ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

April 10, 2018
Committee Secretariat
PO Box 6021
Parliament House
Canberra, ACT, 2600

Sir/Madam:

The Information Technology and Innovation Foundation (ITIF) appreciates the opportunity to make a submission to the Joint Standing Committee on Trade and Investment Growth's (the Committee) inquiry into the global trade system and the digital economy.

ITIF is a non-partisan, non-profit think tank based in Washington D.C. which focuses on the intersection of technological innovation and public policy. Ranked the world's top science and technology think tank in the latest edition of the University of Pennsylvania's Global Go To Think Tank index, ITIF provides research and advice to policymakers from around the world on a range of pertinent issues, including digital trade, intellectual property, advanced manufacturing and automation, the Internet of Things, and data-driven innovation.

Sincerely,

Nigel Cory
Senior Trade Policy Analyst, The Information Technology and Innovation Foundation

INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION | ITIF.ORG | 1101 K STREET NW | SUITE 610 | WASHINGTON, DC 20005
MAIL@ITIF. ORG | (202) 449-1351 | FAX: (202) 638-4922

CONTENTS

OVERVIEW

Australia's economic future will depend on successfully driving innovation and productivity growth. Digital free trade and the free flow of data supports these by improving firm competitiveness and by providing critical economies of scale (via open global markets), which also underpins the ability of Australian firms to invest in the research and development needed for future innovation. However, policymakers need to make conscientious decisions to convert this potential scale into economic value. A pro-active and digitally-focused trade policy is definitely one of the many levers Australian policymakers should use when seeking to build an international framework that supports free and open digital trade. It needs to be a priority as, collectively, countries that support the international trading system have not done enough to ensure it adjusts to the data-driven nature of 21st-century trade, from its (largely successful) focus on addressing barriers to traditional 20th-century trade (tariffs). In this way, Australia's economic and trade policy strategies will need to reflect the emerging set of behind-the-border digital trade barriers that countries are enacting in an attempt to give their local firms an unfair advantage.

Australia has already taken many steps to ensure its trade policy reflects the increasingly digital nature of international trade and economic activity. This is reflected in the fact that 9 of Australia's 10 existing free trade agreements include e-commerce provisions. Australia's commitment to negotiating and completing the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and its high-standard e-commerce provisions go a long way toward setting new global standards on many digital trade issues. This Senate inquiry, the "2017 Foreign Policy White Paper," the Department of Industry, Innovation, and Science's report on "The Digital Economy: Opening Up the Conversation," and the Australian government's International Cyber Engagement Strategy are all welcome steps toward revising and shifting Australia's focus, goals, resources, and structures toward digital issues. Yet, much more can be done to ensure Australian firms are best placed to benefit from trade rules that addresses modern digital issues, as this report outlines. Australia is well placed to build on this progress and use it as the basis for heightened engagement internationally on new rules, norms, and cooperation to support an open and competitive global digital economy.

In reviewing its trade policy, Australia needs to recognize that it cannot afford to stand still, as it is in a global race for innovation advantage. Countries increasingly recognize that conscientious policy decisions impart a tremendous impact on the levels of innovation their economies and societies produce, as ITIF identifies in *Innovation Economics: The Race for Global Advantage*.[1] China, the United States, the European Union, and many other countries are pursuing policies that support their own ability to innovate and compete in new technology. Unfortunately, as this global race for innovation advantage intensifies, many countries have turned to "innovation mercantilism"—a strategy that seeks to achieve prosperity by imposing protectionist- and trade-distorting policies that tip market scales in favor of local firms in order to help them expand domestic technology production. These destructive "beggar-thy-neighbor" tactics are intended to either replace imports with domestic production or to unfairly promote exports. Countries are increasingly using such innovation mercantilist policies in high-value tech sectors such as computers and electronics and Internet services, including by introducing barriers to data flows. Australia's trade policy needs to adjust to this race and the changing nature of protectionism.

The following submission covers several critical policy issues relevant to the Committee's investigation into the trading system, the digital economy, and Australian trade policy. Firstly, the submission focuses on the critical role of data to digital trade, the rationales countries use to enact barriers to data flows, and the impact of these barriers, including relevant econometric studies that estimate the cost of barriers to data flows, including local data residency requirements. In addition to this, Appendix A-D provides a number of case studies to show how China, Indonesia, Vietnam, and Russia have enacted a range of barriers to digital trade, while Appendix E provides an extensive list of data localization policies in these countries and others around the world. The submission then examines issues around the measurement of data flows and digital trade in Australia, which needs improvement in order to provide a better basis of understanding for policymakers. Building on this, the submission analyzes how Australia should do more to improve the measurement of data flows and digital trade at the multilateral level, along with efforts to push multilateral organizations to do more to identify and report on barriers to both data flows and digital trade. In conclusion, the submission looks at the critical role of intellectual property in digital trade.

THE CRITICAL ROLE OF DATA

Australia's digital trade policy should be built on the central feature of the global digital economy—the free flow of data. Provisions and policies that protect the free flow of data—all types, such as health, financial, and other personal data—are critical to this as there is uncertainty about whether current trade rules apply to data, a fact which many countries are exploiting to enact barriers (which this submission will address later). Data should be viewed as central as it 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.

The increased digitalization of organizations, driven by the rapid adoption of technologies like mobile devices, cloud computing, and the Internet of Things, has increased the importance of data as an input to commerce, impacting not just information industries, but traditional industries as well. (In fact, 75 percent of the value of data flows over the Internet accrue to traditional industries such as manufacturing.)[2] Furthermore, the United Nations Conference on Trade and Development (UNCTAD) estimates that about 50 percent of all traded services are enabled by the technology sector, including by cross-border data flows.[3] 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.[4] For example, a 2014 survey found that data analytics are important to 60 percent of U.S. and European businesses with 50 or fewer employees.[5] 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.[6] McKinsey's report "Digital Australia: Seizing Opportunities from the Fourth Industrial Revolution" showcases the size of the benefit of data-driven innovation to Australia, estimating that the broad category of digital technologies could contribute AU$140 billion to AU$250 billion to Australia's GDP by 2025.[7]

In "Cross-Border Data Flows Enable Growth in All Industries," ITIF showed how data flows are critical to all sectors of an economy, not just tech.[8] For example, it included a case study of Rio Tinto, which has operations in over 40 countries across six continents.[9] To make its mining operations more efficient, Rio Tinto created its "Mine of the Future" program to "identify the size, location and quality of ore" by aggregating the data it collects in real time.[10] Rio Tinto collects this data from both the trucks and the drills that it uses in its mines all around the world.[11] This information is then processed at its Processing Excellence Centre (PEC) in Brisbane, Australia, generating millions of dollars in savings across its international organization by rooting out logistics inefficiencies.[12] PEC analyzes data from five of the company's mines in Australia, as well as mines in both the United States and Mongolia.[13] It receives data about 100 milliseconds after it is produced from the mines and then examines that data with 20 different analytical systems.[14] Each day the PEC sends and receives around 30 gigabytes to and from its operations.[15] It currently stores around five terabytes of this data for analysis.[16] PEC also connects to the data systems at each of its individual operations, forming "a common operational picture between the PEC and partner sites."[17] This process incorporates a variety of data from laboratories, process surveillance cameras, control systems, maintenance system logs, and several other sources.[18]

Barriers to Data Flows and Digital Trade

A good foundation for a review of Australia's trade policy in the age of digital trade should be, in part, built to reflect the nature of the barriers to digital trade that are emerging, especially barriers to data flows. 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."[19] Data localization can be explicitly required by law or be 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.[20] 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. ITIF has written extensively on barriers to data flows, including in "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?"[21]

The sizeable and growing threat to free trade in data puts the global digital economy at risk. This section examines the main justifications countries offer when they enact barriers to data flows and analyzes the cost of these barriers.

The Three "Justifications" for Data Localization

This section 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.

Privacy and Cybersecurity Rationales

At the heart of privacy- and cybersecurity-based localization policies lies the mistaken belief—held by a number of policymakers around the word—that data is more private and secure when it is stored within a country's borders. However, in most instances, data-localization mandates do not increase commercial privacy nor data security.[22]

For both of these issues, companies that have a legal nexus in a country—which places the company in that country's jurisdiction—must comply with the country's privacy and data protection laws—wherever they store the data. Companies can't escape complying with a nation's laws by transferring data overseas. 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 enterprise must comply with a counter's data privacy and protection 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. For this reason, companies should be able to move data wherever, since they are still subject to national privacy and security laws.

Policymakers focusing on geography to solve privacy and cybersecurity concerns are missing the point. Consumers and businesses 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 almost always 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 nation in which these systems are located 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.[23] 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.

Government Access to Data

The second motivation often given for why countries enact data-localization policies are concerns over government access to data. Governments obviously need a legal process to facilitate legitimate requests to access data for law enforcement and national security purposes. But this is where the focus should be—mandating ways to ensure access, not focusing on geography. Part of this is based on fear or uncertainty that other countries will withhold data that they may want in the future, whether for regulatory or legal issues. These uncertainties arise as modern technology and business operations means that multiple companies, individuals, and jurisdictions can be involved in owning, storing, and accessing data. For example, there was a recent dispute involving the U.S. Department of Justice and Microsoft about the jurisdiction of data relating to a criminal investigation of a person whose data is stored in Ireland. Thankfully, a new U.S. law—the CLOUD Act—created a legal pathway for the United States to form agreements with other nations that make it easier for law enforcement to collect data stored on foreign soil. Given the new law, both sides of the case have asked that the U.S. Supreme Court to drop the case.[24] However, this simply highlights the need to revise this antiquated process—state-to-state mutual legal assistance treaties—by which countries request assistance to transfer evidence from other countries, as ITIF argues in "How Law Enforcement Should Access Data Across Borders."[25]

Economic Development—"Digital Mercantilism"

The final justification countries use for data localization is to spur local economic development—yet this just constitutes a new form of "digital" mercantilism. 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.[26] 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. For the worst offenders of digital mercantilism, such as Indonesia, Nigeria, Russia, and China, data localization is often just one of many mercantilist tools used to target foreign firms and goods to give local firms an unfair advantage.

Such countries believe that if they restrict data flows they will gain a net economic advantage from companies relocating data-related jobs to their nation. These policymakers believe that, if they restrict data flows, their countries will gain a net economic advantage from companies being forced to relocate data-related jobs to their nations.[27] But 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.[28] 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 Costs of Barriers to Cross-Border Data Flows

Barriers to data flows—whether due to privacy and cybersecurity concerns, law enforcement, or digital mercantilism—affect a growing share of economic activity. Despite the mistaken rationales and self-inflicted damage data localization policies cause, these misguided views are spreading and threaten the foundational role that data plays in today's economy. 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 be moveable. Innovation and economic growth is 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 information technology (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.[29] 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

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.[30] Countries which 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 set themselves up to fail because their enterprises 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 research ones (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.[31]

Likewise, these barriers can impede important medical research. Compared to other categories of data, health data is much less "liquid" and is therefore underutilized due to the barriers put around this data.[32] This has consequences. For example, disease does not stop at national borders, therefore meaning that the data needed to find cures needs to cross borders too. Powerful data analytics applied to bigger global data sets can help speed the development of cures. The rarer the disease, the more important it is to build bigger data sets. By erecting barriers to the exchange of medical information (even anonymous data), countries' protectionist policies harm not only their own citizens but people around the world, all of whom benefit from advancements 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 like Hermes and Alliance Medical provide outsourced analysis of MRI scans, thereby decreasing healthcare 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.[33] 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.

Recommendations

1. Prioritize trade rules that support the free flow of data—all types—in bilateral, regional, and multilateral negotiations and discussions, such as at the newly formed e-commerce subgroup of WTO members.
    a. Do not allow exemptions from these rules for specific categories of data, whether health, financial, or personal data.
    b. For example, the exception for financial data from the Comprehensive and Progressive Agreement for Trans-Pacific Partnership's rules prohibiting barriers to data flows opens a dangerous loophole that countries could use to enact data localization. As ITIF reported in "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements," this provision was unnecessary (given prudential exceptions in typical trade agreements) and dangerous (as it opened a loophole to data localization as it validated the false belief that storing data outside a nation is somehow inherently riskier than storing it locally).[34]

2. Australia should follow through on its decision to join the Asia Pacific Economic Community's (APEC) Cross-Border Privacy Rules (CBPR) system.[35]
    a. The CBPR system provides a mechanism to facilitate the flow of personal information across borders while at the same time providing for the protection of personal information. This recognition is critical to a framework that supports the free of flow—that data protection should flow with the data, wherever it is stored.
    b. APEC's CBPR system also supports the equally critical notion that a company should be responsible, and held accountable, for following the domestic laws of each country it operates in and that these requirements move with the data, wherever it is stored.
    c. The CBPR system also recognizes that there is no one-size-fits-all approach to privacy and that different countries take different approaches, based on local political, social, and cultural values and institutions.
3. Australia should review all laws and regulations that could directly or indirectly act as a barrier to data flows.
    a. Australia should remove its forced local data storage requirement for health data. To be a leader in the global digital economy, Australia needs to lead by example by removing this requirement.
    b. The United States provides an example of how Australia should approach health data protection. U.S. law requires companies to enact proper data-protection measures and safeguards when processing data outside the United States, holding them responsible for the data regardless of where it is processed. U.S. companies mitigate these risks by stipulating requirements in relevant data handling and processing contracts. For example, Australian companies operating in the United States must comply with the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA), which regulates U.S. citizens' privacy rights for health data, even if they move data to Sydney. And, if a company's affiliate in Sydney violates HIPAA, then U.S. data authorities can bring legal action against the Australian company operating in America.
4. Australia should continue to push for a prohibition on customs duties on data transmissions in its trade agreements.
    a. The World Trade Organization (WTO) came close to not renewing the moratorium on these types of customs duties (which needs renewal every two years) at the WTO ministerial conference in Buenos Aires in December 2017 as some countries, such as Indonesia, wanted the moratorium overturned as these countries are considering enacting customs on data transmissions. It's critical that Australia and likeminded countries include rules that prohibit these types of duties as a way to build a broader basis of countries which are permanently committed to not taxing data imports/exports. The risk is that without such broad

agreement, more countries will consider this type of data tax in response to digital disruption.

IMPROVE AUSTRALIA'S MEASUREMENT OF DATA FLOWS AND DIGITAL TRADE

Australia, like many other countries, needs to develop better measures of the value of cross-border data flows and digital trade in order to ensure policymakers have the evidence they need. At the moment, precise, consistent, and comparable metrics on data flows and their value are hard to come by in Australia and many other countries. The same goes for the growing role of cross-border digital trade and e-commerce. More broadly, insufficient measurement of data flows contributes to issues relating to understanding its impact on productivity and GDP. Furthermore, even though the free flow of data across borders is crucial to nearly every sector of the economy, many countries have adopted protectionist data policies. However, it's hard to know the economic impact of these barriers. Just because the negative effects of these policies go unobserved does not mean there is not a significant and growing impact on Australian firms. The scope of the challenge for Australia and other countries focused on the digital economy and trade are clear. An Organisation for Economic Co-operation and Development (OECD) survey of its members' statistical measurement of the digital economy showed this: none of the 33 responses it received from members had conducted a study into quantifying cross-border data flows.[36]

Australia should ensure that it includes a concerted effort to improve its measurement of cross-border data flows and digital trade as part of any holistic review of its digital economy framework. Policymakers need a better understanding of how Australian firms and individuals are benefiting from these major digital economy trends. Australia has already taken a few tentative steps in the right direction; however, further effort is needed. The Australian Bureau of Statistics collects some general household data on Internet activity; business use of information technology; film, television, and digital games; information media; and telecommunications services.[37] Standard Australia's survey of digital trade needs in Australia and across the 10 countries of Association of Southeast Asian Nations (ASEAN) is also a good step in the right direction.[38]

Cross-border digital trade and e-commerce should technically show up in a country's balance of payments statistics as either a good or service import or export, often within the categories of postal and courier services, charges for the use of intellectual property, computer services, information services, and personal, cultural, and recreational services. However, the reality is that this doesn't happen. As this trade is largely intangible, it does not pass through a traditional customs process like with trade in goods, so it is not captured.

Likewise, despite the growing importance of digital trade, little empirical and internationally comparable statistical information currently exists.[39] Digitalization and digital trade raises considerable difficulties for measuring information services and data flows that are delivered digitally (e.g., software, e-books, and data and database services), cross-border services purchased by households, and the sharing economy. For example, international statistics in services trade are likely underreported, especially in regard to imports, as it is more difficult to identify and then sample the population of importers, unlike exporters, who are more easily identifiable. Again, the OECD survey reveals the scope of the challenge: the OECD survey revealed that none of the respondents from its survey had conducted a study to quantify the impact of digitalization on international trade (e.g., 3D printing or the Internet of Things), nor had any tried to study the issue of the

role of digital intermediaries in international trade.[40] It's not hard to see how these are increasingly critical topics for policymakers to understanding as digital trade policy becomes more important.

Australia is not alone in facing this challenge of better measuring and understanding the digital economy. The growing importance of digital trade has encouraged some countries to improve efforts to collect and collate relevant data, which are typically derived from either enterprise surveys (supply side) or consumer surveys (demand side). Given the challenges faced in improving statistical collection elsewhere, one of the current best methods for measuring the value of cross-border e-commerce and digital trade are surveys of sellers concerning their overseas sales. Official statistics on the value of cross-border digital trade are virtually non-existent. Some governments compile demand-side data on the number of individuals that buy from foreign websites, but very few collect data on the actual value of transactions. Furthermore, what is collected is business-to-consumer data, which leaves business-to-business e-commerce, which is likely to be more significant for international trade in goods and services.[41]

Australia can look to some emerging multilateral initiatives and country-level examples for ideas as to how to improve its ability to understand its digital economy. The United Nations Conference on Trade and Development's (UNCTAD) "In Search of Cross-Border E-commerce Trade Data" provides a useful overview of current measurement approaches and initiatives.[42] Another reference point is the OECD model survey on ICT access and usage by households and individuals, which includes questions about online purchases, but doesn't ask about cross-border purchases or sales.[43] Another model to build off, with the addition of a few questions about sales to overseas customers, business purchases online, and a breakdown of B2B and B2C sales, would be Eurostat's "ICT in Enterprises" survey.[44] The OECD's Working Party on Trade in Goods and Trade in Services (WPTGS) identifies some other potential approaches to follow. Germany is developing Trade by Enterprise Characteristics (TEC) data for European Commission statistics (specifically retail sales via mail order), Luxembourg, Netherlands, and Slovenia are exploring the ability to capitalize on ICT surveys, while others flagged the use of credit card data as a way to measure cross-border business-to-consumer e-commerce.[45] Other statistics agencies, such as in the United Kingdom, are working on clarifying terminology and the collection and analysis of data related to measuring the sharing economy.[46]

The U.S. Department of Commerce study, *Measuring the Value of Cross-Border Data Flows*, is another model that Australia could use.[47] The report is based on the challenge that the U.S. government has difficulty measuring the effects of cross-border data flows on productivity because there is not enough information about how exactly firms use data. At the heart of the Department of Commerce's efforts to improve government statistics on the service sector's engagement in digital trade is a plan to expand sample sizes, collect data more often, and provide more specific industry detail. Likewise, the U.S. Department of Commerce's *Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services* provides a framework for replication in analyzing digitally enabled service categories (such as business, professional, and technical services, telecommunications, and royalties) as a proxy (as there's no way to determine the exact percentage of the trade in each category that was digitally delivered) to measure digital trade.[48]

The recommendations from the *Measuring the Value of Cross-Border Data Flows* report are summarized below and provide a useful set of reference points for Australia:

- Improve the overall coverage and quality of official statistics on the service-sector and domestic and cross-border e-commerce and digital trade.
- Develop a standard nomenclature or standard definitions for concepts related to cross-border data flows, distinguishing between concepts such as digital economy, digitally intensive, digitally enabled economy, and information and communications technologies.
- Develop a greater understanding of how firms use cross-border data flows and what economic value the data flows provide.
- Develop improved and consistent macro-economic statistics to measure the value of cross-border data flows and the digital economy, such as the contribution of data flows and the digital economy to GDP.
- Continue the dialogue with private industry to facilitate data sharing and the linking of public and private datasets, where legally and logistically feasible and consistent with strong privacy protections for firms.
- Continue the collaborative efforts with international organizations to ensure that metrics on cross-border data flows and the digital economy are widely available for countries around the world.

The United States International Trade Commission (USITC) is another useful reference for Australia in how it has held multiple investigations into global digital trade and barriers to it, including the use of mandatory and confidential surveys of U.S. firms.

- The United States International Trade Commission's 2014 survey of U.S. firms as part of its investigation of Digital Trade in the U.S. and Global Economies (at pages 253 to 272 of the study report).[49] The survey covers obstacles to doing international business over the Internet and firms' use of the data and the Internet.
- The United States International Trade Commission's 2018 survey of U.S. firms as part of its Global Digital Trade investigation into business-to-business and business-to-consumers issues.[50]

No doubt there are conceptual and practical challenges to overcome in measuring the data flows and digital trade and their respective values, yet given the nature of the technologic innovation, this needs to change. Australian agencies should proactively engage in debates around how to conceptually fit data flows into the current accounting framework and on efforts to develop an internationally agreed upon methodology regarding the valuation of data and classification and treatment of such flows from a statistical standpoint.

Recommendations

1. Task respective agencies, such as the Bureau of Statistics, to undertake a project to conduct case studies and survey firms on their use of data and engagement in cross-border digital trade. The result

of any such effort should include the public release of methods and models so that users can understand how to interpret the data.[51]

2. Setup a working group to consider ways to revise existing surveys so that they better capture to what extent firms and individuals engage in cross-border digital trade. As part of this, agencies should consider how data-sharing partnerships with the private sector and international stakeholders may help them obtain the data they need to understand global data flows and digital trade.

IMPROVE INTERNATIONAL MEASUREMENT OF DATA FLOWS AND DIGITAL TRADE AND REPORTING ON BARRIERS TO BOTH

Just as Australian trade and economic policy needs to improve its measurement and awareness of data flows and digital trade, and barriers to these, so does it need to step up to push for better mechanisms at the international level. As shown by the relatively recent attempts by the World Bank and OECD to develop statistics that account for modern trade practices, such as data flows and global value chains, multilateral institutions have been slow to adapt. In order to properly assess the damage barriers to data flows and digital trade inflict on the global economy, Australia needs to use its membership in international organizations to push for better mechanisms to track and report on them.

Australia should also be proactively engaging in international efforts to develop a better understanding of digital trade and data flows. At the multilateral level, the OECD has started efforts to better understand how countries capture these statistics, but its initial reports show how Australia and others have a lot of work to do to better collect, measure, and analyze the value of data and digital trade. These organizations initially flagged measurement as an issue in 2016. As already mentioned, the OECD sent out a questionnaire to members as part of a tentative effort to build a typology of digital trade and to draft s definition for digital trade.[52] Efforts to clarify nomenclature are important as there is a lack of standard definitions for terms used by researchers, such as "digital economy" and "digitally intensive." This is important as while there has been relatively little study of cross-border data flows, the literature that does exist uses differing terms and definitions that make it difficult to compare one study to another. The OECD's stocktaking questionnaire to members asked the pertinent question as to whether countries can break down merchandise trade flows into those products ordered digitally (e-commerce) and those that were not. The results showed that very few countries are investigating cross-border digital trade and e-commerce.

As it relates to emerging barriers to data flows and digital trade, the International Monetary Fund (IMF), the World Bank, the World Trade Organization, and their respective trade databases do not explicitly track these barriers.[53] This makes it difficult to quantify the economic impact of barriers to data flows on national economies and the global marketplace. For example, the World Bank's World Integrated Trade Solution database lists "non-tariff" measures but does not specify what those non-tariff measures are for the purposes of identifying the problem (e.g., data residency requirements, forced technology transfer, etc.).[54] Another database that does this reasonably well in tracking localization barriers to trade is the Organisation for Economic Co-operation and Development's Services Trade Restrictiveness Index (STRI), which helps identify whether policy measures put forth by countries restrict trade, but it does not do this comprehensively, nor at a level of specificity, to act as a central database for measures which impede digital trade.[55]

Recommendations

1. Australia should conduct a whole-of-government review into the various initiatives underway at multilateral institutions on the measurement of data flows and digital trade as part of a renewed push to engage in these forums and work to improve the collection and reporting of these statistics.
2. Australia should push for these multilateral organizations—the IMF, World Bank, WTO, and OECD—to explicitly track barriers to cross-border data flows and digital trade in order to document the extent of their use and to contribute to further analysis of how they impact global trade.

DIGITAL TRADE AND INTELLECTUAL PROPERTY

To be effective, digital trade requires robust intellectual property (IP) protections, because without them producers will be less able to sell their products and services across borders. If a nation promulgates a weak IP regime and turns a blind eye to rampant piracy, imports of IP-based goods and services paid for with an export of money would by definition decline. Moreover, the knowledge and creativity required to create the goods and services exchanged in the 21st century—from smartphones, to biopharmaceutical drugs, to movies and music—is difficult to develop, but often very easy to steal or pay for at less than full market value. But without fair payment, global innovation and creative output decreases. The notion that intellectual property will not a crucial enabler of Australian digital trade ignores the fact that ideas and knowledge form the basis of many Australian firms' competitive advantage, especially in the services sector.

Critics of IP, trade, or both, try to exploit the fact that the popular understanding of trade is still based around manufactured goods facing tariffs when crossing borders, while IP is behind the border and nations have unlimited rights to do whatever they want with it. Liberal economist Paul Krugman speaks for many Trans-Pacific Partnership (TPP) critics when he asserts that the TPP "is not a trade agreement. It's about intellectual property and dispute settlement." But this narrow focus refuses to acknowledge that what goes on "behind the border" is central to shaping trade in the 21st century. The idea that reducing a tariff on a widget is legitimate in a trade agreement but that reducing the ability of a nation's citizens to steal another nation's goods and services—that is, ensuring robust intellectual property enforcement—is not legitimate is illogical. Trade in goods and services increasingly depends on intellectual property, and that IP needs to be protected in the trade agreements of tomorrow if we are to truly have global, market-based trade.

Nor should the Australian government pay attention to the mercantilist argument on IP—that Australia should not pursue IP protections at home or in trade agreements as it currently has a deficit in payments for IP royalties etc. The Australian government was wise to ignore recommendations for such an approach from Australia's Productivity Commission, which advocated for the removal of IP from Australia's trade agreements, given they viewed it in a purely "balance-of-trade" perspective (i.e., Australia imports more IP than it export; therefore, it should be reduced).[56] If Australia wants to be the home of innovation-intensive firms and those that digitally deliver goods overseas, it needs to protect its own firms' ability to use IP to profit from innovations.

The rise of digital trade makes embedding intellectual property regimes in trade agreements, such as the rules established in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, more imperative, as technology makes the sale of digital goods and services to foreign markets so much easier and cheaper, even as it also makes IP theft much easier. IP provisions need to be included as this is where modern barriers to trade exist. This is based on the fact that modern trade is increasingly in bytes, ideas, and services. Current international trade rules for IP are increasingly out of date given the base-level of global protection for IP—the Trade-Related Aspects of Intellectual Property (TRIPS) Agreement—was established in the 1990s when the Internet and e-commerce as we know it barely existed. The central fact that led to the many international treaties and trade agreements which deal with intellectual property—that intellectual property rights are territorial in character and are critical to trade—remains true for Australia today as it looks to future agreements.

Furthermore, any future Australian trade agreements need an IP chapter that also helps to improve IP enforcement: If they are to be effective, IP rules need to have consequences. While the economic cost of online piracy to Australian businesses is hard to specify, it is undoubtedly high, given the impact that lost revenue has on profits (and therefore taxes), employment, content production, and innovation.[57] As part of this, Australia should ensure that future trade agreements provide the space and recognition for countries to enact measures to better enforce IP online, including through website blocking. Australia is one the growing number of countries which ask domestic Internet service providers (ISPs) to block access to websites dedicated to distributing illegal copies of movies, music, and other copyright-protected works, just as it does for websites facilitating other criminal activities, such as child pornography, malware, and investment fraud.[58] Where countries are using website blocking to fight digital piracy, the record shows it has been effective in driving users from illegal to legal sources of copyrighted material online, such as in a recent study in which Carnegie Mellon University examined the real-world impact of website blocking in the United Kingdom.[59] The Australian Department of Communications and the Arts public consultation on the site-blocking mechanism introduced by the Copyright Amendment (Online Infringement) Act 2015 is a worthwhile opportunity to review the process and consider changes that would improve it.[60]

Recommendations

1. Recognize that digital trade requires robust intellectual property protections to be effective, meaning that Australia should continue to pursue higher levels of intellectual property protection and enforcement in future trade agreements.

APPENDIX A: DATA-LOCALIZATION POLICIES AROUND THE WORLD

Appendix E lists many of the data localization policies around the world.[61] 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 (e.g., 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.

The following appendices provides examples of how China, Indonesia, Vietnam, and Russia have enacted a range of barriers to digital trade and cross-border data flows.

APPENDIX B: CHINA: USING DATA LOCALIZATION AND REGULATIONS TO PRECLUDE ACCESS TO ITS CLOUD COMPUTING MARKET

China makes pervasive use of digital protectionism through the use of data localization, discriminatory and arbitrary regulations, and restrictive market access conditions. In 2016, the United States Trade Representative'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…[62]

In addition to explicit data-localization rules, China uses regulations and market-access restrictions to discriminate against foreign cloud service providers. In 2016, new regulations regarding cloud-computing services in China confirm its persistence in erecting barriers between its tech sectors and digital economy and that of the rest of the world. In March 2016, China made significant changes to the licensing and regulatory regime of Chinese telecom and Internet services that essentially exclude foreign technology firms involved in cloud computing, big data, and other information services from operating in China. These regulations, again, reinforced the requirement for forced local data storage.[63] For foreign cloud-service providers—which include many leading U.S. companies—these regulations have essentially closed access to the Chinese market.

China enacted regulatory changes to make it even harder than it already was for foreign companies to establish and operate Internet-based information services in the country. First, China released regulations for several services it considers valued-added telecommunication services (VATS). By categorizing Internet-based services (e.g., cloud computing, big data, and other information services) as telecommunication services, and not as "computer and related services," it has much greater freedom to restrict market access to foreign tech firms. This is because China made commitments as part of its accession to the World Trade Organization in 2001 to provide nondiscriminatory treatment and market access to foreign firms in "computer and related services."[64] This category of Internet-based computer services includes email, voicemail, online information and database retrieval, electronic data interchange, and enhanced facsimile services, code and protocol

conversion, and online information and/or data processing.[65] Essentially, China's approach is a technical work-around to avoid its commitment to open its market for Internet-based computer services to foreign competition.

Second, China introduced a requirement for telecom and Internet Service Providers (ISPs) to apply for licenses for each subcategory of services, raising the potential for government agencies to discriminate against foreign firms. For example, China's new subcategory, "internet-based resources collaboration services," means that providers of cloud-computing application services, platform as a service, and software as a service would potentially have to apply for multiple licenses, given some firms and services cross over into multiple categories.

Third, China released new requirements that articulate the very small and restricted cloud-computing services space where foreign firms are allowed to operate. In October 2016, the Ministry of Industry and Information Technology released the "Notice on Regulating Business Behaviors in the Cloud Service Market," which outlined how foreign cloud companies are forbidden from working via local partnerships in any capacity beyond "technical assistance." It is not specified what is allowed under "technical assistance," but based on current practice, it is likely to mean that foreign companies are only allowed to license their goods (software and hardware) to their (forced) local partners and show them how to use them. The notice further specifies several activities that cloud service providers cannot perform, such as sign contracts directly with end users. These new restrictions on foreign cloud service providers make an already restrictive situation that much worse. Strict entry requirements and (an already highly) discriminatory licensing process have largely kept foreign firms out of China's market. To operate in China, foreign firms must set up a joint venture with a Chinese partner who must have majority ownership (i.e., greater than 50 percent). A joint venture was a prerequisite for foreign firms to even apply for a license from Chinese authorities, who have proven to be highly discriminatory against foreign firms. Although there are over 20,000 local companies licensed to provide VATS in China, only 30 or so licenses have been issued to foreign companies, including five U.S. companies.[66]

A few large foreign firms have successfully run the gauntlet and decided to operate in China within the confines of these strict conditions by partnering with large Chinese firms—for example, Microsoft with 21Vianet (China's largest private data-center operator), SAP with China Telecom, and IBM with a group of local companies.[67] As described, these foreign firms are severely restricted in what they can do, often being constrained to arrangements whereby they license their products to their local partners, who set up and run the data centers and cloud services and manage relations with end users.

This mercantilist approach to cloud computing is consistent with China's ongoing efforts to develop a local cloud-computing sector that uses indigenously developed technology. China's ambitions in the sector started as part of the country's *National Medium and Long-Term Plan (MLP) for Science and Technology Development (2006-2020)*. Building on this in 2010, China identified cloud computing as one of 11 strategic emerging industries that would receive special attention and funding, all in pursuit of the goal of expanding access to cloud resources in China, developing indigenous cloud-computing technology, and creating an internationally competitive Chinese cloud-computing sector. More recently, the Ministry of Science and

Technology's 12th Five-Year Plan (2011-2015) paid particular attention to cloud computing, where the aim became to develop a cloud-computing standard based on indigenously developed technology.[68] These policies, taken together, show China's efforts to use mercantilist policies at home to support the development of "local champions," who will eventually become more innovative and competitive and able to compete in overseas markets—against the very tech firms that are unable to compete in China.

APPENDIX C: INDONESIA AND VIETNAM: USING DATA LOCALIZATION TO TARGET OVER-THE-TOP SERVICES

Indonesia and Vietnam have both enacted an extensive range of data localization and other barriers to digital trade, most recently targeting over-the-top (OTT) services. On March 31, 2016, Indonesia's Ministry of Communications and Informatics issued Circular Letter No. 3, which notifies companies about new regulations for over-the-top (OTT) services, such as requirements for forced data localization and the need for foreign OTT firms to establish a permanent office in Indonesia as a condition of market entry.[69] In January 2016, Vietnam released a draft regulation—Draft Decree Amending Decree 72—for OTT services that included a forced data-localization requirement and the transfer of power to control OTT services to domestic telecommunications firms.[70] These restrictive policies will raise costs, diminish the incentives for service providers to offer OTTs, reduce competition in a growing market, and potentially weaken data protection and cybersecurity measures, given the need to set up and manage duplicative infrastructure or to use data-center providers who do not use best-in-class protective measures.

OTT services are those delivered via the Internet and are some of the most popular and innovative services available. In broadcasting, OTT service providers (such as Netflix, Hulu, and HBO Go) deliver audio, video, and other media over the Internet without users having a subscription with the usual intermediaries, such as cable companies. For messaging, OTT service providers, such as WhatsApp, Skype, and Facebook, provide instant-messaging services as an alternative to text-messaging services provided by traditional mobile network operators. In using the Internet, OTT service providers and their customers can bypass traditional telecommunications network service providers to compete with services (such as voice) from telecommunications companies. These technological innovations have changed consumer behavior in media and telecommunications markets, among others, allowing consumers to change how they access and consume media and communicate. This is especially the case in developing countries that have deployed mobile-phone services before (or instead of) traditional phone services, thereby leapfrogging costly fixed-line infrastructure, which also led to a vibrant app and digital economy.

The letter from Indonesia's Ministry of Communication and Informatics notified foreign OTT service providers that upcoming regulations will require these providers to abide by a number of mercantilist and trade-distorting measures, such as:

- Forcing fee-for-service OTT providers (such as those that require a subscription) to form a joint venture with a local telecommunications provider;[71]
- Requiring companies to disclose source code as a condition of market access;
- Forcing companies to store data locally;
- Requiring companies to establish a permanent local office to operate in Indonesia;

- Requiring firms to use content filtering in accordance with Indonesian law, such as for security purposes (such as terrorism) or social/cultural purposes (such as pornography);
- Forcing firms to use an Indonesian Internet protocol number; and
- Forcing firms to use Indonesia's National Payment Gateway, a government-owned and run process that aims to make Indonesia's four payment systems interoperable, but in doing so, discriminates against foreign payment providers in a misguided attempt to coerce more local financial activity in e-commerce and other sectors.[72]

For Vietnam, the circular it issued requires OTT firms to locate servers in Vietnam. The draft regulation also restricts how foreign OTT services operate in Vietnam by forcing them to form a joint venture with Vietnamese telecommunications companies. Meanwhile, it promulgates differentiated regulations for free- and fee-based OTT services, as the latter need to get a license from the government, while the former do not.[73]

By introducing data-localization requirements, the Indonesian and Vietnamese governments reduce the benefits that come from competition among foreign OTT services (such as WhatsApp, Viber, and Tango), local providers (such as Zalo, Mocha, and VietTalk), and traditional telecommunications service providers. OTT services are obviously meeting a market demand that traditional carriers are not. This regulation can have a substantial impact on a growing area of digital activity—20 million Vietnamese had OTT apps on their smartphones as of 2015 (Vietnam has a population of 90 million).[74]

In both countries, these protectionist policies seem intended to protect inefficient, state-owned incumbent firms. In Indonesia, this is evident from the requirement to form a joint venture with a local telecommunication firm.[75] Indicative of this, in January 2016, Indonesia's biggest (state-owned) telecommunications provider, Telekom Indonesia, blocked Netflix's entry into Indonesia because it did not have the right license and due to concerns about the content it carries.[76] Following this, Telkom Indonesia found a foreign company willing to abide by Indonesia's strict entry requirements to launch a video-streaming service—Hooq, a Singapore-based company—while still blocking Netflix.[77]

In Vietnam, media reports state that Vietnam's prime minister ordered the Ministry of Information and Communications to restrict free OTT apps, such as Viber and Zalo (a local app), due to the impact these apps were having on traditional mobile carriers. As a Zalo representative rightly pointed out, free email services took over from postal services, but no one banned these services, yet the government seems intent on trying to do this with OTT services.

If Vietnam and Indonesia want a vibrant, competitive, and world-class digital economy, it should reverse these types of policies. Both countries should not be prescribing how users access and use digital services and how these digital services operate, as this limits consumer choice and engagement, and business innovation. Consumers and businesses benefit when there is healthy competition between network and service providers, which is what should be happening between OTT service providers and traditional telecommunications firms. First, by requiring local data storage, the government increases operating costs for local and foreign

firms. Second, by forcing companies to form joint ventures, the government limits the number and ability of firms to innovate and compete, especially small app-makers involved in OTT services. However, while local firms may be affected by both measures, the burden falls disproportionately on foreign firms.

APPENDIX D: RUSSIA: EXPANDING ITS USE OF DATA LOCALIZATION MEASURES FOR DIGITAL MERCANTILISM

The Russian government's parallel moves toward mercantilism and authoritarianism came together in a new surveillance law that includes extensive data-localization requirements for telecommunications data, adding an additional layer to already-extensive barriers to cross-border flows between Russia and the rest of the world. On July 6, 2016, Russia enacted a new law that forces telecommunication companies and ISPs to retain user communications for six months and communications metadata for three years. The law will apply to companies in Russia and overseas. Companies have until July 1, 2018, to implement these measures.[78]

The law aims to help Russian authorities fight terrorism, but its impact will be felt economy-wide (and society-wide), especially by Russia's digital economy. First, the surveillance and localization requirements are much broader than other countries' telecommunications data-retention requirements, such as those of Germany, 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 a user if they fail to respond to a request from law enforcement to confirm their identity (which raises a range of privacy issues). Third, it forces companies to help government authorities in decrypting user communications and prohibits encryption measures unless a decryption tool is available should Russian authorities need it. Fourth, it applies to foreign companies that fall within the broadly defined category of telecom providers and "facilitators of information dissemination by means of the Internet," such as online messaging services, email providers, social media and blogging sites, voice over Internet protocol services (which use the Internet to transmit voice and multimedia), and news sites.[79]

Russia already has one of the most extensive data-localization laws in place, and once this law comes into force, the impact it will have on Russia's economy will increase. In 2015, Russia enacted a law that forces companies with Russian personal data to store it locally.[80] Russian telecommunications companies have complained about the large potential costs of implementing these extensive and intrusive laws. MegaFon, Russia's second-largest mobile-phone company, said that equipment and operating costs of implementing this new law are estimated to be around $3.6 billion.[81] These costs inevitably get passed on to customers, which drags down economic growth. Tele 2, another Russian mobile-phone provider, said that it would likely have to raise prices by two or three times to cover the costs of implementation.[82] Beyond the implications for privacy and freedom of expression in Russia, these policies will certainly chill Russia's digital economy, as it makes it harder and costlier for both domestic and foreign firms to operate.

APPENDIX E: LIST OF DATA LOCALIZATION MEASURES

Country	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.[83]
Australia	In 2012, Australia enacted the Personally Controlled Electronic Health Records Act, which requires that personal health records be stored only in Australia.[84]
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.[85] 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.[86]
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.[87] 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.[88]
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.[89] 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).[90]
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.[91] For example:

- In 2006, China introduced measures for e-banking that require such companies to keep their servers in China.[92]
- In 2011, China introduced a law that prohibits the off-shore analyzing, processing, or storage of Chinese personal financial information.[93]
- In 2013, China enacted new rules regarding credit reporting that requires all credit information on Chinese citizens to be processed and stored in China.[94]
- In 2014, China enacted new rules that require health and medical information to be stored only in China.[95]
- In 2015, China released draft administrative regulations for the insurance industry that included localization requirements.[96]
- In 2016, China enacted new rules the forced companies involved in Internet-based mapping services to store data locally.[97]
- 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.[98] 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.[99] 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.[100]
- 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.[101]
- 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."[102]

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.[103] 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.[104]
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.[105] 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.[106] 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.[107]
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.[108] 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.[109] 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.[110] 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.[111] 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.[112]
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.[113] 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.[114]
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.[115] 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.[116] 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.[117] 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.[118] Germany's Commercial Code requires companies to store accounting data and documents locally.[119] 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).[120] 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.[121]
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.[122] The European Commission has also criticized the law as being inconsistent with the E.U. single market, but it remains in effect.[123]
India	India has proposed a range, and enacted some, laws and regulations requiring data localization. India's Ministry of Communications and Technology enacted restrictive data transfer requirements as part of a 2011 change to privacy rules. 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.[124] 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.[125] 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.[126] 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.[127] 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.[128] 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.[129]
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.[130] 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.[131] 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."[132] 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.[133] 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.[134] 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.[135]
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.[136] 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.[137] In May 2016, Iran ordered foreign messaging apps, such as WhatsApp and Telegram, to store data from Iranian users locally.[138]
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).[139] 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.[140]
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."[141] While no data localization has been enacted (yet), this sounds suspiciously like an attempt to use localization for mercantilist ends.
Luxemburg	In 2012, Luxemburg'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.[142]
Malaysia	In 2010, Malaysia enacted the Personal Data Protection Act, which came into force in 2013.[143] 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.[144] 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.[145]

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.[146] 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.[147]
New Zealand	New Zealand's Internal Revenue Act requires businesses to store business records in local data centers.[148]
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.[149]
Romania	In 2015, Romania enacted new online gambling regulations that requires all data on players and their gambling activities to be stored in Romania.[150]
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.[151] 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.[152] Furthermore, in 2016, Russia enacted extensive new data-localization requirements for telecommunications data.[153] 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.[154] 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.[155] 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.[156] 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.[157]
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.[158] Furthermore, Sweden has accounting requirements that force companies to store data about current company records and accounts in Sweden for seven years.[159] 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.[160]
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.[161]
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.[162] 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.[163] 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.[164]

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".[165]
United States	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 locally.[166]
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.[167] 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.[168] 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."[169] 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.[170]
Venezuela	Venezuela has passed regulations requiring that IT infrastructure for payment processing be located domestically.[171]

ENDNOTES

1. Robert D. Atkinson and Stephen J. Ezell, *Innovation Economics: The Race for Global Advantage* (New Haven, CT: Yale University Press, 2012).

2. Matthieu Pélissié du Rausas et al., "Internet matters: The Net's sweeping impact on growth, jobs, and prosperity," McKinsey Global Institute, May 2011, http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

3. United Nations Conference on Trade and Development (UNCTAD), *Information Economy Report*, (UNCATD, Geneva, 2009), http://unctad.org/en/docs/ier2009_en.pdf.

4. Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries" (The Information Technology and Innovation Foundation, February 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf.

5. Victoria Espinel, "Executive Survey Shows the Benefits of Data Innovation Across the Whole Economy," *TechPost*, December 10, 2014, http://techpost.bsa.org/2014/12/10/executive-survey-the-shows-the-benefits-of-data-innovation-across-whole-economy/.

6. National Board of Trade Sweden, *No Transfer, No Trade*, (Stockholm, Sweden: National Board of Trade Sweden), http://unctad.org/meetings/en/Contribution/dtl_ict4d2016c01_Kommerskollegium_en.pdf.

7. Simon Blackburn, Michaela Freeland, and Dorian Gartner, "Digital Australia: Seizing opportunities from the Fourth Industrial Revolution," McKinsey Global Institute, 2017, https://www.mckinsey.com/global-themes/asia-pacific/digital-australia-seizing-opportunity-from-the-fourth-industrial-revolution.

8. Castro and McQuinn, *Cross-Border Data Flows Enable Growth in All Industries*.

9. "About Rio Tinto," *Rio Tinto*, accessed April 9, 2018, 2018, http://www.riotinto.com/aboutus/about-rio-tinto-5004.aspx.

10. "Rio Tinto accelerates productivity drive with world-first technology to enhance mineral recovery," Rio Tinto website, September 23, 2014, http://www.riotinto.com/media/media-releases-237_12852.aspx.

11. Ibid.

12. "Big data results in big savings at Rio Tinto," *Engineers Australia*, March 25, 2014, http://www.engineersaustralia.org.au/news/big-data-results-big-savings-rio-tinto.

13. Ibid.

14. Ibid.

15. Ibid.

16. Ibid.

17. Ibid.

18. Ibid.

19. 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.

20. There is no one definition of digital trade. The definition used is from the United States International Trade Commission (USITC) report on 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.

21. Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?", https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

22. 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.

23. 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.

24. Jackie Wattles, "Microsoft email privacy case no longer needed, DOJ says," *CNN,* March 31, 2018, http://money.cnn.com/2018/03/31/technology/microsoft-lawsuit-supreme-court-justice-department/index.html.

25. Alan McQuinn and Daniel Castro, "How Law Enforcement Should Access Data Across Borders (Information Technology and Innovation Foundation, July, 2017), http://www2.itif.org/2017-law-enforcement-data-borders.pdf.

26. 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.

27. 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.

28. 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/.

29. 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.

30. Mr. Christian Reimsbach-Kounatze and Mr. 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.

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

32. David Bollier, "The Promise and Peril of Big Data" (Washington, D.C.: The Aspen Institute, 2010), http://csreports.aspeninstitute.org/documents/The_Promise_and_Peril_of_Big_Data.pdf.

33. 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 and 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.

34. Nigel Cory and Rob Atkinson, "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements" (The Information Technology and Innovation Foundation, April, 2016), http://www2.itif.org/2016-financial-data-trade-deals.pdf.

35. "Australia Announces Plans to Participate in APEC Cross-Border Privacy Rules," Hunton and Williams Information Security Law Blog, November 28, 2017, https://iapp.org/news/a/australia-announces-it-will-participate-in-apec-cbpr-system/.

36. Organisation for Economic Cooperation and Development (OECD), *Working Party on International Trade in Goods and Trade in Services Statistics* (Paris: OECD, 2017), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=STD/CSSP/WPTGS(2017)1&docLanguage=En.

37. "Technology and Innovation," Australian Bureau of Statistics website, accessed April 9, 2018, http://www.abs.gov.au/Technology-and-Innovation.

38. "The Future of ASEAN and Australian Digital Trade," Standards Australia website, accessed April 9, 2018, https://www.standards.org.au/news/the-future-of-asean-and-australian-digital-trade.

39. Organisation for Economic Cooperation and Development, *Working Party on International Trade in Goods and Trade in Services Statistics.*

40. Ibid.

41. United Nations Conference on Trade and Development (UNCTAD), *In Search of Cross-Border E-Commerce Trade Data* (Geneva: UNCTAD, April, 2016), http://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d06_en.pdf.

42. Ibid.

43. Organisation for Economic Cooperation and Development (OECD), *The OECD Model Survey on ICT Access and Usage by Households and Individuals,* https://www.oecd.org/sti/ieconomy/ICT-Model-Survey-Access-Usage-Households-Individuals.pdf.

44. "COMMUNITY SURVEY ON ICT USAGE AND E-COMMERCE IN ENTERPRISES 2015," Eurostat website, accessed April 9, 2018, https://circabc.europa.eu/sd/a/7956316e-50f6-4f14-a144-055cb8af4901/Questionnaire%20ENT2015.pdf.

45. Organisation for Economic Cooperation and Development, *Working Party on International Trade in Goods and Trade in Services Statistics.*

46. "The feasibility of measuring the sharing economy: progress update," Office of National Statistics website, accessed April 9, 2018, https://www.ons.gov.uk/economy/economicoutputandproductivity/output/articles/thefeasibilityofmeasuringthesharingeconomy/progressupdate.

47. U.S. Economics and Statistics Administration and the National Telecommunications and Information Administration, *Measuring the Value of Cross-Border Data Flows* (Washington D.C.: U.S. Economics and Statistics Administration and the National Telecommunications and Information Administration, September, 2016), https://www.ntia.doc.gov/files/ntia/publications/measuring_cross_border_data_flows.pdf.

48. Jessica Nicholson and Ryan Noonan, *Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services* (Washington D.C: U.S. Department of Commerce, January, 2014), http://www.esa.doc.gov/sites/default/files/digitaleconomyandtrade2014-1-27final.pdf.

49. U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*.

50. U.S. International Trade Commission, *Global Digital Trade Survey* (Washington D.C: U.S. International Trade Commission, 2018), https://www.usitc.gov/documents/global_digital_trade/global_digital_trade_survey_form_fillable.docx.

51. Andrew Kitchel and Daniel Castro, "Better Measures of the Data Economy Are Needed to Show the High Costs of Cross-Border Data Restrictions" (The Center for Data Innovation, January, 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/.

52. Digital trade involves those cross-border resident/non-resident transactions for which the ordering and/or delivery process is digitally enabled or facilitated via online platforms or web services. Organisation for Economic Cooperation and Development, *Working Party on International Trade in Goods and Trade in Services Statistics.*

53. Stephen Ezell, Robert Atkinson, and Michelle Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy," *The Information Technology and Innovation Foundation,* 69.

54. "World Integrated Trade Solution," *World Bank*, accessed April 9, 2018, http://wits.worldbank.org/.

55. "Services Trade Restrictiveness Index," *The Organisation for Economic Co-operation and Development*, accessed April 9, 2018, http://www.oecd.org/tad/services-trade/services-trade-restrictiveness-index.htm.

56. Australian Government Productivity Commission, *Bilateral and Regional Trade Agreements* (Canberra: Productivity Commission, November, 2010), https://www.pc.gov.au/inquiries/completed/trade-agreements/report/trade-agreements-report.pdf; Australian Government Productivity Commission, *Intellectual Property Arrangements* (Canberra: Productivity Commission, December, 2016), http://www.pc.gov.au/inquiries/completed/intellectual-property/draft/intellectual-property-draft.pdf.

57. Adams Nager, "The Creative Cost of Piracy," Innovation Files, October 3, 2014, http://www.innovationfiles.org/the-creative-cost-of-piracy/; Adams Nager, "Yes, Piracy Costs Content Creators a Fistful of Dollars," Innovation Files, October 8, 2015, http://www.innovationfiles.org/doespiracy-cost-content-creators-a-fistful-of-dollars/; Stephen Ezell, "Global IP Infringement's Significant Cost to the U.S. Economy," Innovation Files, February 26, 2015, http://www.innovationfiles.org/globalip-infringements-significant-cost-to-the-u-s-economy/.

58. Nigel Cory, "How Website Blocking Is Curbing Digital Piracy Without Breaking the Internet," (the Information Technology and Innovation Foundation, August, 2016), https://itif.org/publications/2016/08/22/how-website-blocking-curbing-digital-piracy-without-breaking-internet.

59. Brett Danaher, Michael D. Smith, and Rahul Telang, "Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior" (paper, Carnegie Mellon University, Pittsburg, April 18, 2016), http://ssrn.com/abstract=2766795http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2766795.

60. Rohan Pearce, "Australia's website-blocking regime under review," *Computerworld,* February 14, 2018, https://www.computerworld.com.au/article/633397/australia-site-blocking-regime-under-review/.

61. Cory, *"Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?"*

62. United States Trade Representative, *The 2016 National Trade Estimate report* (Washington, D.C.: United States Trade Representative), https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf.

63. Barbara Li, "China's New Telecom Catalogue Comes Into Force on March 1, 2016," *Norton Rose Fulbright*, February 2016, http://www.nortonrosefulbright.com/knowledge/publications/137503/chinas-new-telecom-catalogue-comes-into-force-on-march-1-2016; Jacob Parker, "US-China Business Council Comments on the Draft Cybersecurity Law" (The US-China Business Council, August 4, 2016), https://www.uschina.org/sites/default/files/USCBC%20Comments%20on%20Cybersecurity%20Law_EN.pdf.

64. World Trade Organization Council for Trade in Services, "Computer and Related Services Background Note by the Secretariat S/C/W/45" (Geneva: World Trade Organization, July 14, 1998), https://www.wto.org/english/tratop_e/serv_e/w45.doc.

65. Stephen J. Ezell and Robert D. Atkinson, "False Promises: The Yawning Gap between China's WTO Commitments and Practices" (Information Technology and Innovation Foundation, September 2015), http://www2.itif.org/2015-false-promises-china.pdf.

66. United States Trade Representative, "2013 National Trade Estimate China" (Washington, DC: United States Trade Representative, 2014), https://ustr.gov/sites/default/files/2013%20NTE%20China%20Final.pdf; Hogan Lovells, "Third Party Payment Licences in China - Are They Within the Grasp of Foreign Investors?" (London: Hogan Lovells, June 2014), http://www.hoganlovells.com/files/Uploads/Documents/14.06_Corporate_China_Alert_-_Third_Party_Payment_Licences_in_China_-_Are_They_within_The_Grasp_of_Foreign_Investors_SHALIB01_1093411.pdf.

67. IBM, "Made in IBM Labs: IBM to Build First Cloud Computing Center in China," news release, February 1, 2008, http://www-03.ibm.com/press/us/en/pressrelease/23426.wss; Rebecca Blumenstein, "Microsoft's Partner Strategy in China," *The Wall Street Journal,* June 8, 2016, http://www.wsj.com/articles/microsofts-partner-strategy-in-china-1465421401; SAP, "SAP and China Telecom Expand Strategic Partnership to Provide SAP Cloud Portfolio in China," news release, November 20, 2013, http://news.sap.com/sap-and-china-telecom-expand-strategic-partnership-to-provide-sap-cloud-portfolio-in-china/.

68. Leigh Ann Ragland et al., "Red Cloud Rising: Cloud Computing in China" (Washington, DC: U.S. Economic and Security Commission, September 5, 2013), http://origin.www.uscc.gov/sites/default/files/Research/DGI_Red%20Cloud%20Rising_2014.pdf; United States Information Technology Office (USITO), "USITO Brief: Ministry of Science and Technology 12th Five Year Plan" (Washington, DC: USITO, August 5, 2011), http://www.semiconductors.org/clientuploads/directory/DocumentSIA/USITO%20Brief%20Ministry%20of%20Science%20and%20Technology%2012th%20Five%20Year%20Plan.pdf.

69. On March 31, 2016, the Indonesian Ministry of Communication and Information Technology issued Circular Letter Number 3 on "over-the-top (OTT)" services, which replicates the data localization requirement in Regulation 82/2012. Regulation 82/2012, in effect since 2012, includes requirements for source code surrender as a condition for market access and a requirement for local storage of data. In mid-2015 MICT released additional draft implementation measures, which contain more detailed requirements for protecting personal data on electronic systems, including requirements to store personal data in primary and backup data centers in Indonesia. Information Technology Industry Council, "ITI Forced Localization Strategy Briefs" (brief, Information Technology Industry Council, July 2016), https://www.itic.org/public-policy/ITIForcedLocalizationStrategyBriefs.pdf.

70. 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.

71. "New Rules on OTT Services in the Offing," Assegaf Hamzah and Partners, accessed December 19, 2016, http://www.ahp.co.id/client-update-27-may-2016.

72. Grace D. Amianti, "BI Working on Integrated National Payment System," *The Jakarta Post,* December 14, 2015, http://www.thejakartapost.com/news/2015/12/14/bi-working-integrated-national-payment-system.html.

73. Van Ly, "Ministry Protects OTT Services," *The Saigon Times Daily,* October 25, 2016, https://www.vietnambreakingnews.com/2016/10/ministry-protects-ott-services/.

74. Van Oanh, "OTT Users Likely to Be Forced to Pay Fee," *The Saigon Times Daily,* October 25, 2016, https://www.vietnambreakingnews.com/2016/10/ott-users-likely-to-be-forced-to-pay-fee/.

75. Nivell Rayda, "When It Comes to Innovation, Joko's Ministers Need a 'Mental Revolution,'" *Jakarta Globe*, December 18, 2015, http://jakartaglobe.id/opinion/commentary-comes-innovation-jokos-ministers-need-mental-revolution/.

76. "Indonesia Gives Netflix One Month to Get Permit, Office," *Jakarta Globe*, January 13, 2016, http://jakartaglobe.id/technology-features/indonesia-gives-netflix-one-month-get-permit-office/; Resty Woro Yuniar, "Netflix Blocked by Indonesia's Top Telecom Provider," *The Wall Street Journal,* January 27, 2016, http://www.wsj.com/articles/netflix-blocked-by-indonesias-top-telecom-provider-1453896220.

77. "Telkom to Bring Netflix Rival to Indonesia," *The Jakarta Post,* March 28, 2016, http://www.thejakartapost.com/news/2016/03/28/telkom-bring-netflix-rival-indonesia.html.

78. 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/.

79. "New Russian Legislation on Massive Telecoms Surveillance," *Jones Day Publications,* July 2016, http://www.jonesday.com/new-russian-legislation-on-massive-telecoms-surveillance-07-12-2016/.

80. Nigel Cory, "The Worst Innovation Mercantilist Policies of 2015" (Information Technology and Innovation Foundation, January 2016), http://www2.itif.org/2016-worst-innovation-mercantilists.pdf.

81. Laura Mills, "New Russian Data Laws Worry Rights Activists, Telecom Companies," *The Wall Street Journal,* July 7, 2016, http://www.wsj.com/articles/new-russian-data-laws-worry-rights-activists-telecom-companies-1467905452.

82. Ibid.

83. 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.

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

85. "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.

86. Ibid.

87. 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.

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

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

90. 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.

91. 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.

92. 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.

93. "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=.

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

95. "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.

96. 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.

97. 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.

98. "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/.

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

100. 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.

101. Ibid.

102. "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/.

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

104. 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.

105. Ibid.

106. Chander and Le, "Data Nationalism."

107. "EU Country Guide."

108. U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*.

109. 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/.

110. "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.

111. Ibid.

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

113. "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.

114. 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.

115. 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/.

116. 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.

117. 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/.

118. "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.

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

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

121. Ibid.

122. 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.

123. 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.

124. Chander and Le, "Data Nationalism."

125. 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.

126. 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.

127. 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.

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

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

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

131. 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.

132. "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/.

133. 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.

134. 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.

135. ITI, "ITI Forced Localization Strategy Briefs."

136. 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.

137. 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.

138. 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.

139. Chander and Le, "Data Nationalism."

140. Ravil Kassilgov, "Kazakhstan—Localization of Personal Data," *Lexology,* January 12, 2016, http://www.lexology.com/library/detail.aspx?g=303621d9-e5b7-4115-9d8c-2a5d1d40ed2c.

141. "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.

142. "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.

143. "Laws of Malaysia Act 709: Personal Data Protection Act" (Malaysia, 2010), http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf.

144. "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.

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

146. 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.

147. 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.

148. "Revenue Alert RA 10/02," Inland Revenue, December 10, 2010, http://www.ird.govt.nz/technical-tax/revenue-alerts/revenue-alert-ra1002.html.

149. 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/.

150. 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/.

151. "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.

152. 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.

153. 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/.

154. 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.

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

156. 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.

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

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

159. "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."

160. "EU Country Guide."

161. 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.

162. "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.

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

164. 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/.

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

166. "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.

167. '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.

168. 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.

169. 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.

170. 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.

171. Business Roundtable, "Promoting Economic Growth Through Information Technology Policy."