation with clear and unfettered competition in the EU for data services, the authors estimate EU GDP to increase by up to 0.06 percent. These results likely underestimate the impact of data localization, as implicit or indirect data-localization measures are not included.[42]

The worst-case scenario estimates that full data-localization policies would remove 0.4 percent from the EU economy each year. The impact varies in individual countries, ranging from -0.27 percent of GDP in Croatia to -0.61 percent of GDP in Luxembourg. The different impact depends on the size of each country's data-intensive sectors and services sectors. Given this, it's unsurprising that the impact is particularly pronounced on the ICT sector. The study estimates that the loss in output in the ICT sector ranges from 0.54 percent in Poland to 3.46 percent in Luxembourg.[43]

RECOMMENDATIONS TO ROLL BACK DATA LOCALIZATION

Rather than build virtual walls at their borders, countries should embrace principles of digital free trade. The United States and other like-minded countries that recognize the value of an open, rules-based digital economy should oppose data-localization policies and work to halt and roll back these corrosive practices. This section is split in two: specific recommendations for the Trump administration and another section for policymakers in other countries. However, even with this split there is crossover in the recommendations. Many of the underlying goals for the Trump administration—such as those involving multilateral negotiations—should be shared by other countries that want to protect and promote global digital trade and the data flows that underpin it.

Recommendations for the United States

Use Trade Agreements to Prohibit and Eliminate Digital Barriers

The United States should leverage trade agreements—both new and reopened plurilateral, bilateral, and regional agreements—to eliminate barriers to data flows. Current

international-trade rules are woefully out of date and need upgrading to account for barriers to digital trade. The United States should embed digital-economy rules in new trade agreements to build new norms that protect data flows, as the World Trade Organization has proven itself incapable of making progress on these issues at the multilateral level. Similar to e-commerce provisions in the Trans-Pacific Partnership trade agreement, future agreements should prohibit countries from enacting barriers to data flows—for all types of data, including financial data, and prohibit countries from forcing companies to use local computing facilities. Similar provisions could be included as part of a revived and revised Trade in Services Agreement (TISA).

Use Trade Agreements to Build Bridges Between Different Privacy Systems

The Trump administration should complement provisions that protect data flows with efforts to use trade agreements to build interoperability between different privacy frameworks, similar to what the TPP tried to do and what the Asia-Pacific Economic Community (APEC) continues to work toward. Greater effort is needed to build interoperability between different privacy systems, which is a far more desirable and realistic goal compared with the European Union's push for harmonization (which aims for a higher level of similarity in both principles and system), which is unrealistic and untenable given the fundamentally different values and approaches to privacy around the world. Without greater attention to interoperability, there is a risk that the Internet will fragment, as some countries enact artificial walls or checkpoints to stop personal data from flowing outside national boundaries, since they don't want data going to countries that don't think have the same system they do. This is a real danger, as there are groups out there that want to prevent data flows, as they fundamentally fear how data is used in today's modern economy and present the issues of data flows and protection as being in direct opposition—a false trade-off.[44]

Trade agreements should be used to prohibit and eliminate digital barriers, and bridge diverse approaches to data protection.

Develop Better Measures of the U.S. Digital Economy and Digital Trade

The negative impact of barriers to data flows often go unobserved, as the government does not properly measure the data economy. The Trump administration should build on the Department of Commerce's ongoing efforts to improve their ability to measure the digital economy, including by:

- Expanding the sample sizes used when measuring trade in services statistics, to collect data more often, and to provide more specific industry detail. This would improve the government's ability to measure the effects of cross-border data flows on productivity.
- Exploring how the department can collect more detailed and specific data on cross-border data flows and develop better measures to capture how the digital economy contributes to GDP, job growth, and productivity. At the moment, the department collects little data specifically on cross-border data flows, as much of the relevant information is from datasets collected for other purposes.
- Continuing the department's efforts to develop a standard nomenclature for terms related to the digital economy, including in collaboration with international

organizations, to better target cross-border data flows, to expand the sample sizes used in measuring trade in services statistics, to collect data more often, and to provide more specific industry detail.[45]

Expand the Focus on Digital Economy and Trade Issues

U.S. trade and economic policy needs to do more to ensure it reflects the growing importance of digital trade to the U.S. economy. USTR only recently started monitoring digital-protectionism measures around the world, including in USTR's annual national trade estimate report on foreign trade barriers.

The Trump administration should build on new initiatives that help USTR and the Department of Commerce create digital trade and economic policy. USTR's still relatively new Digital Trade Working Group (created in July 2016), which is comprised of USTR officials with experience in e-commerce, intellectual property, innovation, and industrial competitiveness, is a good start. The group should be retained, as it improves the U.S. government's ability to identify and respond to new digital trade barriers. Similarly, the Trump administration should keep the Department of Commerce's Digital Economy Board of Advisors, which is made up of digital-economy experts from the private sector, civil society, and academia. While the new administration is within its rights to revise the board's membership, it should retain the board, as it provides a valuable mechanism for outside input into the department's work on the digital economy and digital trade.[46]

U.S. trade and economic policy needs to reflect the growing importance of digital trade to the U.S. economy.

The Trump administration should keep the Commerce Department's network of "digital-economy attachés" in embassies around the world, to ensure it has officials on the ground to identify and respond to digital trade barriers. There are now 12 digital trade officers in U.S. embassies that focus on the Association of Southeast Asian Nations, Brazil, China, the European Union, France, Germany, India, Indonesia, Japan, Mexico, South Africa, and South Korea. This network is essential in terms of feeding information to USTR and other U.S. agencies about new digital-trade barriers as well as efforts to address them in bilateral, plurilateral, and multilateral negotiations, including at the WTO, APEC, and G20.

Pursue Greater Digital-Trade Enforcement

Digital-trade barriers should be part of President Trump's efforts to ramp up U.S. trade enforcement against countries that unfairly target U.S. goods and services. The United States should lead in initiating these cases, but actively seek out other countries to help build broader coalitions to defend digital free trade. While the lack of specific digital-trade rules and jurisprudence make digital-trade cases a challenge (hence the need for new rules), the Trump administration should use current trade rules where possible to deal with the most egregious cases to provide greater digital-market access and certainty about how current rules apply to digital trade.

Indonesia, Russia, and China are the most suitable target for trade dispute cases given their use of data localization and other discriminatory policies that target digital and high-tech sectors. For example, China's pervasive use of digital protectionism should make it a target

of a WTO dispute. In 2016, USTR's National Trade Estimate Report outlined the impact of China's many digital restrictions:

> Over the past decade, Chinese filtering of cross-border Internet traffic has posed a significant burden to foreign suppliers. Outright blocking of websites appears to have worsened over the past year, with 8 of the top 25 most trafficked global sites now blocked in China. Much of the blocking appears arbitrary…[47]

The United States should work with like-minded countries to initiate a case that challenges China's digital protectionism, such as its so-called "golden shield" of measures to block unwanted data transfers from foreign countries for censorship and surveillance purposes. China's efforts to control the flow of information has digital trade implications given it affects commitments it made to liberalize digital trade and data-related services under the General Agreement on Trade in Services (GATS), which were part of the package it signed onto when it joined the WTO. But China uses exceptions within GATS to defend its vague and extensive intervention in managing data flows—that these measures are "necessary to protect public morals and to maintain public order."[48] However, WTO principles and jurisprudence show that the United States and others can make a case that there are less trade-restrictive ways to achieve China's goals (such as selective filtering, which would more specifically address offending material).[49] While such a case, if successful, would not eliminate Internet censorship, it would improve legal certainty for foreign firms by limiting the use of its more commercially damaging forms.[50]

The United States should propose a "Geneva convention on the status of data" to establish legal standards for government access to data and to establish a way to resolve jurisdictional conflicts involving data.

The United States Should Propose a Data Services Agreement

The United States and like-minded countries should propose a plurilateral "Data Services Agreement" at the WTO to protect cross-border data flows and prevent signatory countries from creating localization barriers to data flows. Current WTO laws on localization barriers to trade (e.g., the General Agreement on Trade in Services, or GATS) have proven ineffective at curbing the forced localization of data centers or other barriers to data flows.[51] Short of expanding the WTO definition of localization barriers to trade to include barriers to data flows and forced localization of data centers—a feat that would require all WTO signatory nations to approve a new agreement, which is unlikely given some key users of data-localization policies are in the WTO, WTO members could push for a Data Service Agreement as an alternative mechanism to roll back and prevent the spread of data-localization policies. The success of the Information Technology Agreement and its expansion show that WTO members are capable of negotiating technology-specific plurilateral agreements.

The United States and like-minded countries could use a Data Services Agreement to address modern digital-trade barriers, and in doing so, expand the sphere of influence of the WTO and hold each other accountable for positive data practices. This would allow for companies to bring more WTO cases against participant nations that violate the agreement and would provide a disincentive for signatory countries considering using these trade-distorting practices. But, most importantly, signatory nations could band together to

support these positive practices by putting pressure on other countries in the WTO to sign onto the new agreement.

The United States Should Call for a "Geneva Convention on the Status of Data"

Uncertainty over jurisdiction is at the heart of many policies that act as a barrier to data flows. Different countries impose different legal standards for law-enforcement access, data retention, data security, censorship, and other data-related requirements. This often puts a firm into a legal catch-22, since, for example, a firm that complies with a law-enforcement request from one country may risk violating the privacy laws of another country that also asserts jurisdiction over the data. Related to this, there is also an obvious need for countries to improve how they treat data and government access to data in the wake of revelations about the extent to which many governments are involved in mass surveillance of electronic data and communications. This unpredictability can depress interest in cloud computing and other data-based innovations, and could threaten companies doing business in multiple digital economies (especially for cloud computing), if it leads to greater data-localization measures.

The United States should engage with like-minded countries in creating a "Geneva Convention on the Status of Data."[52] The purpose of this convention would be to establish international legal standards for government access to data and multilateral agreements for questions of jurisdiction and transparency.[53] This convention would not only address the issues of localization and barriers to data flows, but could also limit unnecessary access by governments to data on citizens of other countries and improve mutual legal assistance treaties (MLATs)—agreements that create cooperation between legitimate law-enforcement agencies in different countries. MLATs have come under fire recently for operating too slowly, and thus causing governments to find other avenues within their means to access data stored in other countries.[54] A multilateral agreement could also clarify which countries' laws take precedence when companies encounter conflicting rules. If the United States and its allies work to create a global pact on issues of government access to data, localization, and data flows, countries can encourage economic development in traditional industries, establish jurisdictions for data collection by law enforcement, and promote transparency.

Recommendations for Policymakers in Other Countries

Recognize the Critical Role of Data Flows and Commit to Prohibit Data-Localization Policies

Countries should recognize the enormous societal and economic benefits from innovative new technology and data-based goods and services and commit to allowing the free flow of data across borders. Countries should commit to neither imposing measures that would ban the transfer of data, nor to require the local storage or processing of data nor the use of local facilities. This outcome should be a primary goal for countries as they pursue or revise bilateral, regional, and multilateral negotiations that include an e-commerce chapter. It's critical to ensure new agreements protect data flows, given that new innovations will make data flows even more critical, such as for artificial intelligence and the Internet of Things.

Promote International Interoperability in Privacy and Data Protection

Countries should recognize that privacy protection and data flows can go hand-in-hand and work with other countries to promote international interoperability among different privacy systems. Countries can use trade agreements to bridge diverse approaches to data protection. Interoperability is a more viable goal (compared to harmonization, which aims for a higher level of similarity in both principles and system), as it focuses on developing shared principles and processes, but as part of different privacy systems, so that each country achieves broadly similar data-protection outcomes. This facilitates mutual recognition among different privacy systems, so that data protection flows with the data, wherever it is stored.

The United States and other like-minded countries should push international organizations (such as the WTO and OECD) to monitor, catalogue, and report on digital trade barriers.

Encourage International Organizations to Focus on Digital-Trade Barriers

The United States and other like-minded countries should push international organizations (such as the WTO and OECD) to set up a process to monitor, catalogue, and report on policies that negatively affect digital trade and data flows and are related to localization barriers. The ideal outcome would be for barriers to data flows to become part of the WTO's Integrated Trade Intelligence Portal.

The United States and others should also push international institutions, such as the United Nations Conference on Trade and Development (UNCTAD), the International Monetary Fund, and multilateral development banks (e.g., the World Bank and the InterAmerican Development Bank), to advocate for the free flow of data across borders and push back against countries that force data localization within their borders. As this report shows, these organizations should recognize that forced data localization hurts not only nations that process large amounts of data, but can also be extremely detrimental to budding data-processing markets as well. The World Bank has long advocated that developing nations should invest in their data-processing industries, and many nations have experienced economic growth as a result.[55] To be clear, this refers to the full-fledged growth of industries powered by innovative IT-based services rather than the short-term job gains brought on by the construction of data centers. Otherwise, the value of data processing and innovative insights from data as a development tool is threatened if data protectionism continues to grow.

CONCLUSION

Data flows are essential to today's modern economy. This fact will only become more evident as innovative firms and individuals around the world continuously come up with new ways to leverage data. Cloud computing, data analytics, smartphones, and online platforms have played key roles in shaping today's data-based economy; new innovations will change this yet again. While we do not always know exactly how, we do know that data will be central to this. The Trump administration, enrolling the support of other like-minded countries, needs to realize this when considering what policies are needed to address barriers to data flows as a modern trade issue.

The Trump administration needs to ensure that U.S. trade policy reflects the growing importance of data flows and digital economic activity. There are still many other changes

that can be made to ensure that U.S. companies can continue to rely on the free flow of data for new and innovative goods and services. The distributed nature of the Internet makes trade policy an essential tool in setting rules that protect data flows. Without new rules, countries will continue to exploit the vacuum to enact further barriers to data flows and digital trade. The United States and other like-minded countries that value free trade and the free flow of data can only counter this digital protectionism by setting new, high-standard rules that protect data flows and other crucial facilitators of digital trade and data flows.

As part of this, the United States needs to drive a more-informed debate about data-related policies to dispel the misguided (but persistent) connection some policymakers have made in linking local data storage and privacy, cybersecurity, and economic development. When weighing up legislative changes involving data and data flows, policymakers need to find the right balance of efficacy and proportionality, especially given the growing benefits of data flows. The econometric studies in this report illustrate how important it is that policymakers get this balance right—given the cost for poorly thought-out policies, and choose the least-restrictive measures for the objectives sought, whether this is data privacy, cybersecurity, access, or other objectives.

APPENDIX A: DATA-LOCALIZATION POLICIES AROUND THE WORLD

This appendix captures most of the world's formal data-localization policies (laws or regulations) that have been publicly reported as at April 2017. The entries with icons show where countries have enacted and implemented data localization policies targeting specific types of data. Other entries cover cases where countries have proposed, but not enacted, data localization policies or provide context for data-related policies, such as in the European Union. The list shows that data localization comes in many forms: While some countries enact blanket bans on data transfers, many are sector specific, covering personal, health, accounting, tax, gambling, financial, mapping, government, telecommunications, e-commerce, and online publishing data. Others target specific processes or services, such as online publishing, online gambling, financial transaction processing, and apps that provide services over the Internet (thereby bypassing traditional distribution).

In some cases (such as those for tax and accounting records), data localization stems from outdated legacy laws and rules formulated before the development of the Internet (e.g., laws that require documents to be held at the business's premises). Other data localization stems from countries formulating laws to address technology issues (the Internet, data, or privacy). In a knee-jerk reaction, these countries, instead of tackling the actual issue (such as focusing on data protection or ensuring government access, instead of geography), require local data storage. For others, data localization is a mercantilist tool they think provides them with an advantage over foreign firms, often using public-policy concerns about privacy or cybersecurity as a smokescreen.

TYPES OF DATA BLOCKED BY ENACTED POLICIES

Country	Type of Data	Data-Localization Policy
Argentina		Argentina's Data Protection Act prohibits the transfer of personal data to countries that do not have an adequate level of protection in place, but so far Argentina's government has not determined which countries fall within this category. However, the Act states that the prohibition is not applicable when the data subject has given express consent to the data transfer. In addition, Argentina's National Directorate for Personal Data Protection issued Provision no. 18/2015, which stated that cloud storage is considered an international transfer of data, so that software application that send data abroad must comply with the Data Protection Act.[56]
Australia		In 2012, Australia enacted the Personally Controlled Electronic Health Records Act, which requires that personal health records be stored only in Australia.[57]

Belgium

Belgium's laws require accounting and tax documents to be kept in the office, agency, branch, or other private premises of the taxpayer where they have been kept, prepared, or sent. Companies can apply to Belgian tax authorities for an exemption to this requirement. These accounting records may be kept in another place (such as overseas), provided that immediate access to the records can be granted or that such records can be provided on short notice.[58] Furthermore, Belgium's Companies Code requires companies to keep their register of shareholders and register of bonds at the registered office of the company. Since 2005, it has been possible to keep digital copies of these registries as long as they are accessible at the company's registered office.[59]

Brazil

In September 2013, Brazil began considering a policy that would have forced Internet-based companies, such as Google and Facebook, to store data relating to Brazilians in local data centers. It withdrew this provision from the final copy of the bill.[60] Furthermore, in 2016, Brazilian government agencies, including the Secretary of Information Technology of the Ministry of Planning, Development, and Management, have included forced data localization as a requirement for public procurement contracts involving cloud-computing services.

Bulgaria

In 2012, Bulgaria enacted a new law—the Gambling Act—that required applicants for a gaming license to store all data related to operations in Bulgaria locally. Furthermore, the company's communication equipment and central control point for IT must be in Bulgaria, another EU member country, or Switzerland.[61]

Canada

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.[62]

The tender for the project to consolidate the federal government's ICT services, including email, for 63 different agencies requires the contracting company to store the data in Canada (citing national security reasons).[63]

China

China has one of the widest sets of data-localization policies, which stops the flow of data between China and the rest of the world. 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 several policy changes in the wake of the Snowden revelations that restrict the cross-border transfer of data.[64] For example:

- In 2006, China introduced measures for e-banking that require such companies to keep their servers in China.[65]

- In 2011, China introduced a law that prohibits the off-shore analyzing, processing, or storage of Chinese personal financial information.[66]

- In 2013, China enacted new rules regarding credit reporting that requires all credit information on Chinese citizens to be processed and stored in China.[67]

- In 2014, China enacted new rules that require health and medical information to be stored only in China.[68]

- In 2015, China released draft administrative regulations for the insurance industry that included localization requirements.[69]

- In 2016, China enacted new rules the forced companies involved in Internet-based mapping services to store data locally.[70]

- In 2016, China issued new rules regarding online publishing that require all servers used for a broad range of services involved in online publishing in China to be located in China.[71] This includes app stores, audio and video distribution platforms, online literature databases, and online gaming.

- In 2016, China's new 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.[72] Any movement of data offshore must undergo a "security assessment."

- In 2016, China enacted a new cybersecurity law that forces a broad range of companies to store users' personal information and other important business data in China.[73]

- In March 2016, China enacted new regulations regarding cloud-computing services in China that essentially exclude foreign technology firms and reinforce local data-storage requirements.[74]

- In April 2017, China released a draft circular that outlined extensive localization requirements—both explicit and implicit—as part of a restrictive regime of "security checks" for businesses wanting to transfer data overseas, further to the cybersecurity law, which outlined the need for such security assessments. This draft extends data localization from "critical information infrastructure" to all "network operators," which is likely any owner or administrator of a computerized information network system. Furthermore, any outbound data transfer would be prohibited if it brings risks to the security of the national political system, economy, science and technology or national defense."[75]

Colombia

In 2016, Colombia's Ministry of Information and Communication Technology publicly called for data localization and released a document—on "Basic Digital Services"—that recommends that data-processing centers should be in Colombia, as they perceive storing data overseas to be too great a risk to network security and personal data.[76] Furthermore, there are concerns that Colombia's National Procurement Office (NPO) may include data localization requirements or other barriers to data flows as part of a cloud services procurement project for government agencies. Early drafts show the NPO is considering a vague and arbitrary "adequacy" assessment to decide which countries provide adequate data protection. The NPO has reportedly prepared a draft list of "adequate" countries, which does not include the United States, without detailing how these countries were assessed.

Cyprus

Cyprus has failed to replace several restrictive provisions under the Directive on Data Retention, which was declared invalid by the Court of Justice of the European Union (ECJ). This directive required data operators to retain certain categories of traffic and location data (excluding the content of those communications) for a period between six months and two years and to make them available, on request, to law-enforcement authorities for the purposes of investigating, detecting, and prosecuting serious crime and terrorism.[77]

Denmark

Since 2011, the Danish Data Protection authority has ruled in several cases against processing of local authorities' data in third countries (non-European Union) without using standard contractual clauses. Also, the Danish law on data retention is still in force after the ECJ ruled the Data Retention Directive invalid.[78] In 2011, the Danish Data Protection Agency denied the city of Odense permission to transfer "data concerning health, serious social problems, and other purely private matters" to Google Apps, citing security concerns.[79] Furthermore, Denmark's Book Keeping Act requires companies to store accounting data in Denmark for five years. Under special circumstances, the Danish Commerce and Companies Agency may grant companies permission to preserve accounting records abroad. However, the practice has proven quite restrictive, and permission is seldom granted.[80]

European Union

Data localization is a contentious issue in the European Union, as some members (such as France and Germany) push for localization in relevant policies, while others (such as the United Kingdom and Sweden) push for free flow of data across borders. The European Commission's (EC) effort to build a Digital Single Market is a valiant attempt to remove barriers that inhibit digital economic activity, such as those that require data localization. Yet, as this report shows, many such barriers remain. Large U.S. firms ranked Europe as the area where data privacy and protection requirements represented the largest obstacle to doing business online.[81] Andrus Ansip, EC vice president for the digital single market, has been pushing to remove localization barriers and wants to ban such measures, but his efforts are undermined by others (such as some in Germany and France) that do not want the EC to explicitly ban localization.[82]

A central part of the European Union's policy platform that affects cross-border data transfers is its pursuit of global harmonization of privacy regimes. The EU's law on personal data protection only allows for the transfer of such data to third countries

outside the EU that it has determined provide an "adequate" level of protection. So far, the EU has only recognized 12 countries: Andorra, Argentina, Canada, Switzerland, the Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, the United States (through the U.S.-EU Privacy Shield Framework), and Uruguay.[83] EU personal data is technically not supposed to be transferred to any other country, although it is naïve to believe this is so. Europe has taken a hardline toward the United States about data transfers; however, when its own studies into data protection in other major countries, such as China, show that other countries have little or no level of data protection, it refrains from taking any action.[84] This highlights how untenable the EU's approach is as it tries to set up checkpoints for data flows to each and every country around the world.

Finland

Finland's Account Act (1997) requires that a copy of companies' accounting records be stored in Finland. Alternatively, the records can be stored in another EU country if a real-time connection to the data is guaranteed.[85]

France

The French government has sought over the last few years to promote a local data-center infrastructure, which some have dubbed "le cloud souverain," or the sovereign cloud. In 2016, a French government ministerial circular (dated April 5) on public procurement outlined that it is illegal to use a non-"sovereign" cloud (i.e., foreign cloud provider) for data produced by public (national and local) administration. All data from public administrations has to be considered as archives and therefore stored and processed in France.[86] The French Blocking Statute (Law No. 80-538) makes it illegal to transfer information (such as data) overseas if the information is involved in legal proceedings, absent a French court order.[87]

Germany

Germany, along with France, has been at the center of efforts to force companies to store data only in Europe or even in-country, such as through a "Bundescloud" (a cloud for government data) in Germany.[88] This preference for digital protectionism stands in stark contrast to Germany's otherwise open approach to global trade.

Data requirements can vary by state in Germany. For example, the German state of Brandenburg requires that data on residents can only be stored on cloud computing services located in the state.[89]

On December 18, 2016, Germany introduced local data-storage requirements for a type of telecommunications metadata, through a law that will come into force on July 1, 2017.[90] The law aims to generate and retain telecommunications metadata—the who, when, where, and how, not the what (the content)—of telecommunications for law enforcement and security purposes. This can include citizens' call records, phone numbers, location information, Internet protocol addresses, time and data of Internet usage, and billing information.[91]

Germany's Commercial Code requires companies to store accounting data and documents locally.[92] Also, Germany's tax code requires all persons and companies liable for German taxes to keep accounting records in Germany (with some exceptions for multinational companies).[93] Furthermore, for data processed by public bodies, there

does not seem to be a provision which expressly requires data to be held in Germany. However, such data processing outside the German territory has to be carefully checked.[94]

Greece

In 2001, Greece introduced data-localization requirements through a law implementing the EU Data Retention Directive, which stated that "Data generated and stored on physical media, which are located within the Greek territory, shall be retained within the Greek territory." Even though the Data Retention Directive was invalidated by the European Court of Justice, Greece has not yet reformed the law.[95] The European Commission has also criticized the law as being inconsistent with the E.U. single market, but it remains in effect.[96]

India

India has proposed a range, and enacted some, laws and regulations requiring data localization. India's Ministry of Communications and Technology enacted data transfer requirements as part of a 2011 change to privacy rules that could be (but haven't been) used to restrict data flows containing personal information. These rules limit the transfer of "sensitive personal data or information" abroad to only two restrictive cases—when "necessary" or when the subject consents to the transfer abroad. Because it is difficult to establish that a transfer data abroad is "necessary," this provision would effectively ban transfers abroad except when an individual consents. The ministry clarified that these rules only apply to companies gathering data on Indians and only when the company is located in India.[97] On paper these laws are restrictive, however, India has thus far not used the law to require local data storage.

In 2012, India enacted a "National Data Sharing and Accessibility Policy," which effectively means that government data (data that is owned by government agencies and/or collected using public funds) must be stored in local data centers.[98]

In February 2014, the Indian National Security Council proposed a policy that would institute data localization by requiring all email providers to set up local servers for their India operations and mandating that all data related to communication between two users in India should remain within the country.[99]

In 2014, India's enacted the Companies (Accounts) Rules law that required backups of financial information, if primarily stored overseas, to be stored in India.[100]

In 2015, India released a National Telecom Machine-to-Machine roadmap that requires all relevant gateways and application servers that serve customers in India to be located in India. The Roadmap has not yet been implemented.[101]

Indian government agencies have also made data localization a requirement for cloud providers computing for public contracts. For example, in 2015, India's Department of Electronics and Information Technology issued guidelines that cloud providers seeking accreditation for government contracts would have to require them to store all data in India.[102]

Indonesia

Indonesia has a range of data-localization laws that cover a broad range of sectors and technologies. Indonesia has been expanding its range of localization policies as part of a persistent attachment to state-directed development and digital protectionism strategies.

In 2012, Indonesia enacted a rule—regulation no. 82— regarding the Provision of Electronic System and Transactions, which requires "electronic systems operators for public service" to store data locally.[103] Indonesian officials have stated that "public service" means any activity that provides a service by a public service provider, consistent with the broad definition of the term used in the implementing regulations to the 2009 Public Service Law. In 2014, Indonesia seemed to follow through on this as the government 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.[104] The potentially broad effect of the law was evident by a spokesman's comments that the law "covers any institution that provides information technology-based services."[105] Most recently, Indonesia's Technology and Information Ministry issued regulation 20/2016 on personal data protection that stated that electronic system providers are required to process protected private data only in data centers and disaster recovery centers located in Indonesia.[106]

Localization policies are also spreading to other areas. In 2014, Indonesia's central bank enacted a rule that requires e-money operators to store data locally.[107] In 2016, Indonesia's Ministry of Communications and Informatics issued Circular Letter No. 3, which notifies over-the-top service companies (such as Skype and WhatsApp) about new regulations, including the requirement to store data locally.[108]

Iran

Iran does not have an explicit personal data-protection act, but it has been slowly moving toward developing its own national intranet—the Halal Internet—to separate itself (as best it can) from the rest of the Internet, including moves toward greater data localization. Iran's government operates an extensive online censorship regime. During political protests in 2009, Iran blocked Facebook, Twitter, and YouTube.[109] In 2015, Iran launched its own search engines, which only show approved websites. In August 2016, Iran set up its first government-paid cloud data center.[110] In May 2016, Iran ordered foreign messaging apps, such as WhatsApp and Telegram, to store data from Iranian users locally.[111]

Kazakhstan

Since 2005, Kazakhstan has required that all domestically registered domain names (i.e., those on the ".kz" top-level domain) operate on physical servers within the country).[112] Furthermore, in 2015, Kazakhstan enacted an amendment to its personal data-protection law that requires owners and operators collecting and using personal data to keep such data in-country. The requirement for localization of personal data applies to companies established in Kazakhstan and individual proprietors in Kazakhstan, including branches and representative offices of foreign companies. It is not clear whether the localization requirement should apply to foreign companies without any legal presence in Kazakhstan but whose websites are accessible in Kazakhstan.[113]

Kenya		In June 2016, Kenya released its draft National Information and Communications Technology Policy, which aims to update the government's efforts to revise ICT-related economic policy. In the section on data centers, under the title of policy objectives, the report states that policy should "facilitate the development and enactment of legislation to support growth in IT service consumption—as an engine to spur data center growth."[114] While no data localization has been enacted (yet), this sounds suspiciously like an attempt to use localization for mercantilist ends.
Luxembourg		In 2012, Luxembourg's financial services regulator issued a circular that financial institutions are required to process their data in-country, unless the overseas entity is part of the same company or if the data is transferred with explicit consent.[115]
Malaysia		In 2010, Malaysia enacted the Personal Data Protection Act, which came into force in 2013.[116] Personal data cannot be transferred outside Malaysia, unless the action has been approved by the Malaysian government. Exceptions to this rule include if the data subject has given approval, the transfer is part of a contract between the data subject and data user, if reasonable steps have been taken to protect the data, or if the transfer is necessary to protect the data subject's vital interests.[117] As with other countries, a consent requirement for transfer abroad is a burdensome requirement to satisfy.
The Netherlands		The Netherlands Public Records Act requires public records to be stored in archives in specific locations in the country.[118]
Nigeria		In 2014, Nigeria enacted the "Guidelines for Nigerian Content Development in Information and Communications Technology (ICT)," which introduced several restrictions on cross-border data flows and mandated that all subscriber, government, and consumer data be stored locally.[119] Furthermore, in 2011, Nigeria's Central Bank introduced a measure that required all point-of-sale and ATM transactions to be processed locally. Under no circumstances are these transactions to be processed outside Nigeria.[120]
New Zealand		New Zealand's Internal Revenue Act requires businesses to store business records in local data centers.[121]
Poland		Poland required e-commerce entities to store customer details in Poland, but after an intervention by the European Commission, Poland was forced to lift the requirement, and it is now sufficient that the servers are in the EU. The Polish Gambling Act also requires online gambling firms to store all data relating to customer betting in the European Union.[122]
Romania		In 2015, Romania enacted new online gambling regulations that requires all data on players and their gambling activities to be stored in Romania.[123]

Russia

Russia operates one of the most extensive sets of data-localization policies in the world. In 2015, Russia enacted a Personal Data Law that mandates that data operators who collect personal data about Russian citizens must "record, systematize, accumulate, store, amend, update and retrieve" data using databases physically located in Russia.[124] This personal data may be transferred out, but only after it is first stored in Russia. Russia has threatened to shut down and fine websites, such as LinkedIn, that refuse to store data locally.[125]

Furthermore, in 2016, Russia enacted extensive new data-localization requirements for telecommunications data.[126] Russia's approach is much broader than other countries' telecommunications data-retention requirements, as it requires companies to store the actual content of users' communications for six months, such as voice data, text messages, pictures, sounds, and video, not just the metadata (the who, when, and how long of communications). Second, it requires telecommunications companies and ISPs to cut services to users if they fail to respond to a request from law enforcement to confirm their identity (which raises a range of privacy issues).

South Korea

In South Korea, the Personal Information Protection Act requires companies to obtain consent from "data subjects" (i.e., the individuals associated with particular data sets) prior to exporting that data.[127] The act also requires "data subjects" to be informed of 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 data across borders.

Korea has used data localization requirements to protect local e-commerce and online payment operators. Korea's Regulation on Supervision of Credit-Specialized Financial Business prohibited e-commerce firms from storing Korean customer's credit card numbers outside the country. In 2013, Korea slightly revised this rule by allowing certain foreign e-commerce firms (those with stores in more than five countries) to store such data abroad.[128]

In 2014, South Korea enacted a law—Act on the Establishment, Management, Etc. of Spatial Data—that prohibits mapping data from being stored outside the country due to security concerns.[129] Korea is the only significant market in the world that maintains data localization requirements for mapping data. Korea has defended the policy as it wants to limit the availability of high-resolution commercial satellite imagery of Korea for national security reasons, even though such imagery is already available commercially.

In 2015, Korea enacted the Act on Promotion of Cloud Computing and Protection of Users. Subsequent guidelines—the Data Protection Standards for Cloud Computing Services Guidelines—contain rules that effectively require data localization as cloud computing networks serving public agencies have to be physically separate from networks serving the general public. While these guidelines are only "recommended" and there is no penalty for non-compliance, Korean institutions usually follow such guidelines. This discriminatory policy may have a significant affect as it applies to thousands of institutions, such as educational institutions, public banks, and public hospitals.[130]

Sweden

Sweden's Financial Services Authority requires "immediate" access to data in its market supervision, which, according to business, the supervisory body interprets as being given physical access to servers. This amounts to de facto localization, as companies are forced to store data in Sweden.[131]

Furthermore, Sweden has accounting requirements that force companies to store data about current company records and accounts in Sweden for seven years.[132] In addition, there is the potential for Swedish government regulations to be interpreted such that data processed by a government agency needs to be held within Sweden, which would obviously affect cloud computing and ultimately result in data localization.[133]

Taiwan

Article 21 of Taiwan's Personal Data Protection Act permits government agencies the authority to restrict international transfers in the industries they regulate, under certain conditions, such as when the information involves major national interests, by treaty or agreement, inadequate protection, or when the foreign transfer is used to avoid Taiwanese laws.[134]

Turkey

In 2013, Turkey enacted a law—the Law on Payments and Security Settlement Systems, Payment Services and Electronic Money Institutions—that forces Internet-based payment services, such as PayPal, to store all data in Turkey for ten years.[135] PayPal withdrew from the country after refusing to abide by this data localization requirement.

In 2016, Turkey enacted the Law on the Protection of Personal Data, which limits transfer of personal data out of Turkey and may require firms to store data on Turkish citizens in country.[136] The law places burdensome obligations on data controllers and processors, requiring "express consent" from individuals to transfer personal data to another country. The need for specific and individual engagement holds the potential to act as de facto data localization. Turkey's new law adopts a similarly untenable and unrealistic approach to international data flows and protection as that of the European Union by requiring country-by-country assessments of privacy protections. Turkey's newly formed "Data Protection Board" (staffed with political appointees, not technical staff) will assess whether other countries provide an "adequate" level of privacy protection. Under this law, if the country receiving data from Turkey does not offer "adequate" protection, the Data Protection Board must provide permission for each transfer.[137]

United Kingdom

According to the United Kingdom's Companies Act 2006, "if accounting records are kept at a place outside the United Kingdom, accounts and returns ... must be sent to, and kept at, a place in the United Kingdom, and must at all times be open to such inspection".[138]

United States

The United States has proposed or enacted a few data localization requirements, most of which focus on public procurement. Most recently, the United States pushed for financial services data to be exempt from rules in the Trans Pacific Partnership that prohibited countries from enacting barriers to data flows.[139] However, after the agreement was finalized, the United States sought to limit the scope of this provision through bilateral discussions and via provisions in ongoing negotiations for a Trade in Services Agreement.

In 2016, the U.S. Internal Revenue Service issued publication 1075— Tax Information Security Guidelines For Federal, State and Local Agencies—which outlined (section 9.3.15.7) that federal agencies must "restrict the location of information systems that receive, process, store, or transmit [federal tax information] to areas within the United States territories, embassies, or military installations."[140]

In 2015, the U.S. Department of Defense issued revised rules that require all cloud-computing service providers that work for the department to store data domestically.[141] Domestic data storage requirements are sometimes a requirement for other federal public procurement contracts, but are not an explicit government-wide policy.

Similarly, some state and local governments impose these requirements in contracts. The City of Los Angeles, for example, required Google to store its data within the continental United States as a condition of its contract with the city.[142] In 2004, Tennessee enacted a bill (SB 2344) that gives a preference to local providers when evaluating proposals for state-level procurement contracts requiring data entry and/or call center services. The preference is provided when the contract is provided by U.S. citizens and other persons authorized to work in the United States.[143] Similarly, in 2004, an Ohio state representative proposed a bill (No. 459) that would prohibit transferring personal data overseas without written consent as part of any state procurement projects. The bill never became law.[144] Similar laws were proposed in Missouri and other states.[145] In 2011, a New York State senator proposed a law (S3713) that would prohibit the transfer of personal information outside the United States without the prior written consent of the consumer. It was intended to favor local companies, whilst tangentially trying to connect overseas data storage to consumer fraud and theft.[146]

Vietnam

Vietnam has extensive data-localization policies in place as part of broad efforts to control Internet-based activities (for both political and commercial purposes). For example, Vietnam forbids direct access to the Internet through foreign ISPs and requires domestic ISPs to store information transmitted on the Internet for at least 15 days.[147]

In January 2016, Vietnam released a draft regulation—Draft Decree Amending Decree 72—for over-the-top services (such as WhatsApp and Skype) that included a forced data-localization requirement.[148] In 2013, Vietnam enacted a law—Decree 72—on the management, provision, and use of Internet services and online information that requires a broad range of online companies (such as social networks, online game providers, and general information websites) to have at least one server in Vietnam "serving the inspection, storage, and provision of information at the request of competent state management agencies."[149] In 2008, Vietnam enacted a law—Decree

		90—against spam (unwanted emails and text messages) that forces relevant advertising companies involved in these activities to send emails and texts only from servers in Vietnam.[150]
Venezuela		Venezuela has passed regulations requiring that IT infrastructure for payment processing be located domestically.[151]

ENDNOTES

1. 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.
2. National Board of Trade Sweden, "No Transfer, No Trade—the Importance of Cross-Border Data Transfers for Companies Based in Sweden" (Stockholm, Sweden: National Board of Trade Sweden, January 2014), http://unctad.org/meetings/en/Contribution/dtl_ict4d2016c01_Kommerskollegium_en.pdf.
3. Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, *Localization Barriers to Trade: Threat to the Global Innovation Economy* (Information Technology and Innovation Foundation, September 2013), http://www2.itif.org/2013-localization-barriers-to-trade.pdf.
4. There is no one definition of digital trade. The definition used is from the USITC's *Digital Trade in the U.S. and Global Economies, Part 2*. United States International Trade Commission (USITC), *Digital Trade in the U.S. and Global Economies, Part 2* (Washington, DC: USITC, August 2014), https://www.usitc.gov/publications/332/pub4485.pdf.
5. Daniel Castro, "The False Promise of Data Nationalism" (Information Technology and Innovation Foundation, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.
6. Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law" (Information Technology and Innovation Foundation, March 2016), http://www2.itif.org/2016-unlocking-encryption.pdf.
7. Anupam Chandler and Uyen P. Le, "Data Nationalism," *Emory Law Journal 64*, http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.
8. For more information on mercantilism, see Michelle A. Wein, Stephen J. Ezell, and Robert D. Atkinson, "The Global Mercantilist Index: A New Approach to Ranking Nations' Trade Policies" (Information Technology and Innovation Foundation, October 2014), http://www2.itif.org/2014-general-mercantilist-index.pdf.
9. For example, see Avanti Kumar, "Can Malaysia Really Become a Data Center Hub?" *MISAsia,* February 13, 2017, http://www.mis-asia.com/tech/data-centre/mdec-exclusive-can-malaysia-really-become-a-data-centre-hub/; "Indian Cloud Data Centres Will Make or Break Digital India," *FirstPost,* October 30, 2015, http://www.firstpost.com/business/sponsored-indian-cloud-data-centres-will-make-or-break-digital-india-2475598.html.
10. Michael S. Rosenwald, "Cloud Centers Bring High-Tech Flash but Not Many Jobs to Beaten-Down Towns," *The 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, "The Country's Problem in a Nutshell: 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-carolina-created-50-jobs-2011-11; Darrell Etherington, "Apple to Build a $2 Billion Data Command Center in Arizona," *TechCrunch*, February 2, 2015, https://techcrunch.com/2015/02/02/apple-to-build-a-2-billion-data-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-economics-of-data-center-staffing/.
11. USITC, *Digital Trade in the U.S. and Global Economies, Part 2*.
12. United States International Trade Commission (USITC), *Digital Trade in the U.S. and Global Economies, Part 1* (Washington, DC: USITC, July 2013), https://www.usitc.gov/publications/332/pub4415.pdf; Castro and McQuinn, "Cross-Border Data Flows."
13. USITC, *Digital Trade in the U.S. and Global Economies, Part 2*.

14. James Manyika, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov, and Dhruv Dhingra, "Digital Globalization: The New Era of Global Flows" (McKinsey Global Institute, February 2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.
15. Brendan O'Connor, "Quantifying the Cost of Forced Localization" (Leviathan Security Group, June 2015), http://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization.
16. Christian Reimsbach-Kounatze and Brendan Van Alsenoy, "Exploring Data-Driven Innovation as a New Source of Growth" (Paris: Organization for Economic Co-operation and Development, June 2013), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2012)9/FINAL&docLanguage=En.
17. USITC, *Digital Trade in the U.S. and Global Economies, Part 2*.
18. David Bollier, "The Promise and Peril of Big Data" (The Aspen Institute, 2010), http://csreports.aspeninstitute.org/documents/The_Promise_and_Peril_of_Big_Data.pdf.
19. Bruce Japsen, "In India, IBM's Watson Will Aid Cancer Care Where Doctors Are Scarce," *Forbes,* December 2, 2015, http://www.forbes.com/sites/brucejapsen/2015/12/02/in-india-ibms-watson-will-aid-cancer-care-where-doctors-are-scarce/#7897ca1c4ff9; Matthew Wall, "How Drug Development Is Speeding Up in the Cloud," *BBC,* February 21, 2017, http://www.bbc.com/news/business-39026239; William Vorhies, "Big Data in Medicine—Evolution and Revolution," *Data Science Central,* November 23, 2015, http://www.datasciencecentral.com/profiles/blogs/big-data-in-medicine-evolution-and-revolution.
20. The seven sectors are content, digital communications, finance and insurance, manufacturing, retail trade, selected other services, and wholesale trade. USITC, *Digital Trade in the U.S. and Global Economies, Part 2*.
21. The GTAP model translates the sector-specific employment effects from the survey into changes in real GDP, real wages, aggregate employment, and sector-level production in the United States. The simulations take the sector-specific effects on U.S. employment as given, and estimate the magnitude of foreign barriers that they imply. The simulations also estimate how workers move from other sectors in the economy. The CGE model analysis is based on the standard GTAP model, with one extension. The size of the labor force (and therefore the quantity of labor supplied) in each region is treated as an endogenous variable, and there is a constant elasticity labor supply curve for each region. The 57 sectors in the GTAP database are aggregated into 14 sectors, 5 of which correspond to the digitally intensive sectors described in chapters 3 and 4 of this report—communications (content and digital communications); finance (finance and insurance); trade (retail and wholesale trade, manufacturing); and services (other services). The study uses GTAP simulations to estimate this impact. U.S. employment in the digitally intensive sectors is an exogenous variable of the model, while the trade costs on these sectors' imports into certain countries are endogenous variables in the model. With this closure, the model calibrates tariff-equivalent magnitudes of the import barriers in the digitally intensive sectors. This closure ensures that the CGE model matches the survey estimated sector-level employment effects through a reduction in the barriers to imports in the relevant sectors and countries.
22. The USITC sent questionnaires to a stratified random sample of nearly 10,000 firms in the seven digitally intensive industries. The questionnaires asked firms how they use the Internet and how the Internet has changed their business practices, sales, and productivity. The questionnaires also asked firms about their experiences with foreign barriers and impediments to digital trade. The survey had a response rate of nearly 41 percent. Of the more than 3,600 companies that responded, 80 percent were SMEs.
23. O'Connor, "Quantifying the Cost of Forced Localization."
24. Ibid.
25. The United States, Belgium, Brazil, Australia, Japan, China, Singapore, Ireland, the United Kingdom, Germany, the Netherlands, and France.

26. O'Connor, "Quantifying the Cost of Forced Localization."
27. As part of the proxy variable for data regulations, the study uses part of the OECD's Product Market Regulation in services to create a proxy that comes close to matching the types of regulations that are used regarding data. The real policy regulations for the select countries are then added to this index to estimate the real costs. Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization" (Centre for International Governance Innovation and Chatham House, May 2016), https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf.
28. The study uses U.S. Bureau of Economic input-output tables to identify which sectors are the heaviest users of a prescribed list of data-service sectors (such as software, Internet and broadcasting publishers, Internet service providers and web search portals, and data processing, hosting, and related services).
29. Overall, there is a small panel dataset for three years covering 21 goods and services sectors for 12 countries. The results of the regressions suggest that administrative regulatory barriers in sectors using data-processing services most intensively exhibit a dampening effect on TFP, while also exerting an upward pressure on prices in these sectors. A one standard-deviation change in the DRL variable would therefore decrease TFP on average by 3.9 percent. Similarly, for prices, a one standard-deviation change in the DRL would increase prices on average by 5.3 percent. Bauer, Ferracane, and van der Marel, "Tracing the Economic Impact of Regulations."
30. This second part uses the elasticities for TFP and the price index. It also augments the proxy of administrative barriers with actual or proposed barriers to data flows in the selected countries. This part identifies and weights (by severity of economic impact) the actual or proposed measures in these countries to derive a new index.
31. On a scale of 0–6: Russia is 4.82; China is 3.88; South Korea is 3.82; the European Union is 3.18; Indonesia is 2.42; India is 2.36; Vietnam is 2.19; and Brazil is 0.75.
32. The study uses the results from this augmented index back in the initial regression to calculate the actual TFP impact in the same set of data-intense downstream sectors in this set of countries. The results show that the services economy suffers the most from barriers to data flows, with TFP decreasing by 2 percent in the communication sector in South Korea, China, and the European Union. These downstream TFP estimates are then used in a computable general equilibrium model to estimate the impact on industrial output and trade volumes.
33. The study uses a computable general equilibrium model (CGE) called GTAP8. The effect on productivity is created using a so-called augmented product market-regulatory index for all regulatory barriers on data, including data localization, to calculate domestic price increases or total factor productivity losses. Matthias Bauer, Hosuk Lee-Makiyama, Erik can der Marel, Bert Verschelde, "The Costs of Data Localisation: Friendly Fire on Economic Recovery" (European Centre for International Political Economy, March 2014), http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.
34. See Table 1 on page 4 for the full details for which countries have which policies. Bauer et al., "Costs of Data Localisation."
35. For example, the telecommunications sector is very data intensive (with 31 percent of its inputs being data related) and should be more heavily affected by regulation; similarly, data processing is 5 to 7 percent of the total inputs used by business/ICT and financial services. Intensities of data services for each sector are based on US input/output use tables from the US Bureau of Economic Analysis. Data on TFP and prices for each sector are taken from EU KLEMS databases.
36. Matthais Bauer, Fredrik Erixon, Michal Krol, Hosuk Lee-Makiyama, and Bert Verschelde, "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce" (The European Centre for International Political Economy, March 2013), https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

37. Bauer et al., "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce."
38. This is done by translating the data regulations into a tariff equivalent.
39. This excludes the small number of countries the EU deems to provide "adequate" privacy protections.
40. Matthias Bauer, Martina Ferracane, Hosuk Lee-Makiyama, Erik van der Marel, "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States" (European Centre for International Political Economy, March 2016), http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf.
41. The model applied in this study is GTAP 8, a computable general equilibrium (CGE) model, which is commonly used to estimate the impact of regulatory changes on a broad set of macro-economic and sector-specific economic variables. For further explanation of the model, see the annex of the report.
42. Bauer et al, "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States."
43. Ibid.
44. Kristina Irion, Svetlana Yakovleva, and Marija Bartl, *Trade and Privacy: Complicated Bedfellows?* (Institute for Information Law, University of Amsterdam, July 2016), http://www.ivir.nl/publicaties/download/1807.
45. Andrew Kitchel and Daniel Castro, "Better Measures of the Data Economy Are Needed to Show the High Costs of Cross-Border Data Restrictions" (Center for Data Innovation, January 3, 2017), https://www.datainnovation.org/2017/01/better-measures-of-the-data-economy-are-needed-to-show-the-high-costs-of-cross-border-data-restrictions/; U.S. Department of Commerce (DOC), " First Report of the Digital Economy Board of Advisors" (Washington, DC: DOC, December 2016), https://www.ntia.doc.gov/files/ntia/publications/deba_first_year_report_dec_2016.pdf.
46. Baird and Baker, "First Report of Digital Economy Board of Advisors."
47. United States Trade Representative (USTR), *The 2016 National Trade Estimate Report* (Washington, DC: USTR, 2016), https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf.
48. World Trade Organization (WTO), "General Agreement on Trade in Services" (Geneva: WTO), https://www.wto.org/english/docs_e/legal_e/26-gats.pdf.
49. For a comprehensive reading on the potential issues of such a WTO case, see Frederik Erixon, Brian Hindley, and Hosuk Lee-Makiyama, "Protectionism Online: Internet Censorship and International Trade Law" (European Centre for International Political Economy, 2009), http://ecipe.org/app/uploads/2014/12/protectionism-online-internet-censorship-and-international-trade-law.pdf; Claude Barfield, "Crafting an Action-Driven Response to China's Digital Trade Barriers" (American Enterprise Institute, January 2017), https://www.aei.org/wp-content/uploads/2017/01/Crafting-an-action-driven-response-to-Chinas-digital-trade-barriers.pdf.
50. Erixon, Hindley, and Lee-Makiyama, "Protectionism Online."
51. Ezell, Atkinson, and Wein, *Localization Barriers to Trade*, 69.
52. Castro, "False Promise of Data Nationalism."
53. Brad Smith, "Time for an International Convention on Government Access to Data," Microsoft, January 20, 2014, https://blogs.microsoft.com/on-the-issues/2014/01/20/time-for-an-international-convention-on-government-access-to-data/#sm.000tw7s7v1dygfpmsng1y8slvx25b; "Safety, Privacy and the Internet Paradox: Solutions at Hand and the Need for New Trans-Atlantic Rules," Microsoft, January 20, 2015, http://blogs.microsoft.com/on-theissues/2015/01/20/brad-smith-time-nations-adapt-laws-reflect-todays-technology/.

54. Daniel Castro and Alan McQuinn, "Cross-Border Digital Searches: An Innovation-Friendly Approach," *Information Week*, November 5, 2014, http://www.informationweek.com/strategic-cio/digitalbusiness/cross-border-digital-searches-an-innovation-friendly-approach/a/d-id/1306989.

55. Oliver Cattaneo et al., "International Trade in Services: New Trends and Opportunities for Developing Countries" (Washington, DC: World Bank, June 24, 2010), http://documents.worldbank.org/curated/en/464591468158719636/International-trade-in-services-new-trends-and-opportunities-for-developing-countries.

56. Estudio Beccar Varela et al., "Data Protection in Argentina: Overview," Practical Law: A Thomson Reuters Legal Solution, accessed March 23, 2017, http://uk.practicallaw.com/3-586-5566.

57. Personally Controlled Electronic Health Records Act 2012, no. 63, Australia (2012). https://www.legislation.gov.au/Details/C2012A00063.

58. "EU Country Guide Data Localization & Access Restriction" (De Brauw Blackstone Westbroek, January 2013), http://www.verwal.net/wp/wp-content/uploads/2014/03/EU-Country-Guide-Data-Location-and-Access-Restrictions.pdf.

59. Ibid.

60. Paulo Trevisani and Loretta Chao, "Brazil Lawmakers Remove Controversial Provision in Internet Bill," *The Wall Street Journal,* March 19, 2014, https://www.wsj.com/articles/SB10001424052702304026304579449730185773914.

61. Gambling Act, Bulgaria (2012), http://www.dkh.minfin.bg/document/403.

62. Anupam Chander and Uyen P. Le, "Data Nationalism," *Emory Law Journal 64*, no. 3 (2015), https://ssrn.com/abstract=2577947.

63. United States Trade Representative, *The 2017 National Trade Estimate report* (Washington, D.C.: United States Trade Representative), https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf.

64. Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, *Localization Barriers to Trade: Threat to the Global Innovation Economy* (Information Technology and Innovation Foundation, September, 2013), http://www2.itif.org/2013-localization-barriers-to-trade.pdf.

65. Timothy Stratford and Yan Luo, "3 Ways Cybersecurity Law in China Is About to Change," Law360, May 2, 2016, https://www.law360.com/articles/791505/3-ways-cybersecurity-law-in-china-is-about-to-change.

66. "Notice of the People's Bank of China on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Information," People's Bank of China, January 21, 2011, http://www.lawinfochina.com/display.aspx?lib=law&id=8837&CGid=.

67. Regulation on the Credit Reporting Industry, State Council 228th session, China (2013), http://www.pbccrc.org.cn/crc/jgyhfw/201309/1ca0f775b50744cabaf83538288d77a9/files/e8a8bf080ed64f48914a652da1d8fdc3.pdf.

68. "Interpretation on Population Health Information Management Measures (Trial Implementation)," National Health and Family Planning Commission of the PRC, last updated June 15, 2014, http://en.nhfpc.gov.cn/2014-06/15/c_46801_2.htm.

69. Michael Martina, "Concern over China insurance rules ahead of talks with U.S.," *Reuters,* May 31, 2016, http://www.reuters.com/article/us-china-cyber-insurance-idUSKCN0YM0NN.

70. Ron Cheng, "Latest Developments on China's Cybersecurity Regulation," *Forbes,* June 30, 2016, https://www.forbes.com/sites/roncheng/2016/06/30/latest-developments-on-chinas-cybersecurity-regulation/#7658dc6c3165.

71. "Online Publishing Service Management Rules," China Copyright and Media website, last accessed March 23, 2017, https://chinacopyrightandmedia.wordpress.com/2016/02/04/online-publishing-service-management-rules/.

72. "Protecting Data Flows in the US-China Bilateral Investment Treaty" (AmCham China, April, 2015), http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization.

73. Nigel Cory, "The Worst Innovation Mercantilist Policies of 2016" (Information Technology and Innovation Foundation, January 2017), http://www2.itif.org/2017-worst-innovation-mercantilist-policies.pdf.

74. Ibid.

75. "China Publishes Draft Measures for Security Assessments of Data Transfers," Hunton and Williams, April 11, 2017, https://www.huntonprivacyblog.com/2017/04/11/china-publishes-draft-measures-security-assessments-data-transfers/; Translated: "Circular of the State Internet Information Office on the Public Consultation on the Measures for the Assessment of Personal Information and Important Data Exit Security (Draft for Soliciting Opinions)," China Copyright and Media, April 11, 2017, https://chinacopyrightandmedia.wordpress.com/2017/04/11/circular-of-the-state-internet-information-office-on-the-public-consultation-on-the-measures-for-the-assessment-of-personal-information-and-important-data-exit-security-draft-for-soliciting-opinions/.

76. Translated: *Basic Digital Services* (Bogota, Colombia: Ministry of Information Communications Technology, 2016), http://estrategia.gobiernoenlinea.gov.co/623/articles-18756_recurso_10.pdf.

77. Matthias Bauer et al., "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States" (European Centre for International Political Economy, March 2016), http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf.

78. Ibid.

79. Chander and Le, "Data Nationalism."

80. "EU Country Guide."

81. United States International Trade Commission (USITC), *Digital Trade in the U.S. and Global Economies, Part 2* (Washington, DC: USITC, August 2014), https://www.usitc.gov/publications/332/pub4485.pdf.

82. Jennifer Baker, "EU Commission Aims to Ban Forced Data Localization," *The Privacy Advisor,* October 24, 2016, https://iapp.org/news/a/eu-commission-aims-to-ban-forced-data-localization/.

83. "Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries," European Commission, last updated November 24, 2016, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

84. Ibid.

85. "EU Country Guide"; Translated "Accounting Law (Finland)," accessed March 23, 2017, http://www.finlex.fi/fi/laki/ajantasa/1997/19971336#L2P9.

86. "Joint Statement: Free Flow of Data Is at the Essence of a True European Digital Single Market," Business Europe, Digital Europe; European Coordination Committee of the Radiological, Electromedical, and Healthcare IT Industry; European Automobile Manufacturers Association; and Alliance for Internet of Things Innovation, https://www.businesseurope.eu/sites/buseur/files/media/public_letters/imco/2016-11-29_ffd_joint_statement.pdf; Translated "April 5, 2016, Note Concerning Cloud Computing" (Paris: France, Ministry of the Interior and Ministry of Culture and Communication, April 5, 2016), http://circulaires.legifrance.gouv.fr/pdf/2016/05/cir_40948.pdf.

87. Bertrand Liard, Caroline Lyannaz, and David Strelzyk-Herzog, "Discovery in the US Involving French Companies," White & Case, November 14, 2012, https://www.whitecase.com/publications/article/discovery-us-involving-french-companies.

88. Monika Kuschewsky, "Data Localization Requirements Through the Backdoor? Germany's 'Federal Cloud,' and New Criteria for the Use of Cloud Services by the German Federal Administration," *Inside Privacy*, September 15, 2016, https://www.insideprivacy.com/cloud-computing/germanys-criteria-for-federal-use-of-cloud-services/.

89. Robert Bond, Jose Manuel Cabello, Daniel Fernan, Moritz Godel, and Alexander Joshi, *Facilitating cross border data flow in the Digital Single Market* (the European Commission, 2016), ec.europa.eu/newsroom/document.cfm?doc_id=41185.

90. Lothar Determann and Michaela Weigl, "Data Residency Requirements Creeping Into German Law," *Bloomberg BNA*, April 11, 2016, http://www.bna.com/data-residency-requirements-n57982069680/.

91. "Law for the Introduction of a Storage Obligation and a Maximum Storage Period for Traffic Data," Library of Germany's Parliament, December 10, 2015, http://www.bundesgerichtshof.de/DE/Bibliothek/GesMat/WP18/V/Verkehrsdaten.html.

92. "Joint Statement: Free Flow of Data."

93. "EU Country Guide Data Localization & Access Restriction."

94. Ibid.

95. Stavros Karageorgiou and Maria Mouzaki, "Collection, Storage and Transfer of Data in Greece," *Lexology*, February 8, 2017, http://www.lexology.com/library/detail.aspx?g=58c33c75-7875-4444-8083-1887c19c1860.

96. 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.

97. Chander and Le, "Data Nationalism."

98. India's Department of Science and Technology, "National Data Sharing and Accessibility Policy," http://www.dst.gov.in/sites/default/files/nsdi_gazette_0.pdf.

99. 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.

100. Stephen Mathias and Naqeeb Ahmed Kazia, "Collection, Storage and Transfer of Data in India," *Lexology,* February 8, 2017, http://www.lexology.com/library/detail.aspx?g=00e56cb6-b0ea-46b7-ab1b-1d52de3646d0; "India Companies (Accounts) Rules 2014" (to be published in the *Gazette of India*, Government of India Ministry of Corporate Affairs, New Dehli, March 2014), http://perry4law.org/clii/wp-content/uploads/2014/03/Companies-Accounts-Rules-2014.pdf.

101. USTR, "The 2017 National Trade Estimate report."

102. USTR, "The 2017 National Trade Estimate report."

103. Information Technology Industry Council (ITI), "ITI Forced Localization Strategy Briefs July 2016" (ITI, 2016), https://www.itic.org/public-policy/ITIForcedLocalizationStrategyBriefs.pdf.

104. Matthias Bauer et al., "The Costs of Data Localisation: Friendly Fire on Economic Recovery" (European Centre for International Political Economy, March 2014), http://www.ecipe.org/media/publication_pdfs/OCC32014__1.pdf.

105. "Indonesia May Force Web Giants to Build Local Data Centers," *Asia Sentinel,* January 17, 2014, http://www.asiasentinel.com/econ-business/indonesia-web-giants-local-data-centers/.

106. Eli Sugarman, "How Emerging Markets' Internet Policies Are Undermining Their Economic Recovery," *Forbes*, February 12, 2014, https://www.forbes.com/sites/elisugarman/2014/02/12/how-emerging-markets-internet-policies-are-undermining-their-economic-recovery/#7446a9237932.

107. Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization" (Centre for International Governance

Innovation and Chatham House, May 2016), https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf.

108. ITI, "ITI Forced Localization Strategy Briefs."
109. Kyle Bowen and James Marchant, "Internet Censorship in Iran: Preventative, Interceptive, and Reactive" (Small Media), https://smallmedia.org.uk/revolutiondecoded/a/RevolutionDecoded_Ch2_InternetCensorship.pdf.
110. Sebastian Moss, "Iran Sets Up Its First Cloud Data Center," *Datacenter Dynamics,* August 15, 2016, http://www.datacenterdynamics.com/content-tracks/colo-cloud/iran-sets-up-its-first-cloud-data-center/96770.fullarticle.
111. John Ribeiro, "Iran Orders Messaging Apps to Store Data of Local Users in the Country," *PCWorld,* May 29, 2016, http://www.pcworld.com/article/3076735/iran-orders-messaging-apps-to-store-data-of-local-users-in-the-country.html.
112. Chander and Le, "Data Nationalism."
113. Ravil Kassilgov, "Kazakhstan—Localization of Personal Data," *Lexology,* January 12, 2016, http://www.lexology.com/library/detail.aspx?g=303621d9-e5b7-4115-9d8c-2a5d1d40ed2c.
114. "Ministry of Information Communications and Technology: National Information and Communications Technology Policy June 2016," website last accessed, April 5, 2017, http://icta.go.ke/pdf/National-ICT-Policy-20June2016.pdf.
115. "Joint Statement: Free Flow of Data"; "Circular CSSF 12/552 as amended by Circulars CSSF 13/563 and CSSF 14/597" (Luxemborg: Commission de Surveillance du Secteur Financier, December 11, 2012), https://www.cssf.lu/fileadmin/files/Lois_reglements/Circulaires/Hors_blanchiment_terrorisme/cssf12_552eng_upd241114.pdf.
116. "Laws of Malaysia Act 709: Personal Data Protection Act" (Malaysia, 2010), http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf.
117. "Data Protection Laws of the World: Malaysia" (DLA Piper, April 9, 2017), https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=MY.
118. "Joint Statement: Free Flow of Data."
119. Nigerian Federal Ministry of Communication Technology, "Guidelines for Nigerian Content Development in Information and Communication Technology" (Nigeria: Nigerian Federal Ministry of Communication Technology, 2014), http:// http://onc.org.ng/wp-content/uploads/2014/06/ONC-Framework-2.pdf.
120. Central Bank of Nigeria, "Guidelines on Point of Sale (POS) Card Acceptance Services" (Nigeria: Central Bank of Nigeria, 2011), http://www.cbn.gov.ng/cashless/POS_GUIDELINES_August2011_FINAL_FINAL%20(2).pdf.
121. "Revenue Alert RA 10/02," Inland Revenue, December 10, 2010, http://www.ird.govt.nz/technical-tax/revenue-alerts/revenue-alert-ra1002.html.
122. Anna Wietrzyńska-Ciolkowska, "Poland: Consequences of Proposed Amendment to Polish Gambling Act for Foreign Operators," DLA Piper, October 17, 2014, http://blogs.dlapiper.com/all-in/2014/11/17/poland-consequences-of-proposed-amendment-to-polish-gamblign-act-for-foreign-operators/.
123. Ana Maria Baciu and Oana Albu, "New Gambling Legislation—the Third Part: New Conditions That Remote (Online) Gambling Operators Must Fulfill," *Casino Inside* no. 53, https://www.nndkp.ro/articles/new-legislation-gaming-3/.

124. "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.

125. Alexander Winning, "LinkedIn Not Willing to Comply With Russian Data Law: Watchdog," *Reuters,* March 7, 2017, http://www.reuters.com/article/us-linkedin-russia-watchdog-idUSKBN16E1IQ.

126. Ksenia Koroleva, "'Yarovaya' Law—New Data Retention Obligations for Telecom Providers and Arrangers in Russia," *Latham and Watkins Global Privacy and Security Compliance Law Blog*, July 29, 2016, http://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/.

127. Anupam Chandler and Uyen P. Le, "Breaking the Web: Data Localization vs. the Global Internet" *Emory Law Journal* (April 2014), 40, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858.

128. USTR, "The 2017 National Trade Estimate report."

129. Act on the Establishment, Management, etc. of Spatial Data (Korea: Gov. Body: Ministry of Land, Infrastructure and Transport, June 3, 2014), http://elaw.klri.re.kr/eng_service/lawView.do?hseq=32771&lang=ENG.

130. USTR, "The 2017 National Trade Estimate report."

131. "Joint Statement: Free Flow of Data."

132. "European Document Retention Guide" (De Brauw Blackstone Westbroek, October 2014) http://www.debrauw.com/wp-content/uploads/2015/01/EU-Retention-Guide-2014.pdf; "EU Country Guide."

133. "EU Country Guide."

134. Personal Information Protection Act (promulgated by the Ministry of Justice, Taiwan, May 26, 2010), http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021.

135. "Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions," *Official Gazette*, June 27, 2013, https://www.bddk.org.tr/websitesi/english/Legislation/129166493kanun_ing.pdf.

136. USTR, "The 2017 National Trade Estimate report."

137. Courtney M. Bowman, "An Overview of Turkey's New Data Protection Law," *Proskauer Privacy Law Blog*, April 15, 2016, http://privacylaw.proskauer.com/2016/04/articles/international/an-overview-ofturkeys-new-data-protection-law/.

138. Companies Act 2006 Chapter 46, United Kingdom, 2006, http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf.

139. 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.

140. Internal Revenue Service, *Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies* (Washington, DC: Internal Revenue Service, September, 2016), https://www.irs.gov/pub/irs-pdf/p1075.pdf.

141. "Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)" (Washington, DC: Defense Acquisition Regulations System, Department of Defense, August 26, 2015), https://www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for.

142. "City of Los Angeles: Supplemental Report – Information Technology Agency Request to Enter into a Contract with Computer Science Corporation for the Replacement of the City's Email System," Office

of the City Clerk, City of Los Angeles website, accessed April 26, 2017, http://clkrep.lacity.org/onlinedocs/2009/09-1714_rpt_cao_10-7-09.pdf.

143. "Tenn. governor signs bill discouraging offshore work," *USA Today,* May 16, 2017, http://usatoday30.usatoday.com/news/nation/2004-05-16-tenn-outsource_x.htm.
144. "Table Tracking State and Federal Global Sourcing Legislation", National Foundation for American Policy website, accessed April 26, 2017, http://www.nfap.com/researchactivities/globalsourcing/appendix.aspx.
145. "House Bill No. 1497," Missouri House of Representatives website, accessed April 26, 2017, shttp://www.house.mo.gov/billtracking/bills041/billpdf/intro/HB1497I.PDF.
146. "Senate Bill S3713 of 2011," New York State Senate website, accessed April 26, 2017, https://www.nysenate.gov/legislation/bills/2011/S3713.
147. 'Vietnam: 2015 Country Reports on Human Rights Practices" (Washington, DC: U.S. Department of States, April 13, 2016), https://www.state.gov/j/drl/rls/hrrpt/2015/eap/252813.htm.
148. US-ASEAN Business Council and Informational Technology Industry Council (joint letter to Vietnamese Minister Son, Minister of Information and Communication, January 6, 2016), http://cloud.chambermaster.com/userfiles/UserFiles/chambers/9078/File/ICT/2015/VietnamOTTCircular-USABC-ITILetterFINAL.pdf.
149. Decree No. 72/2013/ND-CP, of July 15, 2013, on the Management, Provision and Use of Internet Services and Online Information, Vietnamese Government, July 15, 2013, https://www.vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF.
150. Decree No. 90/2008/ND-CP of August 13, 2008, on Against Spam, Vietnamese Government, August 12, 2008, http://kenfoxlaw.com/resources/legal-documents/governmental-decrees/2555-vbpl-sp-1842.html.
151. Business Roundtable, "Promoting Economic Growth Through Information Technology Policy."

ERRATUM

This report has been updated on page 15. An earlier version incorrectly identified the U.S. government's Digital Attaché program as being under the direction of the U.S. Trade Representative. It is under the U.S. Department of Commerce.

ACKNOWLEDGMENTS

The author wishes to thank Robert D. Atkinson (ITIF), Stephen Ezell (ITIF), and Daniel Castro (ITIF) for providing input to this report. Any errors or omissions are the author's alone.

ABOUT THE AUTHOR

Nigel Cory is a trade policy analyst at ITIF. He previously worked as a researcher at the Sumitro Chair for Southeast Asia Studies at the Center for Strategic and International Studies. Prior to that, he worked for eight years in Australia's Department of Foreign Affairs and Trade and also had diplomatic postings to Malaysia and Afghanistan. Cory holds a master's degree in public policy from Georgetown University and a bachelor's degree in international business and commerce from Griffith University in Brisbane, Australia.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as one of the world's leading science and technology think tanks, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

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