ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

The Cost of Data Localization Policies in Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam

NIGEL CORY, LUKE DASCOLI, AND IAN CLAY | DECEMEBR 2022

Restrictive data policies coming into effect in Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam will measurably increase import costs and reduce trade volumes, undermining the broader economic role of data. Policymakers should change course or else be left behind in the race for digital development.

KEY TAKEAWAYS

- Restricting data flows has a statistically significant impact on a country's economy—sharply reducing its total volume of trade and increasing import prices for downstream industries that increasingly rely on data.
- Data localization impacts the entire economy. ITIF's model shows that trade volumes decrease in line with imports. Since they are used as inputs in domestic production, higher import costs also reduce exports.
- ITIF has found that a one-unit increase in an industry's data restrictiveness is associated with a 0.5 percent decrease in the following year's trade—including a 0.6 percent decrease in imports and a 0.9 percent increase in import prices.
- After five years, restrictive data policies will reduce Bangladesh's volume of trade by 6 percent, Hong Kong's by 5.7 percent, Indonesia's by 5.8 percent, Pakistan's by 3.7 percent, and Vietnam's by 9 percent.
- Policymakers should avoid the false allure of trying to control data locally. They should instead focus on smart data governance policies, such as enabling digital development and adopting global standards for protecting public data.
- Smart data governance entails updating laws to address legitimate concerns—but in an open, targeted, and balanced way that doesn't undermine the enormous societal and economic benefits of data and digital technologies.

CONTENTS

INTRODUCTION

Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam each have different digital economies, yet they all stand at the same critical crossroad: either implementing core building blocks to support digital development and trade by allowing cross-border data flows or prioritizing control and protectionism by enacting restrictions that stop seamless data flows—a concept known as "data localization."[1] This choice lies at the heart of two contrasting visions—one looks outward to embrace the enormous opportunity of the global digital economy through cooperation and interoperable laws, while the other looks inward in a costly, misguided, and nationalistic pursuit of control and protectionism. Instead of the latter, policymakers should pursue a data governance framework that addresses legitimate public policy concerns—such as privacy, cybersecurity, and government access to data—in a smart and balanced way that does not fall prey to the false allure of data nationalism. While data localization may only be one part of the much broader, complex puzzle policymakers in these countries and territories face in getting their respective digital development plans right, it is a foundational one. Data flows will only become even more important as the global economy continues to digitalize, and whether countries recognize and embrace this central point as part of smart data governance will be both telling and consequential.

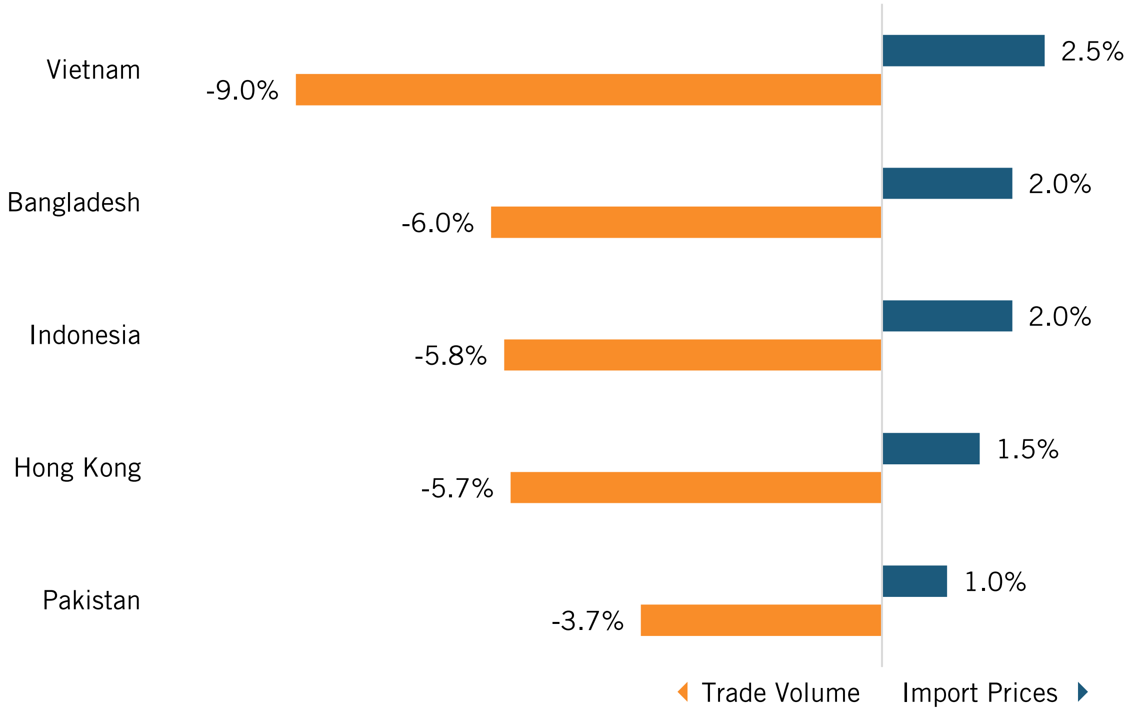
Data will flow across borders unless governments enact restrictions. While some countries allow data to flow easily around the world—recognizing that legal protections can accompany the data and that local and international laws and agreements help ensure firms provide governments with access to data for legitimate purposes—many have enacted new barriers to data transfers that make it more expensive and time consuming, if not illegal, to transfer data overseas. It's obviously fair and legitimate for these countries to enact or update laws and regulations to address privacy, cybersecurity, regulatory and financial oversight, law enforcement access to data, and other issues. But false and costly "data nationalism" policies not only do not address their stated aims—whether they're used in the name of privacy, cybersecurity, digital development, or regulatory oversight—but also impose broad and significant costs on national and regional economies. They are also counterproductive, as they preclude the much-needed international cooperation and legal agreements to address legitimate issues between countries as it relates to data. Unfortunately, many policymakers in the countries covered in this report have recently enacted, or are considering, laws and regulations that enact data localization practices.

Data localization is just one aspect of the digital development puzzle—and countries that embrace this misguided approach only set themselves back in the global digital economy.

The economic stakes are high. COVID-19 drove digital adoption in these countries, just as it did around the rest of the world. For example, a World Bank-Shopee survey of 15,000 digital merchants in Indonesia shows that 80 percent remained open when COVID first hit in 2020, 25 percent started their online business during COVID, and, on average, total sales rose to pre-pandemic levels around six months after the first peak of cases.[2] This is indicative of the impact of digital technologies and the opportunities for global connectivity. The absence of restrictions on data flows and the information and digital goods and services they deliver has played a role in helping each of these countries make the remarkable progress they've achieved in helping more people and businesses get online and benefit from data, digital technologies, and global connectivity.

The Information Technology and Innovation Foundation's (ITIF's) econometric modeling ranks proposed and enacted localization measures in Vietnam as the most restrictive, followed by Bangladesh, Indonesia, Hong Kong, and Pakistan. The model projects that data localization policies currently enacted or under consideration will reduce trade volumes and imports and increase import prices in all these countries and territories.

Figure 1: Projected change in import prices and trade volumes after five years due to restrictive data policies



These changes in both trade volume and the prices of key inputs involved in trade flows will inevitably impact both economic productivity and exports, as data-related goods and services are critical inputs. These results are consistent with a growing body of research from the Organization for Economic Development and Cooperation (OECD), the World Bank, academia, and other think tanks: Data localization and other restrictive digital policies undermine the growing impact data-intensive services and technologies have on economic productivity and innovation—and by extension, trade. As it reflects a central point for digital economic policy, an economy is most productive and innovative when individuals and firms can engage in digital activity and commerce without unnecessary restrictions on how they can use and transfer data.

Many policymakers focus on the location of data storage, in part, because addressing the underlying factors that actually address associated issues is more complex and challenging. For example, with data privacy, consumer protection, and law enforcement access to data for cross-border investigations, it's much harder to build the expertise and institutional capacity in government to properly address these concerns and enforce local laws. Likewise, with cybersecurity, it's challenging to build cybersecurity awareness among users and firms and encourage firms and government agencies to adopt and remain committed to best-in-class cybersecurity practices and services.

Enacting smart data governance frameworks and outcomes is challenging given the stakeholders and interests involved. People need to have confidence that their personal data is respected and protected. Government agencies need to know that they can access the data they need for legitimate purposes, such as consumer protection, financial oversight, and law enforcement investigations. Businesses need to know what they need in order to be accountable in collecting, protecting, and using both personal and nonpersonal data. This complexity is especially challenging for policymakers in developing countries who often lack the resources and expertise to help craft effective digital policies. However, there are many countries, development agencies, and other organizations to work with, and best practices, norms, and principles to learn from, to help countries build smart data governance policies.

This report highlights why localization policies in Bangladesh, Indonesia, Pakistan, Vietnam, and Hong Kong are both costly and misguided. It aims to help policymakers in these countries and territories recognize what's at stake in avoiding the pitfall that is data localization and how there are alternatives that address associated public policy concerns without unnecessarily incurring self-inflicted data localization costs. The first section of this report analyzes the central role of data and digital technologies in economic development and summarizes what's at stake in getting future digital policies right given the considerable progress each of the countries and territories has made in advancing their digital economies. The second section analyzes each country's misguided attraction to data localization, as while there are similarities, the prevailing motivations for data localization differ by country and territory. The third section provides a quantitative assessment as to the considerable economic impact of data localization in these countries and territories. The final section provides recommendations, while Appendix A includes a list of data localization policies and Appendix B provides details of the econometric methodology.

HOW DATA FLOWS AND DIGITAL TECHNOLOGIES DRIVE ECONOMIC GROWTH

No matter a country's level of development, data is critical to economic development. Access to affordable and high-quality information communication technologies (ICTs) is one of the modern economy's chief drivers of productivity, innovation, and economic growth. ICTs are such powerful tools precisely because they represent a general-purpose technology that enhances the productivity and innovative capacity of every individual, enterprise, and industry they touch throughout an economy. Policies that make ICTs more expensive, or simply cut off access to best-in-class ICTs, thereby introduce a broadly negative economic impact. This points to the central way ICT drives a country's economic growth, which is not through the production of ICT goods (i.e., the manufacturing of computers or smartphones or design of software). Rather, the vast majority of the economic benefits generated from ICT, especially in developing countries, stems from greater adoption of ICT across an economy.[3] As Richard Heeks, professor of development informatics at the University of Manchester, estimated, "ICTs will have contributed something like one-quarter of gross domestic product (GDP) growth in many developing countries during the first decade of the 21st century."[4]

The economic impact of ICTs only grows as global trade becomes increasingly digital. The Internet has not only removed the impact geography had on trade—in that, in traditional 20th century trade, firms from any of the countries in this study would've traded little, if at all, with customers from countries on the other side of the world—but the increasingly digital nature of trade makes it easier for firms and workers around the world to engage in services trade.[5] The unbundling of trade has made services an increasingly important component of economic activity, both as tradable "products" in and of themselves and as intermediate goods in the network of production and trade in goods and services.[6] The two interrelated trends—increased digitalization and increased unbundling of services—have created a global market for services tasks that has contributed to the tripling of services trade over the past 15 years, particularly for business services such as legal, advertising, consulting, and accounting.[7] From 2005 to 2019, global exports of digitally deliverable services grew at an average nominal rate of 12 percent per year and at a rate of as much as 21 percent in Asia. The share of digitally deliverable services in total global services exports had already increased from 45 percent in 2005 to 52 percent in 2019.[8] As the following section details, many of the countries and territories in this study are early beneficiaries of this digital evolution in trade and commerce.

WHAT'S AT STAKE FOR BANGLADESH, HONG KONG, INDONESIA, PAKISTAN, AND VIETNAM

Each of these countries and territories has made truly remarkable progress in helping more people and businesses get online and benefit from data, digital technologies, and global connectivity. Table 1 shows that while Bangladesh and Pakistan are at a similar level of digital development, Indonesia, Vietnam, and Hong Kong are at different levels. Whatever their similarities, local political, economic, legal, and social factors also mean they each face their own path ahead to further digital development. Obviously, a lot more remains to be accomplished in helping address the digital divide and other digital development issues in these countries and territories. However, it's important to highlight the progress they have made in the following summaries so as to recognize what's at stake in considering data localization and the need to not enact localization policies in order to get the next phase of digital policy right.

Table 1: Comparative global rankings in key indices of digital development[9]

Index	Bangladesh	Hong Kong	Indonesia	Pakistan	Vietnam
UNCTAD B2C E-commerce Index (152 economies)	115	10	83	116	63
ITU ICT Development Index (176 economies)	147	6	111	148	108
WEF Network Readiness Index (130 economies)	95	32	66	97	63

Bangladesh

Bangladesh's digital economy shows enormous promise. The government's "Digital Bangladesh" vision has set the foundation for its digital economy, along with subsequent initiatives and policies such as the A2I initiative, the National Digital Commerce Policy 2018, and the National ICT Policy 2019. The digital economy constitutes a significant national development opportunity for Bangladesh and a chance to diversify from traditional industries prevalent in the country.[10] The United Nations Conference on Trade and Development (UNCTAD) estimated that, since 2010, Bangladesh's ICT sector has grown at an astonishing average pace of 40 percent annually.[11]

Bangladesh has not only performed well at home but also globally in taking advantage of the digitalization of trade. Over the past 15 years, the average annual growth rate of IT and IT-enabled services exports was more than 15 percent against 13.6 percent growth in nominal GDP. There's enormous room to catch up. Bangladesh's services export-GDP ratio is just 1.5 percent, compared with around 40 percent in India, the Philippines, and Sri Lanka.[12] The domestic and export growth no doubt contributes to Bangladesh's efforts to attract considerable foreign direct investment (FDI) from Malaysia, the United States, India, and Norway. In 2019–2020, the ICT- and IT-enabled services sector attracted $758 million in FDI.[13]

Despite myriad development challenges, Bangladesh has performed remarkably well in taking advantage of digital commerce at home and globally.

Bangladesh possesses a fast-evolving e-commerce sector, driven by a flourishing ICT sector and a fast-growing middle income consumer base, which has become accustomed to using modern ICT services. For example, usage of Facebook for commerce (known as "f-commerce") is widely popular in Bangladesh. In 2017, the eCommerce Association of Bangladesh estimated that there were many more Bangladeshi e-commerce Facebook pages (7,000) than formal e-commerce websites (700). In many cases, these allow buyers and sellers to interact online but having to conclude transactions offline. This informal activity is estimated to be significantly larger than the number of formal e-commerce transactions.[14] All this progress is significant, but so are the remaining hurdles. A recent, thorough UNCTAD Rapid eTrade Readiness Assessment of Bangladesh points toward the need to improve telecommunication infrastructure, trade logistics, payment solutions, laws and regulations, and skills.[15]

Hong Kong

Hong Kong is different from the other countries in this report given its status as a special administrative region of China and the fact that it already has many enviable advantages—it has an advanced digital economy and society and is a central business hub for the Asia Pacific and mainland China. For example, over 95 percent of households have broadband Internet and own a smartphone; 86 percent of consumers use social media for an average of nearly two hours per day; and following credit cards, digital wallets are the second-most popular payment option (at 25 percent).[16] Hong Kong's success is due in no small part to the government's extensive, sophisticated digital policy plans.[17] Hong Kong's digital policy is also a critical component of China's development plans for the Guangdong-Hong Kong-Macau Greater Bay Area initiative and as a Digital Command Hub for China's Digital Belt and Road strategy. [18]

An emphasis in Hong Kong's 2022 budget is promoting innovation and technology development. In order to accelerate the progress of its digital economy, the government will set up a "Digital Economy Development Committee" in support of building Hong Kong into an international innovation and technology hub, which is a goal of China's 14th Five-Year Plan. Hong Kong's budget includes extensive plans and capital to build out its tech economy and expand the use of digital technologies such as artificial intelligence (AI), big data, blockchain, cloud computing, and cybersecurity.[19] Yet, as this report analyzes, the central challenge for Hong Kong is how to balance efforts to maintain its position as a digital-savvy tech hub with mainland China's growing efforts to exert a greater degree of control over the region's digital life and economy with vague and restrictive cybersecurity and national security laws.

Indonesia

Indonesia holds enormous promise in developing its large, dynamic, and tech-savvy domestic digital economy into a leading regional and global digital economy. President Joko Widodo clearly recognizes this potential and has stated his goal for Indonesia to become both a major market and a player in digital technologies at home and in the global digital economy.[20] In 2020, Indonesia's estimated e-commerce gross merchandise value was $32 billion, an increase of 54 percent from 2019.[21] One study estimates it could grow to reach $146 billion by 2025.[22] Again, as the other countries in this report, huge challenges—but also benefits—remain.[23] Nearly half of Indonesian adults are not connected to the Internet and there's a gulf across spatial, economic, and social dimensions.[24] In 2019, the proportion of Internet-using households that reported buying and selling online was 12.8 and 5.1 percent, respectively.[25] Indonesia's government is focused on addressing these issues. For example, the government of Indonesia, has launched the MSMEs (micro, small-, and medium-sized enterprises) Go Online program, which provides capacity-building to expedite digitization.

Pakistan

Digital development has already proven enormously beneficial to Pakistan.[26] The country produces more than 20,000 IT graduates annually, has seen over 700 tech start-ups launched since 2010, and has the fourth-highest-earning information technology (IT) workforce in the world.[27] Pakistan's technology sector represents a large and fast-growing exporter, with annual revenue from exports of IT and IT-enabled services accounting for $1.4 billion in 2020 (having grown at 10.8 percent per year since 2010).[28] Much of this is based on surging Internet connectivity, particularly via smartphones, penetration of which has increased from approximately 6 million in April 2014 to nearly 80 million by December 2019.[29] Obviously, Pakistan still has many challenges to address in order to extract economic and societal benefits from data and digital technologies. There's a growing digital divide, in part due to relatively high Internet costs.[30] Digital literacy is limited, and digital adoption by the government is lower than that of its regional neighbors. Pakistan's government, development agencies, and private sector have introduced strategies, investments, and policies to support and expand the impact of digital technologies, such as via the Digital Pakistan Policy, the Pakistan Software Export Board's software technology parks, and the World Bank's digital connectivity program.

Vietnam

Vietnam holds enormous potential to leverage data and digital tools to bolster its growing and dynamic consumer digital market alongside its role as a central part of global production networks.[31] Data and digital services will be critical to Vietnam's efforts to move from low-tech manufacturing to a higher-value-added manufacturer and service-oriented economy. The potential is clearly there. Vietnam's digital economy has grown 16 percent from 2019 to $14 billion, which places it among the biggest digital markers in Southeast Asia.[32] Vietnam is playing a growing role in high-tech production, with high-tech goods as a share of exports hitting 42 percent in 2020, up from 13 percent in 2010.[33] In particular, Vietnam has the opportunity to capitalize on firms looking for an alternative to China given that nation's trade dispute with the United States and restrictive approach to data governance and cross-border data flows.[34]

To its credit, Vietnam recognizes the need to build digital connectivity with its trading partners, such as via the data and e-commerce provisions in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) trade agreement. Vietnam has also enacted a series of thoughtful strategic plans and policies to support digital development, including its National Digital Transformation Plan and ongoing efforts to design a National Strategy on the Digital Economy and Society. It is also engaged, sometimes in a leadership role, in building digital governance with its Association of South East Asian Nations (ASEAN) and Asia-Pacific Economic Cooperation (APEC) partners, such as via the APEC Da Nang Declaration and the ASEAN Digital Masterplan 2025.[35] There are many issues Vietnam needs to address to develop digitally, such as issues with skilled labor, good and secure access to information, and efforts to promote e-learning, e-payments, and e-government.[36] But this hasn't stopped Vietnam from considering potential broad and harmful data localization policies. While data flows represent just one aspect of these plans and Vietnam's digital economy, it is a key one, especially given the country's development goals and reliance on global trade, investment, and connectivity.

Case Study: Global Gig Work and Services Exports in Bangladesh, Indonesia, Pakistan, and Vietnam

Bangladesh, Indonesia, Pakistan, and Vietnam are playing a growing role in global services exports. For example, Bangladesh is the world's second-largest source of online labor (after India), accounting for about 15 percent of global Internet workers.[37] It has a growing freelancer sector with a half-million people actively participating in the global gig economy. According to Bangladesh's ICT minister, its online workers earn around $500 million every year.[38]

Meanwhile, Pakistan currently is the fourth-largest provider of workers to online freelancing platforms globally.[39] Oxford's Online Labour Index 2020 provides a broader picture as it tracks all the projects/tasks posted on the five largest English-language online labor platforms, representing at least 70 percent of the market by traffic. It shows that Bangladesh is home to the 2nd-largest group of global gig workers (15 percent), followed by Pakistan in 3rd (12 percent), with Indonesia in 12th (1.4 percent).[40]

Most gig workers in Bangladesh and Indonesia are involved in creative and multimedia work, while most in Pakistan and Vietnam are involved in software development and tech service work.[41] International gig work opens up opportunities for more women to get involved, and overall pays better than do other sectors.[42] The geographic spread of these jobs across nations also highlights how countries are competing to have as many of these workers as possible and how policies that make this harder and more expensive will inevitably lose out.

HOW EACH COUNTRY SUCCUMBS TO THE ALLURE OF DATA LOCALIZATION

Policymakers in Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam have used a variety of misguided motivations in considering and enacting data localization policies. Appendix A provides a detailed list of all their enacted and proposed data localization measures. The following section provides analytical context for these measures. While there are similarities, they also differ in some important ways. This analysis points to the constructive alternatives (as detailed in the recommendations) to data localization that are available to each country in an effort to help them shape smart data governance policies.

Bangladesh: Buying Into All of Data Localization's False Promises

Bangladesh is learning many of the worst lessons from its neighbors in China (and also India) when it comes to enacting restrictions on data transfers for misguided data privacy, cybersecurity, law enforcement, and national security reasons.[43] This is clearly evident in its draft data protection act and national cloud policy.[44] Bangladesh's draft data protection act is misguided not only due to its data localization measures, but also because it conflates privacy and content moderation in a way no other countries do in not only forcing firms to store sensitive data locally but also the broad (and practically infeasible) category of user-created or generated data.[45] It's a particularly dangerous and costly path for Bangladesh (as compared with India and China, never mind Indonesia and Vietnam) to follow, as while it is a promising emerging digital market, it is relatively small and thus most likely to result in firms avoiding, withdrawing, or downgrading services and market operations in the face of uncertain, onerous, and costly digital restrictions.

Key Bangladeshi policymakers prioritize state control over data, data flows, and digital technologies over other associated economic, social, and legal interests. By control of data, what they tend to mean is an idealized, but ultimately unrealistic, ability to have unfettered access to it.[46] They hope such policies will help Bangladesh take back control and provide sovereignty from foreign technology firms and governments and force them and foreign governments (namely, the United States) to force firms to hand over data. This is part of both Bangladesh's draft data protection bill and cloud strategy.[47] Beyond local security and political concerns, geopolitical risk is also a factor in Bangladesh. In 2021, U.S. human rights sanctions against the government's "Rapid Reaction Battalion" led to an upswell of nationalism and protectionism that included support for localization.[48]

Bangladesh is learning all the worst lessons from China regarding data localization and digital control.

Bangladeshi policymakers focus on the location of data storage instead of the legal and institutional structure and processes that facilitate legitimate, efficient, and legal access (both domestically and internationally). Bangladeshi authorities are frustrated that U.S. companies—like all firms from rule-of-law countries—manage requests for data from governments according to laws in their home country and as specified under legal agreements between countries (e.g., Mutual Legal Assistance Treaties (MLATs)). If requests from Bangladesh don't meet set legal criteria, firms can't provide access to data. This is made that much harder, as there isn't a U.S.-Bangladesh MLAT. It's fair to criticize MLATs and other traditional mechanisms for law enforcement data exchanges as outdated, slow, and frustrating, but this is why this should be the focal point for action. Localization is not the silver bullet some policymakers think it is. Firms don't manage user data by some name-by-name traditional filing system. Any one user or activity will likely involve multiple intermediaries, people, and jurisdictions. The digitalization of crime means law enforcement needs for cross-border cooperation will only increase. Hence the need for updated legal tools.

Bangladeshi policymakers also try to justify localization as necessary to protect commercial and government data. They believe data is more private and secure when it is stored within a country's borders. However, in most instances, data-localization mandates increase neither commercial privacy nor data security.[49] Companies doing business in a nation—all domestic companies and most foreign—have "legal nexus," which puts the company in that country's jurisdiction. For example, a global bank or manufacturer that has branches or plants in a nation is subject to that nation's privacy and security laws and regulations. Companies simply cannot escape from complying with a nation's laws by transferring data overseas. Wherever there are cross-border jurisdictional issues (as all firms that manage data from multiple countries manage multijurisdictional issues and tend to apply a single approach to all), again, the focus needs to be on the tools and capabilities and how to use them effectively.

As much as it relates to cybersecurity and surveillance, policymakers misunderstand that the confidentiality of data does not generally depend on which country the information is stored in, but rather only on the measures used to store it securely. A secure server in Bangladesh is no different from a secure server in Malaysia. 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 sensitive government data and services, governments can specify in their procurement contracts that providers must use the latest cybersecurity standards and encryption, or other advanced protective measures.

Policymakers focusing on geography to solve privacy and cybersecurity concerns are missing the point. Consumers and business can rely on contracts or laws to limit voluntary disclosures to ensure that data stored abroad receives the same level of protection as data stored at home. In the case of inadvertent disclosures of data (e.g., security breaches), to the extent nations have security laws and regulations, again a company operating in the nation is subject to those laws, regardless of where the data are stored. Moreover, security breaches can happen no matter where data is stored—data centers everywhere are exposed to similar risks. 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 cyberattacks. The location of these systems has no effect on security.

Bangladesh's policymakers fail to recognize that foreign cloud and digital service providers only deploy data centers sparingly and that it simply doesn't make sense to deploy IT systems in each and every market. Never mind the fact that the location of data and data centers does not lead to digital development. Some policymakers in Bangladesh focus on data centers, in part, because they are misguidedly attracted to a data localization-based digital sovereignty, as they mistakenly think "data is the new oil." While it is certainly true that data has become invaluable, the oil analogy is fundamentally flawed (see the Recommendations section of this report).[50] Policymakers should understand how data is transforming the economy, but looking to oil as a historical example is not productive.

Hong Kong: Openness Threatened by Mainland China's Drive for Control

Hong Kong's government is under pressure from mainland China (the world leader in data localization and digital control) to enact restrictions on data flows in the name of "cybersecurity."[51] This is in addition to other new laws that impact data and digital content, especially its National Security Law. The problem is that China equates cybersecurity with national security, and national security with regime security. This is a profoundly different conceptualization of cybersecurity and national security from that of most countries.

Hong Kong's government is cognizant of the risk localization poses to its position as a regional and global business hub—which is already under threat from other legal and political issues created by China—and has therefore been considering far narrower data localization requirements (as compared with the broad impact mainland China's cybersecurity law has on data transfers). Whether a narrow approach to localization will satisfy Beijing is a major question. Hong Kong has been talking with certain foreign firms (namely, firms that operate on the mainland and are therefore familiar with its localization requirements) about this new cybersecurity proposal.

However, it's a fundamental misreading of the situation if Hong Kong thinks narrow localization will not send another troubling signal to global businesses. This should be clear given the reaction to the National Security Law, which caused many large tech firms to draw down operations in Hong Kong and shift future expansion to other countries.[52] But it's not just the National Security Law and cybersecurity law. For example, the Cyberspace Administration of China is enacting regulations that would make mainland companies seeking initial public offerings in Hong Kong subject to a cybersecurity review on national security grounds. It is the first time the government said such reviews would apply to listings in the city.[53]

Beijing's fears of political control are pushing Hong Kong to consider data localization for supposed "cybersecurity-related" reasons.

Hong Kong's new National Security Law is the clearest example of Hong Kong's shift to greater digital restrictions.[54] Until recently, Hong Kong's Internet had been uncensored and unrestricted. One example of this is people in Hong Kong have long been able to access services and apps blocked in the mainland, such as Facebook and Google. The National Security Law moves its Internet within China's censorship and government access apparatus. China wants to use the National Security Law and a new cybersecurity law to ensure it retains the legal and technical capability to intervene, access, and control data and digital content and communications. In 2019, Hong Kong's government made just over 5,500 requests for user data and 4,400 requests for removal of content.[55] However, this likely doesn't capture the full extent of such requests, as investigations into national security crimes can be deemed a state secret, with any trials potentially heard in closed court and tech companies being forbidden from disclosing what the police ask them for.

One major concern about Hong Kong's new National Security Law is it targets content removal and access to data on a potentially global basis. While it's impossible to know how China uses this new law (Macau has had a similar law in place for over a decade and there have been no reported enforcement cases), there's the potential to see how articles 38 and 43 could be used in this way, as they apply to offenses committed outside Hong Kong and allow authorities to ask the publisher, platform, host, or network service provider to remove or restrict access to the data or produce information about a user.[56] The threat of vague, broad, extraterritorial requests for data will likely force firms to either localize data to ensure they're in compliance (and thus avoid punishment in Hong Kong, on the mainland, or both) or to simply withdraw, downgrade services to avoid or minimize the potential for major legal and compliance risks in other markets, or both.

Indonesia: Simultaneously Taking Steps Forward and Backward

Despite its enormous digital promise—or perhaps due to it—Indonesia's digital policy debates often feature data localization proposals. Indonesia has enacted localization measures for public sector entities and banking and nonbank financial institutions; however, to its credit, the country has also removed or reduced potentially broad localization requirements, such as in its new data protection law, in rules for public and private systems operators, and in relation to payments data.[57] The battle to ensure Indonesia adopts further smart data governance policies that support its evolution into an integral part of the global digital economy is far from over. For example, there are fears that Indonesia's data and digital policies will backslide after being the G20 host in 2022, including as part of implementing regulations for its data protection law and in consideration of enacting duties on digital transmissions.

Indonesia's motivations for considering data localization vary, but a central one is that it represents the latest iteration of the country's historical attraction to state-directed, protectionist industrial policy. Many Indonesian policymakers look to China as their model, thinking they too can use their large domestic market and digital protectionism to support locally owned (and often state-owned) operators in its data center, cloud, payment, and e-commerce sectors.[58] For example, Indonesia's central bank tried (though it eventually backed down) to use localization to favor locally owned payment operators.[59] Indonesian data center operators also publicly supported localization and opposed efforts to remove localization requirements.[60]

It is not too late for Indonesia to enact smart data governance policies to become a leading global digital economy.

Data localization is also featured in debates over cybersecurity and government access to data, including due to concerns about law enforcement access to data held in other countries, such as Singapore. Likewise financial regulatory authorities have used localization due to concerns regarding access to data for regulatory oversight. For example, Indonesia's Financial Services Authority (OJK) mandates that banks and nonbank financial institutions have data and disaster recovery centers in Indonesia, though some data transfer exceptions apply.[61] Certain Indonesian policymakers also consider localization as part of a misguided effort to improve the data security and privacy of sensitive government data and services, including from foreign government surveillance (e.g., from China).[62]

Pakistan: Broad Political and Security Concerns Fuel a Drive to Control Data

Similar to Bangladesh, Pakistan is taking all the wrong lessons from India, China, and Russia in considering restrictive data laws and regulations for misguided, and very costly, national security and digital protectionist purposes. Pakistan has enacted several laws and regulations that explicitly and indirectly restrict the movement of data, such as the Prevention of Electronic Crimes Act (PECA, commonly known as the Cyber Crimes Law) and its draft Personal Data

Protection Bill.[63] The impact on domestic and foreign firms will be significant, especially as these laws significantly increase the potential legal risks for firms managing personal data. For example, as appendix A details, PECA goes beyond traditional cybercrimes and criminalizes certain online speech and gives authorities unchecked powers to curtail and prosecute it. Similar to Bangladesh, the misleading appeal of China's digital control to Pakistan's policymakers will entail much clearer and greater costs in the latter, as Pakistan simply doesn't make sense for firms to set up expensive and duplicative IT systems in such a promising, but highly problematic, digital market.

Pakistan's primary motivation for data localization is national security—namely, its intelligence services want immediate and unrestricted access to data for political, social, and security reasons. Pakistan clearly prioritizes security and political interests over economic and trade interests, as well as human rights concerns. Pakistani policymakers can certainly make that trade-off, but they should be aware of the large economic and trade costs involved. Pakistan's policymakers also obviously do not want to make this trade-off clear as they try to avoid or minimize debate and scrutiny over their digital and data policies.[64] Pakistan's commitment to data localization is clear, as it considered and enacted amendments to PECA in 2021 but kept the problematic provisions, including data localization and the need for foreign firms to set up a local office and have local staff based in the country (in order to hold them personally liable for the firms' compliance).[65]

Pakistan uses localization as a cudgel to force firms to access user data, store data locally, and remove a broad range of digital content. Indicative of this, in relation to PECA, a Pakistani military spokesman boasted in a press conference that the intelligence agencies were able to look into individual social media accounts, thus implying dire consequences—including many years in jail—for posting dissent online.[66] For example, a case under Section 20 of PECA was lodged against a political activist in Lahore accused of propaganda.[67] PECA is particularly problematic due to the lack of legal safeguards and oversight. The rules allow a broad range of state agencies to make confidential requests for content removal through the Pakistan Telecommunication Authority (PTA), without any visibility regarding the source of the complaint. PTA is also responsible for hearing reviews and appeals against its own decisions.[68]

Pakistan clearly prioritizes the use of data localization for supposed national security reasons over associated economic, trade, and human rights interests.

Mixed into these security motivations are misguided privacy, cybersecurity, and digital protectionism goals—but these are definitely secondary. For example, in Pakistan's Draft E-Commerce Policy, it states that "home to the world's 6th largest population, data generated in Pakistan is a very valuable asset due to its huge size and there is a dire need to ensure that all the data generated in Pakistan is stored and processed in Pakistan as it is primarily ownership of the citizens to whom it relates."[69] Similarly, it reveals that "ownership of data is determined by location of the data centers where data is stored."[70] As this report shows, focusing on the limited investment and few jobs that go into local data centers over the broader economy's growing use of data and digital services is a very costly trade-off. Such misguided data nationalism will only hold Pakistan back, as what matters is having the education, skills, infrastructure, and regulatory environment to help individuals and firms actually use data—regardless of where it's stored, as what actually matters is cloud access and skills—to use data to actually create economic value.[71]

Vietnam: Trying to Balance Digital Openness and Strict China-Like Controls

Vietnam is unique in its use of data localization. Like the Chinese Communist Party, the Communist Party of Vietnam sees localization as a critical tool to assert political control. Yet, it is different, as its efforts to move its manufacturing and services sectors up the value chain economically and via trade agreements means it can ill afford restricting the movement of data. Vietnam has data localization requirements for personal, payments, and a broad range of data managed by social networks, search engines, and other digital firms. Vietnam is also unique in that it faces the real prospect of a trade law challenge (via e-commerce provisions in the CPTPP) if it doesn't allow the free flow of data.[72] Until Vietnam realizes that it needs a smart data governance strategy that addresses legitimate data privacy, protection, and cybersecurity concerns while allowing data to flow freely, it'll never fully realize its full digital potential.

Vietnam uses privacy and data protection concerns to justify localization, and while its laws address many legitimate parts of these issues, it's clear that at the heart of these policies are political and social interests around controlling certain data and digital content.[73] Its institutional arrangements show this; Vietnam's data protection agency is the Ministry of Public Security (MPS), while in most other countries, there's an independent, specialized data protection agency. Vietnam's Law on Cybersecurity (LOC), and its various implementing regulations (namely, Decree 53), gives MPS the authority to request firms to store data locally and set up a local office if they're judged to not be cooperating with government requests for data and to remove content in a timely manner.[74] It's just a matter of time to see how extensively MPS uses this authority, and thus how broad the localization requirement will be. Vietnam has also considered an onerous personal data transfer assessment and notification scheme.[75] The country has a de facto localization requirement for payments data, along with other restrictions, to support a state-owned payments firm.[76]

Vietnam wants to attract data-intensive manufacturing and service firms to upgrade its economy, yet it is enacting data localization requirements that undermine this goal.

The main targets of Vietnam's restrictive data regime are broadly used digital services such as search and social networks, given their role in facilitating social and political discussions. Unlike China with its "Great Firewall," Vietnam allows foreign social media and search firms to operate, although authorities are making these firms' operations increasingly difficult via vague and potentially onerous localization and content moderation requirements, such as broad and urgent requests to verify users, remove a broad range of content, and suspend user accounts. Due to the impact on privacy, free speech, and other rights, Human Rights Watch and Amnesty International have both condemned Vietnam's Cybersecurity Law.[77]

Similar to China, Vietnam has tied cybercrime and cybersecurity policies (which address legitimate issues) to social and political goals.[78] For example, article 4 of Vietnam's cybersecurity law designates that "the principle of protecting cyber security [is] under the leadership of Vietnam's Communist Party."[79] Article 8 and 15 prohibit "the use of cyberspace [to] prepare, post, and spread information [that] has the content of propaganda opposing the State of the

Socialist Republic of Vietnam," or "offends the nation, the national flag, the national emblem, the national anthem, great people, leaders, notable people, and national heroes." As it relates to traditional nation-state cybersecurity threats, Vietnam is unique in that while it was inspired by China's cybersecurity law, the country adopted the law in no small part to defend itself against China-backed and -based cyberattacks.[80]

Vietnam will struggle to have it all in terms of being an attractive country for high-tech and digitally intensive manufacturing and services while enacting potential broad, vague, and restrictive restrictions on the flow of data, the digital services they support, and the management of digital content. Removing or severely degrading social and search firms and their services will not only send a clear signal that Vietnam is not truly committed to playing a role in global production networks and the global digital economy, but inevitably impact these and associated digital services used in everyday business for data analytics, communication, marketing, advertising, and support services. Potentially severe criminal and financial penalties (including holding firms' representatives personally responsible) will cause social, search, and other firms that manage digital content and services to reconsider their operations, selectively engage, or simply not operate there at all. If Google, Facebook, and other large firms struggle to operate in Vietnam, smaller firms that manage some of the same data and content don't stand much of a chance.[81] It'll lead to fewer foreign firms and digital goods and services in Vietnam, which will inevitably negatively impact Vietnam's economy.

PREVIOUS RESEARCH ON THE CONSEQUENCES OF DATA LOCALIZATION

The spread of data localization policies in Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam will negatively impact their domestic digital economies. It would also add to the growing threat that localization and other digital barriers pose to the potential for an open, rules-based, and innovative global digital economy. Ultimately, data localization makes the Internet less accessible and secure, more costly and complicated, and less innovative.

Developing an econometric model for the impact of data localization on these countries and territories was challenging, but ultimately worthwhile, in that it shows clear and convincing results about the negative economic and trade impact of data localization. In particular, it was challenging due to the simple fact that not all these countries are included in major trade and economic databases used for this type of econometric modelling. For example, OECD's Services Trade Restrictiveness Index (STRI) database covers only a small number of emerging countries, while the World Bank STRI data is only available periodically, with the latest STRI covering 2016 policies released in early 2020.[82] There is ongoing work to extend coverage and analysis, including via Hoekman and Shephard's "Services Policy Index," which extends the OECD STRI to countries included in the World Trade Organization's (WTO's) Integrated Trade Intelligence Portal (I-TIP), but not in the OECD database.[83]

This report contributes to a growing body of research with similar results showing that data localization and other restrictive digital policies undermine the growing impact data-intensive services have on economic productivity and innovation, and by extension, trade.[84] At the country level, in 2014, the European Center for International Political Economy (ECIPE) estimated that economy-wide data localization and other administrative barriers in Indonesia and Vietnam would decrease GDP by 0.7 percent and 1.7 percent and domestic and FDI by 2.3 percent and 3.1 percent, respectively.[85] More recently, in 2022, Research and Policy Integration for Development

(RAPID) in Bangladesh performed an interesting study on the economic impact if Bangladesh enacted localization requirements similar to India and Vietnam. In these two scenarios, it estimated that this would decrease digital services exports by from 29 to 44 percent and decrease GDP by 0.6 to 0.9 percent. If its trading partners retaliated in kind, digital service exports would decrease 32 to 37 percent and decrease GDP by 0.76 to 0.9 percent.[86]

Broader economic and trade studies support these country-level results, as restrictive data and digital trade policies negatively impact firms using services as inputs, reduce the competitiveness of services exporters, and increase prices, lower the quality of services available to households, or both. ITIF's past econometric analysis (2021) of data localization's general impact estimates that a one-unit increase in a country's data restrictiveness index (DRI) results (cumulatively, over a five-year period) in a 7 percent decrease in its volume of gross output traded, a 1.5 percent increase in its prices of goods and services among downstream industries, and a 2.9 percent decrease in its economy-wide productivity.[87]

The World Bank's 2020 World Development Report finds that "restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies... Countries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies, whereas the benefits of reducing data restrictions on trade in services would on average be about 5 percent."[88] Conversely, in terms of associated digital openness, a 2018 OECD report notes that digitalization is linked with greater trade openness, selling more products to more markets, and that a 10 percent increase in bilateral digital connectivity increases trade in services by over 3.1 percent.[89] While any indicator of services trade restrictiveness should be a strong predictor of bilateral services trade, other recent research shows that because of the input–output relationships that exist between services and other sectors, it's also likely that services policies affect total trade (i.e., goods and services).[90] Converting Shephard and Hoekman's "Services Policy Index" to an ad valorem equivalent (i.e., a percentage of the price) shows that services policies are typically much more restrictive than tariffs on imports of goods, in particular in professional services and telecommunications sectors. However, while their model includes Bangladesh, Pakistan, and Vietnam, results are aggregated and not broken down by country.

HOW ITIF MODELED THE ECONOMIC COSTS FOR THE COUNTRIES IN THIS STUDY

This section details ITIF's econometric analysis of the impact data localization would have specifically on Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam. Appendix A includes a full list of data localization policies; appendix B includes details about the model's methodology.

To estimate the economic impact data localization has on data-reliant industries, ITIF designed a model to observe empirical changes in economic indicators of a country's industries due to the enforcement of added data restrictions. This section provides a quantitative analysis of the effects of restrictions given the relationship between data flows and economic performance.

While econometric analysis only provides an indicative estimate of the economic impact (given challenges with measurement and data availability), it is still important to do so to reinforce for policymakers the economic and trade costs of restricting data flows.

ITIF's analysis is unique because it covers a larger sample of countries not covered in past models, utilizes a longer panel dataset than found in other literature, and compares both trade volumes and trade costs as response variables. Further, the index in this model differs from other analyses in that its index's calculation is most precisely a function of data localization policies (both explicit and indirect) rather than a function of digital regulations. This methodology should give an accurate assessment of the relationship between economic performance and data localization, since the index encompasses far fewer confounding factors that could add error/statistical noise during econometric analysis.

The structure of ITIF's quantitative study in this report follows the same core analysis conducted in its 2021 report on data localization, whereby a composite index—the data restrictiveness linkage (DRL)—measuring the linkage of a country's data restrictions to its industries (based on data intensity) is regressed among a set of variables related to volume of trade, consumer prices, and productivity.[91] However, measurements scoring a country's data flow restrictiveness come from ITIF's own calculation methodology, rather than through the use of a proxy variable. This report also expands on ITIF's previous work by conducting data analysis on a sample size inclusive of a wider range of non-OECD economies in Asia. The model conducts an ordinary least-squares regression on separate models that take log transformations of trade volumes, imports, unit import values, and nontariff trade costs on DRL, and then analyzes coefficient estimates in order to assess the changes associated with an increase in data localization measures. These statistical findings are then applied to Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam.

Data Restrictiveness Index

This report's focus on non-OECD Asian economies means ITIF was not able to use datasets (related to data restrictiveness) as used in past and related models.[92] Instead, ITIF calculates its own data restrictiveness index that measures the weighted running total of a country's data localization measures up to a given year. Given that not all data localization measures are equally impactful to the economy, a data localization measure is weighted in its count toward DRI based on its directness, d, and the kind of data it restricts, $k.$ Therefore, the data restriction of policy j is defined as

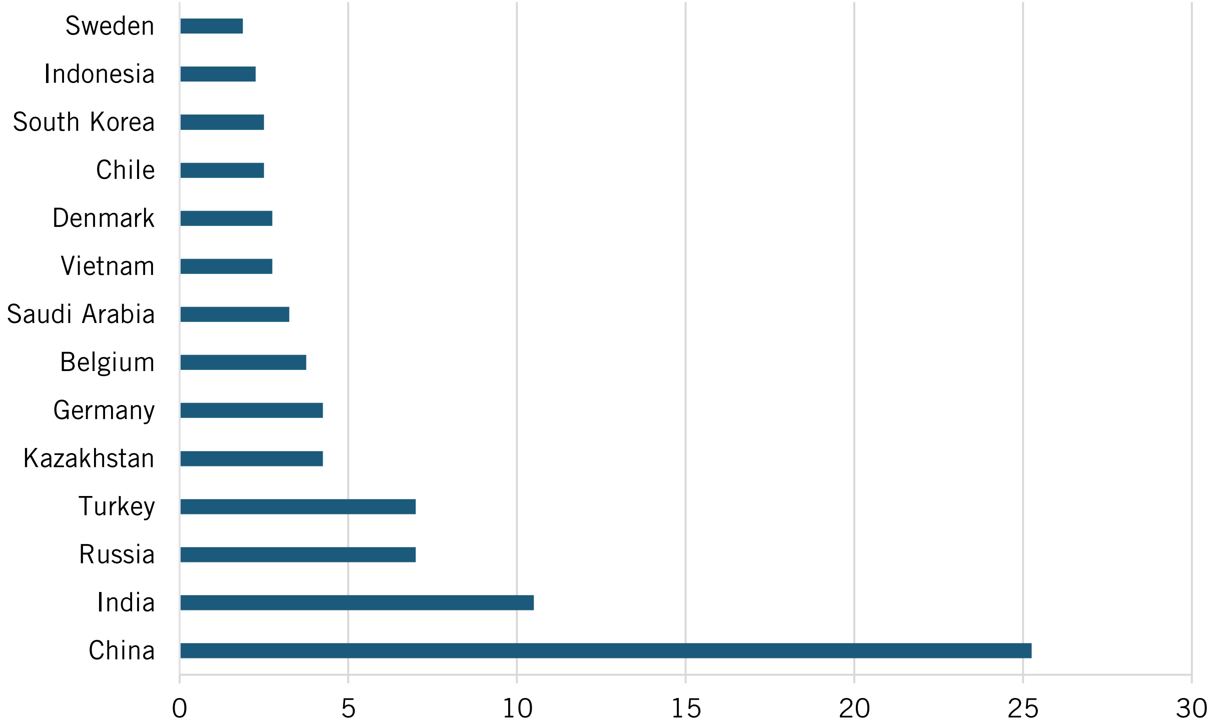
$$data\ restriction_j = d_j * k_j$$

See table 4 in appendix B for the possible values for d and k. A data restriction is scaled higher based on how direct it is and how important the restricted data is to the economy. A higher value assigned to a given data restriction imparts that that data restriction carries greater severity. Therefore, a country's DRI score in a given year is the sum of the data restrictions of its policies in place in that year—that is, if a country c has n data restriction policies in place in year t, its DRI is calculated as:

$$DRI_{c,t} = \sum_{j=1}^{n} data\ restriction_{j,c,t}$$

The primary data source utilized to tabulate a country's data restriction by year of enactment, its directness, and its kinds of data affected is in "Appendix A: List of Data Localization Measures" of Cory and Dascoli 2021.[93] A higher DRI reflects a higher degree of data restrictiveness enforced by a country. Figure 2 shows the most-restrictive economies by way of cross-border data transfers, based on DRI scores for 2020. Following this methodology, data on 64 economies is recorded using data localization measures passed between 1989 and 2020.

Figure 2: Countries with the highest scores in ITIF's data-restrictiveness index, 2020[94]



Data Intensity Modifier

While data is increasingly important to all industries, not all industries are equally reliant on data. For example, firms in finance utilize data far more than do firms in agriculture or home health care. This model assumes that industries more reliant on data are therefore more impacted by the restrictive effects of data localization than are industries with less reliance on data. Therefore, ITIF calculates a data intensity modifier (DIM) to control for differences in an industry's reliance on data. Like ITIF's prior study, and other related studies, data intensity is approximated by measuring the software usage per worker in each U.S. industry. The model further controls for endogeneity by using the base year 2013 to calculate DIM, as opposed to calculating country- and year-specific DIMs. This control, however, assumes equal technology among countries and over time. Data for intangible software expenditure per industry is taken as noncapitalized software expenditures listed in the 2013 U.S. Census Information and Communication Technology Survey.[95] This data is divided by the number of workers in each corresponding industry as provided by the U.S. Bureau of Labor Statistics (BLS) for the same reference year of 2013.[96] DIM is taken as a natural log to align with previous literature on factor intensity. That is, the DIM of industry i is calculated as

$$DIM_i = \ln\left(\frac{Noncapitalized\ software\ expenditure_i}{Employment_i}\right)$$

Figure 3 in appendix B shows the distribution of DIM ratios among 23 different aggregate industries.

Because this report is concerned with country-level figures for the five countries of interest, country-level DRLs are needed. Moreover, because this report calculates the country-level effect on trade volumes and imports separately, country-level DRLs for total trade *and* imports are needed.[97] This requires computing country-level DIMs for both total trade and imports. To do this, ITIF takes the weighted average of the industries' individual DIMs where weights are industries' share of total trade or imports (depending on which country-level DIM is being calculated) per WTO Stat data. The equation for calculating the DIM of country c is therefore:

$$DIM_c = \sum_{i=1}^{23} \omega_{c,i} DIM_i$$

where $\omega_{c,i}$ is industry i's share of total trade or imports in country c. A higher DIM—and therefore DRL—of imports than of total traded goods and services implies that, in aggregate, the country's imports are from sectors that are more data reliant than its exports. Country-level DRLs therefore allow for some variation in the effects data localization policies have on total trade and import-based sector composition. Appendix B provides a list of each of the five countries' total-trade and import DIM scores.

Data Restrictiveness Linkage

Data-intensive industries should be noted as being more susceptible to changes in data localization than are non-data-intensive industries. Therefore, this model provides a score of data restrictiveness for a given industry within a country by linking DRI values with DIM ratios. ITIF draws this linkage as the product of DRI for a given country and year with the DIM for a given industry in order to calculate the DRL for that country's given industry. Thus, the formula for the DRL of a given industry i in country c and year t is given as

$$DRL_{c,t,i} = DRI_{c,t} * DIM_i$$

DRL serves as a composite index of data localization at the level of country-year-industry. This composite index allows for more precise econometric analysis on the impact of data localization by allowing industry-level comparisons. In this final index, the sample size includes 57 unique countries, 23 unique industries, and observations between 2005 and 2020. The tables providing the full list of countries and industries can be found in Appendix B.

Econometric Modeling

The composite index DRL is tested in separate regression models against response variables indicating trade, while the DRI is tested against a response variable capturing the price of imports and nontariff trade costs (as data for these response variables is not available at the industry level). Given how integral data storage, transfers, and analytics have become in several areas of the economy, ITIF predicts that increased restrictions on the flows of data will suppress trade volumes, since those restrictions limit the use of data to facilitate economic activity and thus trade activity. Data localization, by way of limiting a firm's access to using data to add value, also prevents foreign firms from entering new markets, making their business operations less productive and potentially unviable. This would imply that not only does data localization have a negative impact on productivity and growth, but it also restricts a country's ability to increase transactions from leading firms and thus decreases the competition less-productive domestic firms face. Data localization's suppression of competition may also likely have continued negative effects on productivity because domestic firms, in their now-favored position, will have less incentive to innovate. For foreign firms still trying to provide competition in domestic markets employing data localization measures, the cost of compliance and loss of access to more-efficient business processes would likely increase their costs of facilitating trade, leading to increased prices for their imports. Therefore, four separate econometric models are designed to regress variables of trade volumes, imports, import unit values, and nontariff trade costs against ITIF's own country-year indicator on data localization DRI and country-industry-year indicator DRL.

Because the impacts of data localization policies likely take some time to affect economic decisions, each regression employs a one-year time lag such that DRI or DRL in one year is used to predict the relevant economic indicator in the next. All regressions are fixed-effects models with dummy variables for country, industry, year, or some combination thereof.

Trade volume is taken as the sum of export and import data in a given country, industry, and year. Data for the response variable is taken from the WTO Stats database under the dataset "International Trade Statistics."[98] This indicator is reported in current U.S. dollars. Loss in trade volume reflects a country's loss in transactions and worsened involvement in global trade. Industry-level imports data by country is also taken from this WTO Stats dataset.

Unit import value is taken as an index on the estimated per-unit cost of a country's imports in a given year based on its expenditures and quantities imported. While not directly a measurement of price, unit import value is very closely related to a measurement of import prices. This data is also taken from the same WTO Stats dataset under the indicator "import unit value fixed-base indices - annual (2015=100)."[99]

Nontariff trade costs are taken as the sum of estimates of bilateral trade costs for a country with all its trade partners. These are nontariff trade costs, meaning costs recorded in this indicator are attributable to transaction costs, compliance costs, and logistics. Compliance costs may exist in the form of fines firms must pay as penalties on prohibited cross-border data transfers, whereas market inefficiencies may arise from foreign firms being unable to operate the most-efficient data-driven business processes and thus incurring higher operating costs than would otherwise be the case under the scenario in which data flows went unrestricted. Therefore, changes in a country's estimate of nontariff trade costs are induced not by tariffs but by changes in a country's regulatory and/or logistical framework. This data comes from the United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) and World Bank joint database.[100]

Final panel data is merged between response, predictor, and control variables containing a sample of 23 industries, 56 countries, and 15 years. While this would give a maximum number of observations equal to 19,650 entries, the actual number of observations carried out through regression analysis is notably less because of missing data. On regression using DRI as the independent variable in regression, the maximum number of observations for regression analysis would be 840. This model's final sample size contains entries for several economies, providing a diversity of countries ranging in development, geography, and OECD status. The following are the four primary regression models analyzed, wherein c denotes country, t year, and i industry:

$$\ln(Trade\ Volume)_{c,t,i} = \beta_0 + \beta_1 DRL_{c,t-1,i} + \alpha_c + \gamma_t + \delta_i + \varepsilon_{c,t,i} \tag{1}$$

$$\ln(Unit\ Import\ Value)_{c,t} = \beta_0 + \beta_1 DRI_{c,t-1} + \beta_2 GDP\ per\ capita_{c,t} + \gamma_t + \varepsilon_{c,t} \tag{2}$$

$$\ln(Imports)_{c,t,i} = \beta_0 + \beta_1 DRL_{c,t-1,i} + \alpha_c + \gamma_t + \delta_i + \varepsilon_{c,t,i} \tag{3}$$

$$\ln(Nontariff\ Trade\ Cost)_{c,t} = \beta_0 + \beta_1 DRI_{c,t-1} + \beta_2 GDP\ per\ capita_{c,t} + \alpha_c + \gamma_t + \varepsilon_{c,t} \tag{4}$$

β_0 represents the intercept. β_1 is the coefficient for the predictor variable. This coefficient indicates the relationship between data restrictiveness and the selected economic indicator. β_2 is the coefficient for the control variable GDP per capita, which estimates the effect that change in GDP per capita incurs on the response variable in question. GDP per capita is only added as a control variable for regressions using DRI as the predictor variable instead of DRL. This control is only needed in those cases where direct change in wealth is required to be isolated in regression models so that the substitution effects of an increase in income are captured. This justification is explained in further detail in appendix B. The dummy variables α, γ, and δ represent country, year, and industry fixed effects, respectively. These fixed effects control for all other unobserved factors that undoubtedly influence response variables that are specific to only either countries (e.g., geography), years (e.g., global economic shocks or trade agreements unfolding over time), or industries (e.g., import intensity). The error term ε captures the residual value between predicted and observed values.

Ideally, the model would be more comprehensive and robust for these countries (to be consistent with past and related reports on data localization), but the lack of data and the sample of countries makes this difficult (e.g., including China and India complicates the relationships between labor productivity growth, the size of the economy, and DRI). In particular, in Cory and Dascoli 2021, the relationship between DRI and total factor productivity (TFP) was analyzed for 28 OECD countries. Unfortunately, TFP data is unavailable for many of the countries in this report (including all the non-high-income countries). Labor productivity, measured in GDP per hour worked (adjusted for purchasing power parity, or PPP), could be used with data from the Penn World Table 10.0.[101] Still, data is not provided for all 57 countries. Just for curiosity's sake (into the potential impact), ITIF used a subsample of only 36 countries that still includes our five countries and territories of interest; all the countries excluded from this subsample are non-high-income countries. Because of this smaller sample, complications arising from the inclusion of China and India (which assume greater importance in a smaller sample), and the increased relative weight of observations from high-income countries, the model to test the relationship between DRI and labor productivity and the test's results are presented in the appendix and not in the main results tables.

OVERALL FINDINGS

Regression models show that increased data localization measures yield multiple statistically significant negative impacts on an economy. The regression table estimates negative relationships for trade volume and imports associated with an increase in data restrictiveness, while estimating positive relationships for unit import values and nontariff trade costs. Coefficient estimates for trade volumes and unit import values are statistically significant at the

95 percent confidence level, while imports are statistically significant at the 99 percent confidence level (estimated p-values are less than 0.05 and 0.01, respectively). Coefficient estimates from the log-linear regression provide the percentage changes in response variables associated with a one-unit increase in DRI or DRL.

Table 2: Results of primary regression models

Dependent Variable	Ind. Variable	Coefficient Estimate	Pr(>ltl)	Standard Error	Degrees of Freedom	R-Squared
ln(trade volume)	DRL	-0.005	0.012**	0.0020	17,825	0.84
ln(Unit Import Value)	DRI	0.009	0.015**	0.0035	805	0.52
ln(Imports)	DRL	-0.006	0.002***	0.0019	17,775	0.84
ln(Nontariff Trade Costs)	DRI	0.009	0.134	0.0060	702	0.86

*Note: Statistically significant at *** p<0.01, ** p<0.05, * p<0.1*

The model finds that a one-unit increase in an industry's DRL is associated with a 0.5 percent decrease in its trade volume in the following year. While the most data-intensive industries identified in the model—such as telecommunications and finance—would be most affected, nearly every industry requires some usage of data to facilitate trade and would thus face some degree of loss in trade volumes.

Based on regression findings for this sample, imports are most sensitive to increased data restrictiveness. Increased data restrictions hinder firms' use of data in activities such as data analytics, targeted advertising, and supply chain management. The regression results suggest that a one-unit increase in an industry's DRL is associated with a 0.6 percent decrease in its imports the following year.

Regression results suggest that, on average, a one-unit increase in a nation's DRI is associated with a 0.9 percent increase in unit import value the following year for that country. Assuming the control variable GDP per capita accounts for increases in unit value due to consumers importing higher-/lower-quality products as incomes rise/fall, the coefficient estimate of DRI can be interpreted as a direct association to an aggregate measure of prices for a country's imports. Therefore, a one-unit increase in a nation's DRI reflects a 0.9 percent increase in its prices paid on imports in the following year. This effect on import prices is likely the result of a combination of market inefficiencies and compliance costs incurred from data localization measures. These higher costs of doing business for foreign firms from increased data localization would expectedly result in a rise in import prices passed along to buyers.

As further evidence that increased import prices are the result of rising trade costs incurred from data localization, regression analysis on the log transformation of nontariff trade costs reports a positive coefficient estimate. A one-unit increase in DRI is associated with a 0.9 percent increase in national aggregate nontariff trade costs among its trading partners the following year. Though the estimate is not statistically significant at the 90 percent level, it is consistent with the original hypothesis and the statistically significant estimated effect on import costs.

An increase in import prices coupled with a decrease in imports suggests that data localization constitutes a supply constraint for imports, consistent with the original hypothesis. That overall trade volume decreases in line with (but slightly less than) imports suggests that exports, too, are affected by such policies. This is unsurprising given that imported intermediate goods are often used in the production of final goods for exports, in which case the data localization policies also constitute a constraint on the country's exports.

DETAILED FINDINGS FOR EACH COUNTRY

In recent years, data localization has unfortunately increasingly captured the attention of policymakers in Asia. To illustrate what these estimated costs associated with increasing data restrictions may look like for those policymakers, ITIF extends its econometric findings to model costs of various proposed and enacted data localization measures for Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam.

In analyzing all the policies listed in this report, the model estimates that Vietnam's measures are the most restrictive, followed by Bangladesh's. (See table 3.)

Assuming that these policies are adopted and implemented over a five-year period, and assuming that the countries' DRI scores increase at a constant rate each of those five years, ITIF extends its econometric findings against the average annual change in DRI per country during a five-year period. Due to rounding, the total DRI increase does not always equal five times the average increase. Expected changes in the response variables at the end of the five-year period are reported.

It's worth recalling that the DRI is the country-level measurement of data restrictiveness. Meanwhile, the DRL is a measure of the restrictiveness at the country and industry level (using proxy data from the United States on how different industries use data to different degrees via the Data Intensity Modifier, or DRI). To determine the effects on a country's trade and imports, country-level DRLs are computed using the country's weighted-average DIM, where weights are industries' shares of total trade or imports. Since each country's trade profile is different, country-level DRLs allow for some variation in the effects data localization policies have on total trade and imports. A higher DIM—and therefore DRL—of imports than of total traded goods and services implies that, in aggregate, a country's imports are from sectors that are more data reliant than its exports.

Table 3 provides estimates of the economic impacts of data localization anticipated in these five country case studies. Note that nontariff trade barriers are not included in the table. This is both because of the lack of statistical significance at the 90 percent level and because the estimated effects on nontariff trade costs are approximately equal to those on import prices.

Table 3: Effects of data localization policies after five years

Country	Change in Data Restrictiveness Score	Change in Import Prices	Change in Imports	Change in Overall Trade Volume
Bangladesh	+2.0	+2.0%	-7.7%	-6.0%
Hong Kong	+1.6	+1.5%	-6.8%	-5.7%
Indonesia	+1.8	+2.0%	-6.9%	-5.8%
Pakistan	+1.1	+1.0%	-4.7%	-3.7%
Vietnam	+2.8	+2.5%	-10.8%	-9.0%

Based on the estimated annual change in Bangladesh's DRI implied by its current proposal, ITIF estimates that Bangladesh's level of trade will be approximately 6 percent lower after five years, with imports being 7.7 percent lower. Bangladesh's import prices are also expected to be 2 percent higher.

For Hong Kong, while estimates do not address any active legislation and only speak to a hypothetical plan, costs are still indicative of the economic burdens that could be incurred from a base data localization policy. Hong Kong's trade volume and imports would be roughly 5.7 percent and 6.8 percent lower, respectively, after five years and its import prices would be 1.5 percent higher.

Indonesia's increased frequency of data localization in recent years also brings notable consequences. Adoption of these policies is associated with a 5.8 percent decrease in trade volume and a 6.9 percent decrease in imports after five years. Indonesia's import prices are expected to be 2 percent higher after the five-year period.

Of the five countries of interest, Pakistan is the one proposing the least-restrictive data localization policy; however, it's still expected that after five years, its trade volume will be 3.7 percent lower, its imports 4.7 percent lower, and its import costs 1 percent higher.

In contrast, Vietnam's data localization policies are the most restrictive of the five countries considered. Its data restriction policies suggest that trade volume and imports would be 9 percent and 10.8 percent lower at the end of the five-year period, respectively. Import prices are estimated to be 2.5 percent higher.

RECOMMENDATIONS

Building a smart data governance framework that addresses legitimate public policy concerns in a balanced and effective way is challenging, especially for policymakers in developing countries such as Bangladesh, Indonesia, Pakistan, and Vietnam who face myriad other pressing issues and resource constraints. However, given the importance of data and digital technologies for economic development, it's critical that policymakers strive to get this balance right. In many ways, working toward a smart data governance framework is even more important for developing countries during the early stages of digital transformation and development, as it'll have a disproportionate impact as they try to not only catch up but get ahead of other countries. Likewise, if policymakers remain wedded to costly and misguided data localization policies, other countries with better, smarter digital policies will inevitably benefit, and then those countries' own firms and economies will struggle and likely fall further behind. The situation for Hong Kong is somewhat different from the other countries in this report, as it's already at a high level of digital development and connectivity and has thus far been committed to smart data governance policies. However, this means is it has more to lose if it moves ahead with localization.

The following recommendations provide a holistic set of policy ideas—both conceptual and tangible—for these countries to use instead of the false, costly appeal of localization.

Use the Right Conceptual Framework for Data Policy

Using the right conceptual framework to understand data is important for policymakers to develop smart data governance policies—and conversely, ill-fitting conceptual frameworks—lead policymakers to bad conclusions and outcomes. Policymakers in Bangladesh, Indonesia, and Pakistan need to reframe their understanding of data away from fundamentally misleading analogies they've used, especially that data is the new oil, as it will inevitably have a significant effect on the economic impact that data and digital technologies have on their economies

Data is the new oil is a bad analogy for many reasons. For example, oil is rivalrous and excludable—if I have it, you don't; and once I use it, it's gone. Data is non-rivalrous, as many people and firms can collect, share, and use the same data simultaneously, and do so again and again. Similarly, when consumers "pay with data" to access a website, they still have the same amount of data after the transaction as before. As a result, users have an infinite resource available to them to access free online services. In other words, if someone gives you $10, they have $10 less. But if they tell you they are a basketball fan, then you both know that information. Sharing their data does not preclude them from sharing the same data with others to access any number of services. Ad-supported digital services turn data into value by functioning as two-sided markets that connect consumers and advertisers.

Similarly, policymakers mistakenly think that since personal data is valuable in the same way oil and other commodities are valuable, then localization and strong privacy protections will help individuals capitalize on their data the same way a landowner benefits from owning a plot of land with oil under it. However, data is neither cash nor a commodity, and pursuing policies based on a misconception such as this will lead to policies that damage a country's digital economy. While there is significant value in large datasets, the marginal costs of each additional data point may be minimal, and not outweigh the transaction costs.

Ultimately, there is no perfectly good analogy for data, so policymakers just have to think about data as data and focus on the factors that actually help individuals, firms, and their country as a whole get the most out of using data and digital technologies. And, much more than anything else, policymakers should focus on helping both individuals and enterprises across all sectors of an economy understand how to unlock the value data can create to drive modern economic growth.

Acknowledge That Data Localization Imposes Economic Costs

Policymakers' attraction to the false sense of control they think localization gives them is constant across each country. Many policymakers clearly prioritize this sense of control over data (whether it's for law enforcement, national security, political, or regulatory ends) in supporting localization. When they talk about localization and the associated reasons, they obviously focus on what they feel it gives them. Often, they don't realize or appreciate that this pursuit of control is costly and ultimately counterproductive, as localization precludes the types of cooperation government agencies will inevitably need in terms of working with other countries on issues that inevitably spill across borders. Many policymakers act as if there are no costs, so facing up to these and making them clear is a critical starting point.

Policymakers in Bangladesh and Pakistan need to realize that the costs of localization will be particularly significant for their economies. While localization has an impact in all countries—both big and small—they're particularly acute in small and less digitally developed ones. The cost-benefit analysis foreign firms inevitably make in considering whether to enter or leave a market in the face of changes in market conditions, including restrictive regulations, simply does not add up in terms of spending large amounts of money setting up expensive, duplicative local IT systems in each and every market. Bangladesh and Pakistan may be promising emerging digital markets, but doing so simply doesn't make commercial sense. Meanwhile, changing the price and availability of increasingly important digital tools will impact their whole economy—never mind the additional costs if trading partners enact retaliatory measures.

Policymakers' attraction to the false sense of control localization gives them is both economically costly and counterproductive, as not only does it not lead to greater data privacy or cybersecurity, but it also precludes the international cooperation countries inevitably need given the global Internet.

The focus on control is not surprising, as policymakers everywhere are figuring out how to ensure that laws are best fit for today's digital era. Unfortunately, policymakers mistakenly think that forcing firms to store data locally is the best option or that data localization is the only way to get firms to respond to governments' requests. This reflects the mistaken belief that firms can avoid oversight and requests for data by simply transferring data out of a country, and that firms can pursue some form of regulatory or legal arbitrage in terms of picking and choosing which country's laws they follow and which they don't. Data localization requirements do not change who is responsible for the data, regardless of where it is stored.

In this way, policymakers mistakenly think that localization enhances the state's agency and that of their own firms and people. At best, the agency gained by data localization is illusory. In most cases, it is costly and counterproductive. And in the case of human rights, it is often predatory given that the agencies localization supports are often those involved in surveillance and social and political control. Not only is localization a costly distraction from policies that actually address legitimate cross-border data-related issues, it's a barrier to them. Digitalization means that cooperation and data sharing between governments is both inevitable and only going to get more important. The sooner policymakers realize that localization is not the silver bullet they think it is and focus on constructive tools to address legitimate underlying issues, the better.

Recognize That Controlling Data Is Both Impractical and Counterproductive

Some policymakers misguidedly pursue "control" over data via localization and laws that include broad sweeping prohibitions on foreign jurisdictional reach over local data. For example, Bangladesh's draft data privacy bill includes an outright prohibition in article 42 of any "other state's court, law enforcing agency or authority" having jurisdiction over, or access to, data generated in Bangladesh.[102] Such sweeping legal prohibitions are not only costly but also impractical and counterproductive. They fail to recognize that the Internet is a global technology platform, local digital services will inevitably have global connections by default (except in extreme situations such as in China), these countries will naturally assert their legal authority over it within their own jurisdictions, and governments will inevitably need to cooperate on data.

Such misguided or poorly designed jurisdictional restrictions can subject organizations to conflicting and unworkable laws. Moreover, they create toothless rules subjecting organizations (both foreign and domestic) to regulations that are impractical (given the global Internet) and regulators cannot realistically enforce. While any country can demand only local jurisdiction or extraterritorial application of its laws, it may not always be able to enforce them (as this can be quite complex). A law being overly broad and unclear in terms of its application leads to firms geo-blocking a country's users from some or all of their services (meaning they become inaccessible) as a precautionary measure to avoid inadvertently infringing on the law.

Enacting sweeping legal provisions that prohibit data transfers in order to prevent foreign jurisdictional reach is misguided, impractical, and counterproductive, as it precludes engagement in the types of legal agreements and cooperation that help countries address data-related issues.

These types of sweeping prohibitions are also misguided as they essentially preclude or make it more difficult for a country's judicial or other governmental authorities to gain access to relevant evidence or data in other countries. Such international cooperation is increasingly important to many data-related issues. It essentially disqualifies a country from participating in international treaties or agreements regarding mutual legal assistance (MLA) and access to evidence in civil, commercial, and other matters, such as the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters. These agreements are increasingly important given the digital nature of modern law enforcement and regulatory investigations and enforcement.

Policymakers should remove such sweeping and problematic prohibitions and jurisdictional assertions and instead make clear in local laws that they apply to firms with a legal nexus in a country (in line with the accountability principle, detailed ahead) and that the government can participate in bilateral, regional, and multilateral agreements on data, such as the Hague Evidence Treaty, bilateral MLA agreements and treaties, and other agreements between government authorities.

Focus on the Fundamentals of ICT Adoption

To maximize the economic and societal benefits of data and digital technologies, policymakers need to avoid the fatal attraction to data nationalism and digital protectionism and instead focus on the fundamentals of ICT adoption, education, digital infrastructure, and smart data governance policies.

The summaries of these key components below align with many from UNCTAD and other organizations involved in supporting digital development.[103] These actually address issues commonly cited in surveys of e-commerce firms in these countries.[104]

- **Reducing or eliminating artificial costs associated with data and data-reliant goods and services:** Cost is a major driver of ICT adoption for consumers and firms alike, as rising prices generally lead to falling demand. ICTs are a general purpose technology that have a major economic impact.[105] Cost should be a central concern, as the basics—having Internet access and a smartphone—remain beyond the reach of many millions of people around the world. Policymakers should aim to eliminate tariffs on ICT imports, eliminate discriminatory taxes on ICT goods and services, and ensure that users can buy best-in-class technology. Focusing on cost and accessibility is critical because, for many countries, major gains in digital development will come from getting as many firms as possible to adopt and use existing ICT equipment, computer software, and cloud services.
- **Maximizing the supply of reusable data:** To promote the availability of data and encourage businesses to use it, policymakers should both avoid laws and regulations that stifle the supply and flow of data, such as overly burdensome data-protection rules and data-localization policies, and increase the supply of data, such as via open data and freedom-of-information policies.[106] Maximizing the supply of reusable data is also about getting more firms to use ICT to generate, collect, and analyze data (which brings it back to the issue of cost as a driver of deployment and adoption). The more firms use ICT services, the more data they can generate, collect, and analyze in order to improve efficiency and drive further research and development. Government agencies can contribute through "open data" laws that facilitate access and use of the large amounts of data they collect.[107]
- **Focusing on deriving insights from data, not trying to store it locally:** Data localization policies are premised on the faulty assumption that the location of data matters in maximizing the value of that data. It doesn't. Success in the data economy depends on how effectively firms and individuals can leverage data to generate insights and unlock value.[108] Policymakers should focus on how to assist local firms in understanding how they can generate and create value from data, such as through the use or development of data analytics services or by creating data streams around manufactured or agricultural goods. Much of the value firms derive from data comes not from individual data points but from collective data, such as aggregated user data. This means policymakers should be encouraging data sharing as well as the development of digital platforms that make it possible to collect and analyze large-scale datasets.
- **Improving physical infrastructure:** Infrastructure is a priority issue for digital development, as Internet connectivity depends on it. Obviously, improved Internet penetration and speeds are crucial to data-driven innovation and digital trade, as inadequate fiber-optic networks lead to poor-quality data services and inconsistent coverage, thereby holding back the spread of mobile Internet services in urban and rural areas.

- **Improving human capital:** Data innovation does not just happen; people make it happen. Success in the data economy requires a workforce with the skills necessary to operate the latest technology and processes and analyze complex datasets. Policymakers in all countries face the challenge of encouraging the development of these data-related skills through their education systems and professional training programs. The Center for Data Innovation's reports "The Best States for Data Innovation" and "The State of Data Innovation in the EU" provide a potential model for countries and organizations to follow in conducting an analysis of how they are doing in addressing the various aspects of human and business capital.[109]

Adhere to the Accountability Principle

Instead of focusing on localization and "control," policymakers should focus on legal accountability such that rules travel with the data. The accountability principle is based on the fact that modern technology, especially the Internet and cloud data storage, means that each country's domestic regulatory regime for data (e.g., for privacy) needs to be globally interoperable as, each country faces the same challenge in applying its laws to firms that may transfer data between jurisdictions. Interoperable privacy frameworks are the international extension of this accountability-based approach in that data therein is still able to flow between different privacy regimes, and countries' data protection rules flow with it.

Most simply, policymakers can bring the accountability principle to life in data privacy and other laws by clearly stating that these laws apply to all firms, whether foreign or domestic, that do business in a country and thus have a legal nexus/presence. Having a legal presence or engaging in significant business activity (e.g., having offices, employees, bank accounts, physical property, or substantial marketing) is usually sufficient to establish a legal nexus that enables countries to enforce their laws.[110]

Instead of focusing on localization and "control," policymakers should focus on legal nexus and accountability in order to ensure local rules travel with the data.

Policymakers can explicitly state that this legal responsibility extends to the third-party data processors these firms use, regardless of where they are located. In other words, a country's local laws travel with the data. Companies doing business in a given country would have a strong incentive to assist their partners outside that country in adhering to its privacy protections, because its citizens and the government could seek remedies from that company for any privacy violations, such as a data breach, irrespective of whether that company or its partners were at fault. An example of this is Article 43 of Bangladesh's draft data protection act that highlights the obligations of companies (both data transferor and recipient) to protect data regardless of its location of storage. If this law focused on this legal accountability and not localization, it would constitute much better legislation.

The concepts of legal nexus and responsibility are used in data privacy and protection laws worldwide. The accountability principle was first developed by OECD and subsequently integrated into many legal systems and tools, including those of the EU, Japan, New Zealand, Singapore, Canada, the APEC Privacy Framework, the APEC Privacy Recognition for Processors system, APEC Cross Border Privacy Rules system, and the ASEAN Model Contractual Clauses.

Adopt Global Tech Standards, Accreditations, and Best-in-Class Tools for Government

Many policymakers are understandably concerned about ensuring government data and services are secure, which leads many to consider data localization. Policymakers misunderstand that the confidentiality of data does not generally depend on which country the information is stored in, but rather only on the measures used to store it securely. As noted, a secure server in Malaysia 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. Instead of localization, policymakers should focus on developing standard cloud cybersecurity requirements and contracts for government agencies to use in selecting cloud service providers. The central point is to develop criteria to judge whether a cloud service provider is truly committed to international cybersecurity best practices.

Governments can do this by ensuring cloud providers are audited and certified against international standards. For example, Germany and Singapore have adopted the ISO/IEC 27001 (the world's best-known standard for information security management systems), ISO/IEC 27017 (guidelines for information security controls applicable to the provision and use of cloud services), and ISO 27018 (code of practice for protection of personally identifiable information in public clouds) as the baseline requirements in their respective accreditation schemes.[111] Policymakers should use international standards, not only due to their high level of protection, but also because imposing additional country-specific security requirements beyond international standards leads to unnecessary duplication, an increase in compliance costs, and a focus on documentation and not on improved security outcomes.

Policymakers misunderstand that the confidentiality of data does not generally depend on which country the information is stored in, but rather only on the measures used to store it securely. For government data and services, policymakers should use international cybersecurity standards and accreditations.

To maximize the usefulness of global cybersecurity standards and certifications, policymakers should use qualified, specialized third-party assessors to perform security assessments to ensure that firms conform to the agreed upon standards and requirements. Using third-party assessors avoids unnecessary and wasteful duplication and keeps the focus on the underlying security situation rather than on trying to recreate this capacity within government. Relying on a slow, in-government auditing process ensures that the focus is on effective oversight rather than developing and maintaining specialized expertise for security audits and conformity assessments.

Policymakers could also formally recognize, accept, and/or adapt accreditations from countries that use high-standard cloud cybersecurity accreditation regimes as a fast way to identify cloud firms and service offerings that adhere to cloud cybersecurity best practices. For example, New Zealand recognizes Australia's Information Security Registered Assessors Program (IRAP) accreditation.[112] It could also include the U.S. FedRAMP or Germany's C5 accreditations. This would lead to more suppliers, as it would remove a major source of uncertainty about providing services to the government. Countries could recognize other accreditations individually or, ideally, in cooperation with neighboring or like-minded countries via regional or multilateral accreditation reciprocity agreements. For example, Kuwait's memorandum of understanding

(MOU) with Bahrain on cloud cooperation is an example of the type of cooperation that would hopefully lead to more formal recognition of cloud cybersecurity accreditations.[113]

Adopt Model Agreements to Support Law Enforcement Access to Data

Policymakers should review and reform domestic and international legal frameworks to help law enforcement ensure they can request and receive—in a timely manner—the data they need for criminal investigations.

For law enforcement, the need to improve these legal tools and processes is clear. The globalization of criminal evidence should drive reforms regarding how law enforcement can access communications and other records in other countries as part of legitimate investigations while abiding by privacy and human rights protections. Criminals should not escape the law simply because police cannot efficiently access the data they need. For example, the EU's "e-evidence" proposal streamlines cooperation between service providers and law enforcement in the bloc.[114] The EU and United States already have one agreement (the Umbrella Agreement), and are talking about other agreement to expand this cooperation.[115] Unfortunately, in the absence of updated legal mechanisms, there exists the potential for a legal arms race calling for mandatory data localization requirements, which would ultimately hurt all law enforcement efforts to deal with what is a global problem. If everyone requires localization, cooperation will only get significantly harder to achieve than it already is.

The first goal for Bangladesh, Pakistan, Indonesia, and Vietnam should be to improve domestic processes and law enforcement capabilities as part of updated MLA agreements, MLATs, bilateral request mechanisms, or a combination thereof.[116] There are various issues involved in improving legal cooperation and compatibility: the standard of proof, authorized authorities and the judicial or independent validation of requests, necessity and proportionality, the ability for service providers to challenge requests, the types of crimes covered, and other issues.[117] At the moment, MLAs and MLATs remain the most common tool for enabling cross-border data exchanges; however, in many cases, they are not working well and need updating. Law enforcement and policymakers in these countries are fair in criticizing these tools as slow, as some countries take years to respond to requests, while others, such as Russia, often do not respond at all.[118] For instance, Bangladesh and Indonesia reported that it generally took 6 to 12 months to get a response to their requests for MLA.[119]

Bangladesh, Pakistan, Indonesia, and Vietnam should improve legal processes and law enforcement capabilities as part of updated MLA agreements, MLATs, bilateral request mechanisms, or a combination thereof. They should also join the Budapest Convention.

Instead of localization, governments should work with relevant stakeholders (including international partners) to formulate reforms and model data transfer agreements and request templates. Pakistan has considered (but not negotiated) an MLAT with the United States (and will also be signing the Budapest Convention, see ahead).[120] There are no U.S. MLATs with Bangladesh, Indonesia, and Vietnam.[121] Indonesia is clearly able to negotiate updated agreements, as it negotiated an MLAT with Switzerland in 2020.[122] At a regional level, ASEAN-developed MLATs have been used between some, but not all, members (e.g., Indonesia and Vietnam).[123]

The ultimate goal for these countries should be to sign on to the Budapest Convention on Cybercrime—the world's first cybercrime treaty, negotiated 20 years ago—and support ongoing efforts to improve it via a new (second) protocol. Along the same lines as the prior steps, this new protocol helps law enforcement agencies secure evidence from service providers in foreign jurisdictions.[124] Despite their complaints about this issue, none of the report's target countries are signatories, or observers.[125]

Provide a Clear and Level Playing Field for Digital Payments

Seamless digital payment services are critical to cross-border e-commerce and digital trade. Localization and other payment service restrictions make this very difficult and costly.[126] Countries should remove payment data localization and instead focus on ensuring each country has an efficient, secure, and competitive payment sector that is interoperable with the rest of the global economy. Otherwise, their consumers and businesses will struggle to get paid for goods and services provided over the Internet.

One way to do this would be by establishing payment councils to create a public-private dialogue on payment policy issues. For example, the Monetary Authority of Singapore set up the Singapore Payments Council comprising 20 representatives from payment service providers, financial institutions, trade associations, and merchants.[127] For Indonesia and Vietnam (as ASEAN members), the focus should be on the ASEAN e-Payments Coalition, which is working with the ASEAN Working Committee on Payment and Settlement Systems (made up of central bank representatives) to develop a regional payment framework that improves user payment experiences, promotes regional integration, increases trust and security, and improves the livelihoods of the underbanked.[128] Bangladesh and Pakistan could work with other regional financial regulatory authorities in a similar way, whether bilaterally or regionally.

CONCLUSION

To maximize the social and economic benefit of data and digital technologies, policymakers should focus on the fundamentals and the need for balance as part of smart data governance. Countries should pursue a framework that supports individuals and firms using data to generate new insights and value (wherever data is stored, given modern cloud computing) alongside domestic and international legal tools and cooperation to support the enforcement of domestic data-related laws, legitimate government access to data, and regulatory oversight. Alternatives to localization will be challenging and will take time, effort, resources, and cooperation and support from international partners. But as they remain essential to supporting digital development, it's better if policymakers realize this and focus on these foundational policies. Ultimately, data localization represents a costly and misguided distraction from much-needed policies that actually help everyone—individuals, firms, government agencies, and society and the economy as a whole—succeed and benefit from global data flows and digital technologies.

APPENDIX A: DATA LOCALIZATION POLICIES IN EACH COUNTRY

Bangladesh

Telecommunications Law

Bangladesh's Telecommunication Law requires mobile operators to obtain a license and specifies the criterion that they establish local data centers for national security purposes (to enable intercepts).[129]

Bank Company Act

Bangladesh's (1991) Bank Company Act (section 12) states that banks can't transfer business-related documents outside the country without first getting the Bangladesh central bank's permission.[130]

Draft Data Protection Act

Bangladesh's draft Data Protection Act (DPA, 2022) includes data localization requirements (Sections 44 and 45).[131] It essentially requires firms to segregate data post-processing into sensitive, critical, and general personal data, which is technically impracticable. It also only allows consent or ad hoc governmental approvals as a basis for transferring certain types of data, and includes extremely broad and far-reaching investigative powers, including the power to obtain access to all personal data and access to any premises. Section 44 directs that sensitive data, user-generated data, and classified data (as designated by the government) shall be stored only in Bangladesh and that "the same (data) shall be beyond the jurisdiction of courts and law enforcement agencies or authorities of any other state, other than the courts and law enforcement agencies or authorities of Bangladesh." If enacted, this prohibition would disqualify Bangladesh from participating in international treaties or agreements regarding MLA and access to evidence in civil, commercial, and other matters, such as the Hague Evidence Treaty.[132] Firms that transfer sensitive data out of Bangladesh must inform the Bangladesh government.[133]

Draft National Cloud Policy

Bangladesh's draft National Cloud Policy (2020) includes explicit data localization for all personal and government data. Transfers of data are only allowed for backup purposes, but only if the data doesn't include any personal or sensitive information or is data that is otherwise "not detrimental to the security of Bangladesh and important infrastructure" and if the transfer is to a country where Bangladesh can fully enforce its laws through bilateral or multilateral agreements.[134]

The draft Cloud Computing Policy states:

> The primary location of cloud service provider's data storage must be in Bangladesh. Information may be allowed to be taken outside Bangladesh for back-up and retrieval purposes where the such [*sic*] information do not have any personal, sensitive or any such information and information which is not harmful to the security and critical information infrastructure of Bangladesh. All that information should be hosted in those countries where the Government of Bangladesh has multilateral or bilateral relations for unconditional and instantaneous laws can prevail.[135]

The localization impact of the draft Cloud Computing policy is potentially broad. It lacks a clear definition for restricted data categories ("personal information," "sensitive information,"

"information that is harmful to the security and critical information infrastructure"), with the likely result that firms overclassify information into these categories. Similarly, the impracticality of segregating broad categories of data types from other data types (e.g., personal and nonpersonal data and sensitive and nonsensitive data) will inevitably result in much broader localization in order to avoid potential legal risks.

Hong Kong

There are currently no explicit restrictions on the transfer of data out of Hong Kong. However, there have been several policy proposals that opened the door to localization, and there are several indications that Hong Kong is considering localization (even if indirectly, via de facto localization).

Hong Kong's Personal Data (Privacy) Ordinance (PDPO) does not currently restrict the transfer of personal data outside Hong Kong, including to mainland China. However, Hong Kong's Office of the Privacy Commissioner for Personal Data (the Privacy Commissioner) issued its Guidance on Personal Data Protection in Cross-border Data Transfer, which stipulates the conditions in which data can be transferred outside Hong Kong, including adequacy and consent. Section 33 of the PDPO does contain provisions restricting the transfer of personal data outside Hong Kong; however, this section has not yet been enacted. The Privacy Commissioner has for some years pushed for Section 33 to be brought into force and is prepared for when that happens.[136]

Hong Kong's Securities and Futures Commission released a circular in October 2020 that requires banks and other regulated groups to store data locally or ensure their cloud provider guarantees it will hand over information on request.[137]

In October 2021, the chief executive of Hong Kong announced plans to require public utilities and other crucial infrastructure operators to strengthen their systems against cyberattacks. The scope may include public utilities, Internet service providers (ISPs), and transport.[138] The concern is that Hong Kong follows China's broad definition of critical infrastructure and a restrictive approach to associated data (including localization). Similarly, China's proposed regulation to screen mainland companies for cybersecurity before their initial public offerings in Hong Kong includes assessing their data on national security grounds.[139] Given Chinese sensitivity over Chinese-listed firms providing data to U.S. financial regulatory authorities as part of listings in the United States, it seems likely that Hong Kong listings will include specifications to store data locally (or, at least, not in the United States).

There are two major laws that may lead to data localization. First, on June 30, 2020, Hong Kong enacted a new National Security Law. The Chinese Communist Party carefully planned the surprise introduction of the National Security Law, meaning the public was not aware of the existence of such a proposal until a week before it was voted on in Hong Kong. However, over the course of the next few years, elements of the Cybersecurity Law could be slowly introduced in Hong Kong, starting with law enforcement access to data, security and localization requirements for mainland citizens' and organizations' data, in addition to critical information infrastructure protection measures.[140]

Beijing's role in directly imposing the law effectively ended Hong Kong's autonomy and has infringed on human rights guaranteed under Hong Kong's Basic Law and international human rights laws in force in Hong Kong.[141] Under Article 43 of the National Security Law and the implementing measures enacted by Hong Kong's government, police can order the blocking and deletion of content by message publishers, platform service providers, hosting service providers, network service providers, or a combination thereof, and can intercept and access communications or conduct covert surveillance.[142]

Second, Hong Kong is actively considering a restrictive cybersecurity law similar to that of mainland China that would require critical information infrastructure providers to store data locally. However, Hong Kong authorities (and the local business community) are cognizant that an overly broad critical information infrastructure bill would adversely affect its position as a global business center and the government's plans for Hong Kong to play a central role in its "Greater Bay Area" (Guangdong-Hong Kong-Macao) economic development strategy.[143] Indicative of this, Hong Kong has advocated that the mainland government ensure data can flow between Hong Kong and the mainland, even if data cannot be transferred onwards.[144]

Indonesia

Indonesia has considered a series of data localization efforts, many of which stem from Ministry of Communication and Informatics Regulation 82 of 2012, which requires "electronic systems operators for public service" to store data locally, mandating that all operators come into compliance by October 2017. Regulation 82 has been revoked and replaced by regulation 71 of 2019 on Organization of Electronic Systems and Transactions. Unlike Regulation 82, Regulation 71 draws a distinction between public and private electronic systems operators, and only imposes data localization obligations on public electronic systems operators. In GR 71/2019 draft implementation regulations, storing and processing of data offshore by any "Electronic Systems Providers" (ESPs) would require prior approval from the government.[145] The definition of Public Scope ESPs includes government agencies, which goes beyond national security and intelligence data. There is no further clarity regarding the circumstances by which data can be stored and processed offshore in the case of Public Scope ESPs, including the guidelines that the Minister of Communications and Informatics will use when reviewing data offshoring required by Privacy Scope ESPs. GR 71 establishes an interagency committee to set up and oversee the exception for Public Scope ESPs to store and process data offshore, yet this committee does not seem to have met or helped clarify who exactly GR71 applies to. Essentially, this creates an ambiguous data localization requirement for firms associated with Public Scope ESPs. There is also a Ministry of Communications and Informatics Circular Letter that requires all ministries to obtain clearance from the Ministry of Communications and Informatics for any IT procurement to ensure maximum utilization of the National Government Data Center, which acts as a de facto localization and data processing barrier.[146] Foreign firms have lost, and continue to lose, business in Indonesia due to the ambiguity in these data localization requirements.

E-commerce

Indonesia's regulation No. 80/2019 on E-Commerce stipulates that personal data cannot be transferred offshore unless the receiving nation is deemed by the Ministry of Trade as having the same level of personal data standards and protection as Indonesia.[147] This could act as a de facto localization policy. Hopefully, Indonesia's new data protection bill will provide clarity as to where and how firms can transfer data to address and avoid this potential outcome.

Payment Data and Services

Indonesia considered, but revised, certain rules that would've effectively prohibited foreign firms from playing a role in its domestic payments sector as part of its initiative to launch a domestic payment gateway.[148] These restrictions would've led not only to data localization but also forced data sharing so that a single state-supported company would be solely responsible for processing credit and debit data. The initial proposal by Indonesia's central bank would've forced payment firms to store data locally and mandated that payment gateway providers must be approved by the central bank and 80 percent domestically owned. This would've included the "standards institution," which is in charge of creating, developing, and managing the technical and operational specifications (including security and data protection) of the domestic gateway. It also would've included the "switching" institution, which is in charge of processing domestic payment transactions data.

Prior to this proposal, Indonesia allowed 100 percent foreign ownership. In 2018, Indonesia's central bank reconsidered these restrictions and excluded credit card transactions from the rules, thus allowing them to transfer this data offshore.[149] However, Indonesia maintains local ownership requirements for payment systems. In 2021, Indonesia's central bank released new regulations that require nonbank payment services to have at least 15 percent Indonesian ownership. At least 51 percent of shares with voting rights must be owned by Indonesians, individuals, or entities.[150]

Banking Data and Services

Indonesia's overall approach to financial data governance is still based on data localization. The Bank of Indonesia still requires core/important financial transactions to be processed domestically, while the Financial Services Authority (known as OJK) has incrementally allowed some electronic processing systems to be based offshore for banking services, insurance services, multi-financing services, and lending-based technology. Despite some progress, the overall policy requires businesses to domestically process their financial transactions.[151] In 2021, OJK enacted a regulation (4/POJK.05/2021) on IT risk management for nonbank financial institutions that they must have data centers and disaster recovery centers in Indonesia, though some exceptions apply.[152]

Pakistan

Pakistan has proposed and enacted several restrictive data laws and regulations. The State Bank of Pakistan requires financial and banking data to be stored and processed locally.[153] In 2022, Pakistan launched a Cloud First Policy, which allows government agencies to require local data storage for a broad range of data categories ("restricted," "sensitive," and "secret"). Pakistan's Cloud First Policy does include a fair degree of sensible analysis and advice, yet it still clearly prefers local data storage (see the section on "data sovereignty and data flows").[154]

Draft Personal Data Protection Bill

In February 2022, Pakistan's Cabinet approved a draft data protection bill, which will go to a parliamentary committee for consideration and deliberation (exactly when is unclear).[155] Section 14 states that "critical personal data shall only be processed in a server or data center located in Pakistan." Section 15 states that "personal data other than those categorize[d] as critical personal data may be transferred outside the territory of Pakistan under a framework (on conditions) to be devised by the Commission … The Commission shall also devise a mechanism for keeping some components of the sensitive personal data in Pakistan to which this act applies, provided that related to public order or national security."[156] Critical and sensitive data is to be defined by the Personal Data Protection Authority, which will reportedly have extensive powers to introduce new regulatory frameworks and data access requirements. Segregation of data into sensitive, personal, or critical data in order to give them special treatment, such as local storage, is technically not feasible for many businesses, particularly local and small to mid-sized businesses. Furthermore, the Authority has the power to impose data mirroring requirements that would require a copy of the data to be stored in Pakistan.[157] It also does not protect personal data from state surveillance because of broad exceptions—allowing collection and storage of personal data "for legitimate interests," which is undefined by the bill, and giving the government the ability to exempt any provision from applying to itself.[158] These provisions appear to be modeled after India's draft data protection bill.

The draft bill includes vague and broad extraterritorial applications (section 3), stating that it applies to (A) all persons that process, have control over, or authorize the processing of personal data, where the data controller or data processor is located in Pakistan; (B) all foreign-incorporated data controllers or data processors who operate (whether "digitally or non-digitally") in Pakistan and are involved in any commercial or non-commercial activity in Pakistan; (C) all processing outside of Pakistan in places where Pakistani law applies "by virtue of private and public international law"; and (D) any data subject in Pakistan. The thresholds in this version of the draft bill are much wider than those under Europe's General Data Protection Regulation (GDPR), including foreign entities engaged in the broadly worded "non-commercial" activity in Pakistan, and foreign entities to which Pakistani laws apply "by virtue of private and public international law."[159]

The Cyber Crimes Law and Removal and Blocking of Unlawful Online Content

In 2016, Pakistan enacted PECA (commonly known as the Cyber Crimes Law).[160] PECA goes beyond traditional cybercrimes and criminalizes certain online speech, while giving authorities unchecked powers to curtail and prosecute it. Section 37 of PECA gives unbridled powers to the Pakistan Telecommunications Authority (PTA) to block or remove online content, thereby restricting the right to freedom of expression, as guaranteed by Article 19 of the constitution. Under PECA, the Ministry of Religious Affairs and Interfaith Harmony can also review Internet traffic and report blasphemous or offensive content to the PTA for possible removal or to the Federal Investigative Agency for possible criminal prosecution.

Under PECA, in 2020, Pakistan enacted Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2020.[161] Pakistan considered and enacted amendments to this legislation in 2021, but most problematic provisions remain unchanged, including data localization and a local office/staff.[162] Rules 7 and 8 provide for blocking and removal of unlawful online content. Rule 9 stipulates further obligations of ISPs and Social Media Companies (SMCs). For example, it requires social media platforms (with more 500,000 users in Pakistan or in the list of ISPs or SMCs with the PTA) to (a) register with the PTA within nine months; (b) establish a permanent registered office in Pakistan within nine months; (c) appoint a focal person based in Pakistan to coordinate with the authorities for compliance with domestic law; and (d) establish a database server in Pakistan within 18 months. Rule 9 further obliges ISPs or SMCs to issue certain community guidelines for access and usage of any online system. It requires SMCs to provide the designated investigation agency with any information or data in a decrypted, readable, and comprehensible format. If the service provider doesn't respond, the government may degrade or completely block the services of such service providers for a period of time and fine them up to Rs500 million. These restrictive requirements are problematic, but so is the oversight. The rules allow a broad range of state agencies to make confidential requests for content removal through the PTA without any visibility into the source of the complaint. Similarly troubling, the authority has been empowered to hear reviews against its own decisions.[163]

Vietnam

Law on Cybersecurity

Vietnam's LOC took effect January 1, 2019; however, key provisions need further guidance before implementation, including data localization and local office requirements. The localization requirement is broad and the requirement for data access and content takedowns may not be practical, in the scope of the regulation, for all types of firms that may not have the necessary visibility into data stored on their platform.

The law includes expansive data localization mandates and content requirements. A central mechanism to the localization requirement is that the Vietnamese MPS will instruct firms to localize data on a case-by-case basis, depending on their ability to provide access to data upon request and to remove certain content. MPS has stated that the localization and office establishment will only be triggered when entities fail to cooperate with the authority in providing information serving the investigation and handling of crimes. Firms would have 12 months to set up local data operations. But details of how this will work in practice and the extent of this requirement are unclear.

The service providers and type of data required to be stored are broad. Regulated services include telecommunications services; storing and sharing data in cyberspace; providing national or international domain names to service users in Vietnam; e-commerce; service providers of online payments; payment intermediaries; connectivity transport services through cyberspace; social networks and social media; online video games; and services providing, managing, or operating other information in cyberspace in the form of messages, voice calls, video calls, emails, and online chat. Under the law, covered service providers are required to store personal data of Vietnamese end users, data created by users, and data regarding the relationships of a user within the country for a certain period of time. LOC Article 26.3 states that only "domestic and foreign companies, which provide services on telecom networks and on the Internet and other value-added services in cyberspace in Vietnam having the activities of collecting, exploiting, analyzing and processing personal data, data about the relations between the users of the services, and data created by the users in Vietnam" shall store these data in Vietnam. It also sets out the conditions under which a foreign firm can be instructed to localize data and establish a branch or representative office in Vietnam.[164]

Data localization requirements will be enforced via implementing regulations. In 2022, Vietnam issued Decree No. 53/2022/ND-CP (known as Decree 53) detailing the implementation of a number of provisions, particularly on data localization. It went into effect in September 2022. Decree 53 requires "foreign" and "domestic" online service providers (as specified in the LOC) to store user data within Vietnam's territory and establish a branch or representative office in

Vietnam. Article 27 of Decree 53 requires that the covered data shall be stored for at least 24 months from the date of receiving the request for the storage.

However, Article 26.2 of Decree 53 could be interpreted as all domestic companies being required to store the data in Vietnam, creating an inconsistency with the previously mentioned provision of the LOC. Furthermore, Article 26.2 of Decree 53 stipulates, "domestic enterprises shall store the data specified in clause 1 of this Article in Vietnam." It is, however, currently unclear whether domestic enterprises are expected to store (a) a copy of the data locally or (b) the required data can only be stored in Vietnam.[165]

Decree 72 on Content Moderation

In July 2021, the Vietnamese government proposed amendments to the Ministry of Information and Communication Decree 72/2013, including requiring all foreign firms providing cross-border services with over 100,000 Vietnamese unique visitor access per month to store data locally, set up a branch or representative office in Vietnam, and enter into a content cooperation agreement with Vietnamese press agencies when providing information cited from the Vietnamese press. Article 44.i.3 and 44.k.4 set out the disproportionate, unnecessary, in many cases technically infeasible data localization requirements. The decree, as worded, potentially applies extraterritorially.[166]

Requirements for content removal are onerous and sweeping, especially in light of the broad definitions of what "prohibited acts" could entail. For instance, any act the Vietnamese government considers to be "adversely affecting social ethics, social order and safety and the health of the community" would be in scope.

Amendments to Decree 72 (or Draft 1.3) have maintained, and in some cases exacerbated, the overly prescriptive, expansive, and at times ambiguous provisions of the previous draft, for example, the unfettered expansion of takedown authority (Article 22.2 (a)), or the ambiguous concept of multiservice online platforms (Article 23.6 (dd)).

Decree 72 also requires digital platforms, including cross-border providers, to take down violating content within a 3-hour or 24-hour period (Articles 22.3(b), 22.3(dd), and 22.5)). These obligations are simply impossible for companies to comply with. Proactive screening of billions of pieces of content would be operationally and technically burdensome. Furthermore, the provisions requiring a content cooperation agreement with local media (Article 22.3(c)) and child protection measures (Article 44d.2) remain unclear and unfeasible to comply with.[167]

Personal Data Protection Decree

On February 9, 2021, Vietnam's MPS released the full text of the Draft Decree on Personal Data Protection (PDP), which includes localization requirements. The current draft prescribes conditions a personal data processor must fully satisfy with regard to the treatment of personal data of Vietnamese citizens, including "registration" of transfers of such data overseas, which will impact cross-border data flows. Before transferring Vietnamese citizens' personal data out of Vietnam, the processor must fulfill four stipulated conditions, one of which is the original data must be stored in Vietnam (a concept known as "mirroring"). The firm must also build a system to store its data transfer history for three years. A related draft Decree on Administrative Penalties for cybersecurity contains high penalties for violations of the PDP of up to 5 percent of total revenue.

The draft is broad and onerous. For example, firms must register sensitive personal data with the Personal Data Protection Commission, which processes each valid application within 20 working days from the date of receipt. This requirement is very burdensome for companies.[168]

Payment Data and Service

Vietnam uses de facto payment data localization and other restrictions to support a state-owned electronic payments firm by requiring that all credit and debit payment transactions be processed by a government-owned monopoly.[169] This makes the state-owned firm a direct competitor in the payments sector, while precluding foreign market access.

APPENDIX B: DETAILED MODELING METHODOLOGY

Previous Analysis and Best Practice Modeled

The quantitative model employed in this report follows best econometric practice on the analysis of data localization's impacts on economies as exhibited through work of OECD, the European Center for International Political Economy, the Global Commission on Internet Governance, and Vox EU/CEPR.[170] These works highlight that modelers devise a scoring-weighting methodology over a series of categorical policy changes in order to quantify a measurement of restrictiveness over trade that is otherwise not explicitly measured. With respect to the issue of data localization, the same high-level approach can be used to score countries' restrictiveness due to data localization measures based on a common quantitative index. Given the increasing volume of work on measuring digital trade restrictiveness, an index measuring data localization may be selected through proxy. For example, OECD's Digital Services Trade Restrictiveness Index, ECIPE's Digital Trade Restrictiveness Index, and OECD's Product Market Regulation database are three measurements of countries' trade restrictiveness on which their measurements are impacted by the barriers imposed on data flows. In ITIF's previous work in 2021 estimating the economic impacts of data localization, a proxy measurement on data restrictiveness was selected via OECD's PMR database sub-indicator data. However, the currently available sources on which to design a proxy index measuring data restrictiveness are insufficient for this report, the purpose of which is to provide an analysis of sufficient sample size that is capable of generating estimates on economic burdens of data localization for Asian economies. This model seeks to build a sample size inclusive of all countries recorded in ITIF's 2021 data localization report along with observations for Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam. The available sources of proxy data localization do not include measurements on all economies of interest. Given those constraints, this model differs from ITIF's previous work by designing its own methodology to quantify data restrictiveness of countries based on tabulations on the number of enforced measures restricting the flow of data within them.

Data Restrictiveness Index

ITIF calculates its DRI here as a function of a country's number of data restrictions in place up to the given year. Measurements of DRI are taken at the level of country year and show how data localization policies differ across countries and over time.

As previously shown, a country's DRI in a given year is calculated as

$$DRI_{c,t} = \sum_{j=1}^{n} data\ restriction_{j,c,t}$$

where c denotes the country, t the year, and j the data localization policy (of which there are n total). A data localization policy j's "data restriction" measure is computed as

$$data\ restriction_j = d_j * k_j$$

where d denotes a policy's directness and k the type of data restricted. Possible values for d and k are presented in table 4.

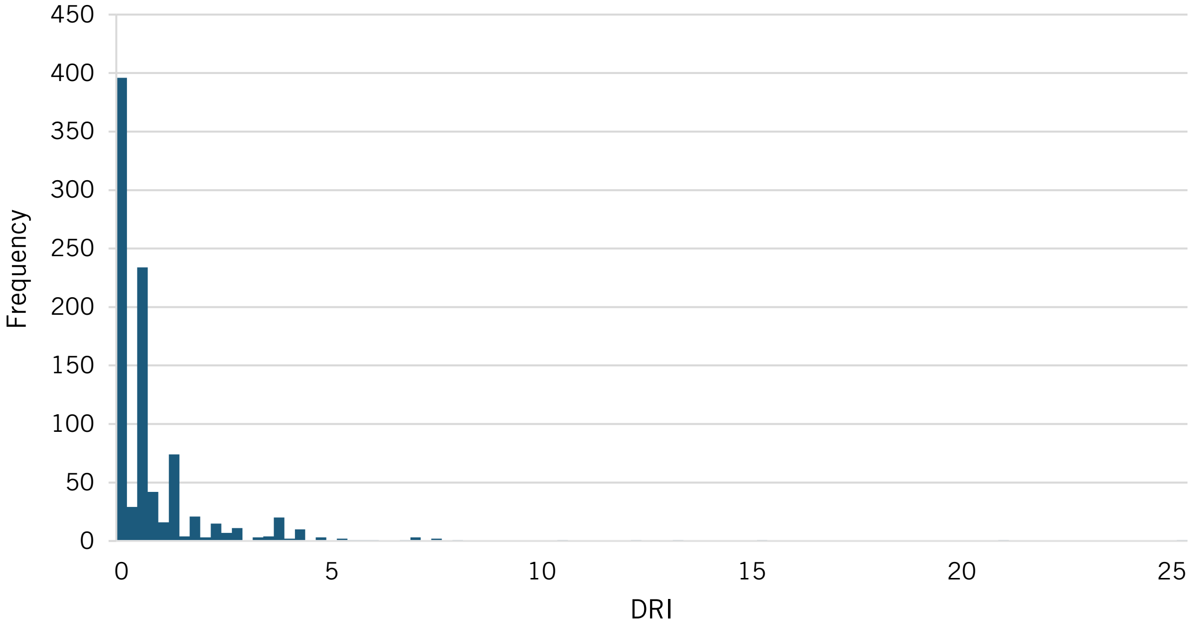
Table 4: Weights used to calculate a policy's data restriction

Weights for Directness *d*		Weights for Type of Data Restricted *k*	
Direct	1.0	National personal data	1.00
Indirect	0.5	Subnational personal data	0.25
		Financial, tax, and banking data	1.25
		Payment data	1.25
		Mapping data	0.50
		Health and genomic data	0.75
		Government data and services	0.50
		ICT and telecommunications data	0.50
		Local cloud (nongovernment)	1.25
		Nonpersonal data framework	1.25
		Other	0.25

DRI is therefore equal to the weighted sum of the data restrictions of the policies in place in country c at time t. These scores provide a common quantitative scale to measure the level of restrictiveness imposed on a country's flow of data, wherein a higher DRI means stricter regulation/limitations on the transfer and usage of data between parties and across borders. The variables d and k are used to scale data restriction values added to DRI based on whether a law enacted is explicit or indirect, and further scaled based on the kinds of data restricted by such laws, since not all data localization laws levy equal economic impacts. The source of laws/policies enacted concerning the restriction of data used in the calculation of DRI scores is "Appendix A: List of Data Localization Measures" of Cory and Dascoli, 2021.[171] The ECIPE's DTE database filtering for laws under the chapter "Data policies" and sub-chapter "Restrictions on cross-border data flows" is also consulted in reviewing data inputs.[172]

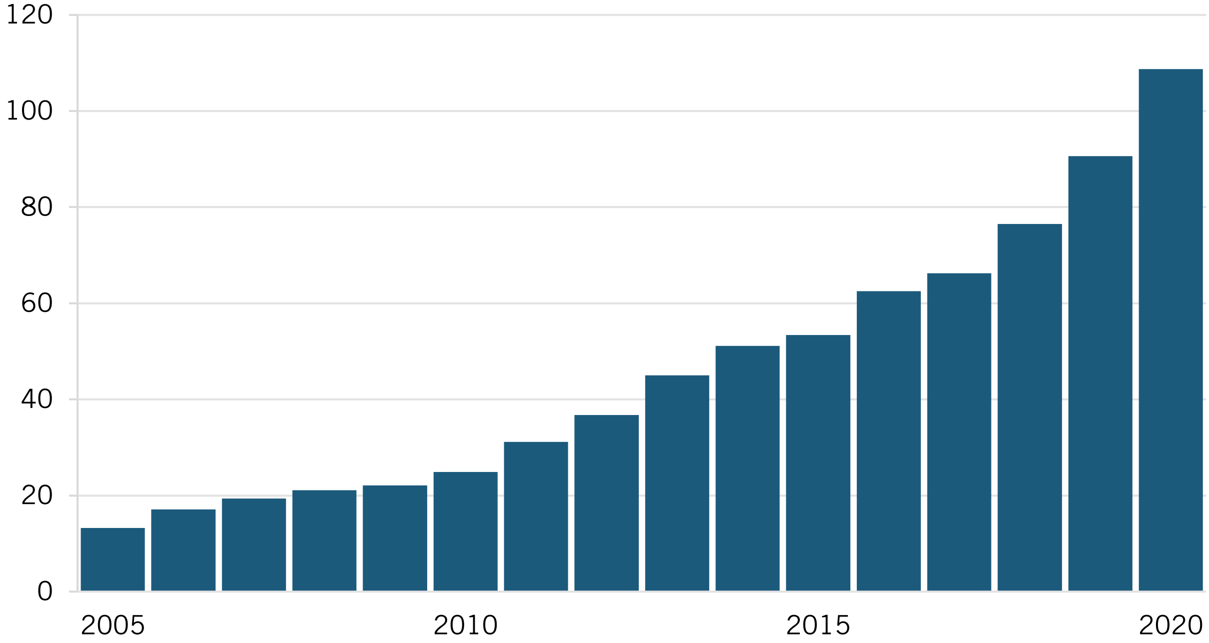
An index suitable for econometric analysis should have enough variation in its distribution to accurately capture effects associated in response variables. The histogram of figure 3 shows the raw distribution of DRI scores between 2005 and 2020.

Figure 3: Distribution of DRI scores, 2005–2020



While DRI has an exponential distribution that is positively skewed, its shape is easily explained by its correlation with year. See figure 4 on the global sum of DRI between 2005 and 2020.

Figure 4: World sum of DRI scores, 2005–2020



Since DRI is recorded in entries of country year and is thus panel data, it is unsurprisingly correlated with year, since data localization policies have increasingly been enacted with each passing year. From 2005 to 2020, the average DRI among 58 countries more than doubled from less than 0.5 to 2.5. This means the average country went from having almost no restrictions on cross-border data flows to approximately two to three restrictions in place during the past 15 years, with a coefficient of variation equal to 196 percent (average observation is 1.96 standard deviations from the mean). These findings in combination indicate sufficient variation in the DRI for statistical analysis.

Comparing This DRI With the DRI in Cory and Dascoli's 2021 Paper

DRI in the 2021 paper was calculated as a weighted average of OECD PMR indicators that are measured on a scale from 0 (least restrictive) to 6 (most restrictive). DRI can therefore only take on a value between 0 and 6.[173] This is very different from for the DRI in this report, which is a weighted sum of data restriction policies in place in a country. For example, China's 2021 DRI is 25.75. DRI for the 2021 paper could only be computed every five years because that's how often the OECD updates its data, whereas the DRI for the 2022 paper was computed for each year.

Crucially, the relationship between DRI as calculated in last year's paper (called "Old DRI") and DRI as calculated in this year's paper (called "New DRI") changes over time. For example, in 2008, New DRI was on average 0.29 times Old DRI. In 2013, it was 0.57 times, and in 2018, it was 0.88 times. Correlation coefficients also changed over time. In 2008, the correlation coefficient between the two measures was only 0.16. In 2013, it was 0.29, and in 2018, it was 0.50. Because there's no consistent relationship between the two measures, readers should avoid making direct comparisons between the two results, other than to say that both are measures of data restriction, and both papers show that data restriction policies have negative economic consequences.

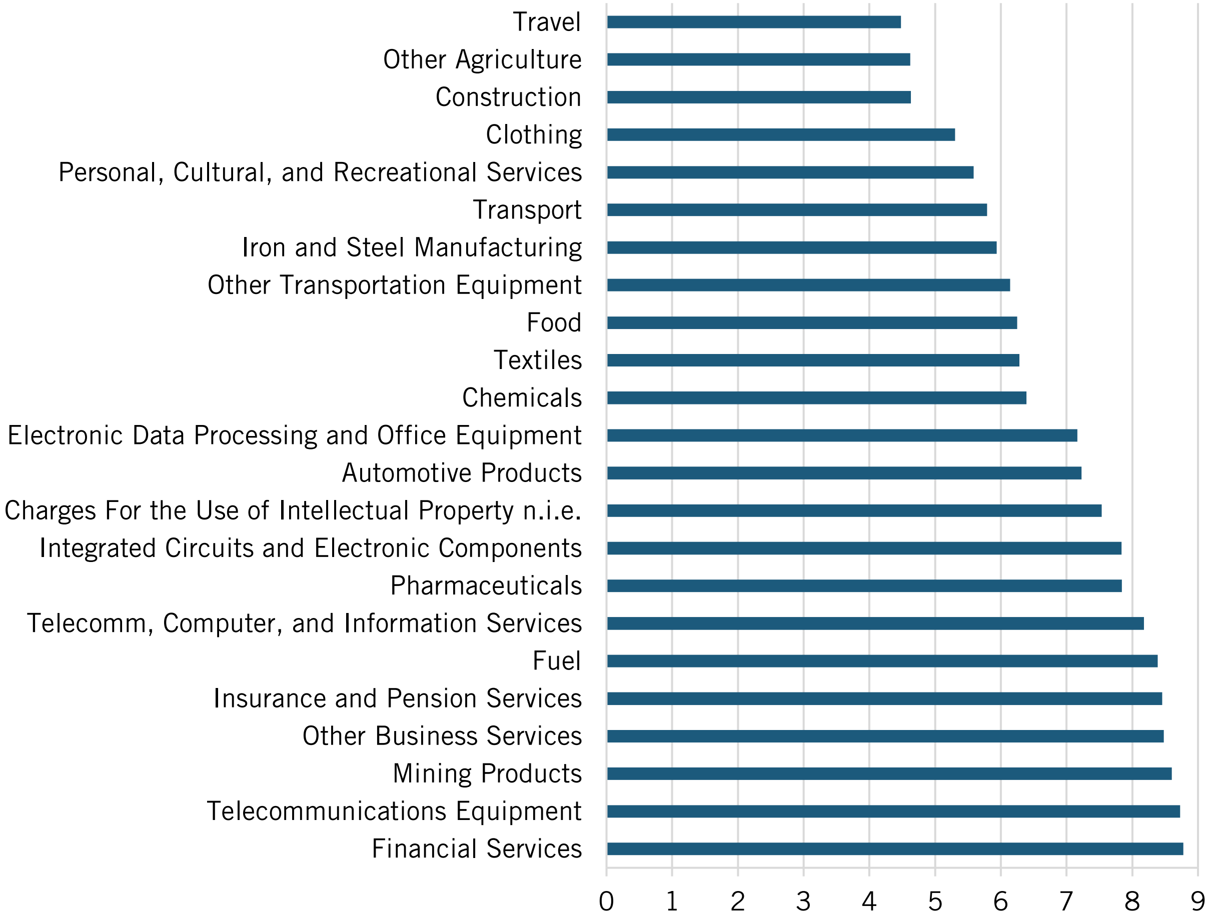
Data-Intensity Modifiers

ITIF's model assumes that restrictions on data flows have greater effects on industries that are more reliant on data and data-related tools and services. To best weigh country-level measurements of DRI at the precision of industry-specific scores, a data-intensity modifier (DIM) is calculated to help correct for bias in the proxy DRI by weighting each downstream industry's linkage with national data restrictiveness for every nonoverlapping industry within the WTO Stats' "International Trade Statistics" products/sectors categorization. Furthermore, this model selects U.S. national data as a reference in a given baseline year for computing industry-specific measurements of DIM to be applied to countries in the sample. However, this approach assumes that all countries have technologies equal to the national estimates for the United States. U.S. Census ICT 2013 Survey data on intangible software expenditure and U.S. Bureau of Labor Statistics data of employment by industry in the same year are gathered to compute the ratios of data-related service expenditures per worker in each industry. ITIF's methodology for calculating DIM is based on best practice as demonstrated by ECIPE's studies on data localization. Employment is recorded in number of workers employed, and noncapitalized software expenditure is recorded in millions of U.S. dollars. DIM is taken as a natural log to align with previous literature on factor intensity. The equation to calculate the DIM of industry i is thus as follows:

$$DIM_i = \ln\left(\frac{Noncapitalized\ Software\ Expenditure_i}{Employment_i}\right)$$

Figure 5 shows the distribution of DIM among the 23 industries in this analysis.

Figure 5: Data-intensity modifier by industry



Composite Index: Data Restrictiveness Linkage

The country-year-level index DRI and industry-level modifier DIM function as components of a composite index at the country-year-industry level. This composite index links the level of data restrictiveness within a country to the level of data reliance faced by an industry to provide a measure of the effective restrictiveness faced by a country's industries due to restrictions on data flows. This DRL is the composite index and final independent variable observed to analyze the economic impact of data localization at the industry level. Conducting this analysis at the level of country-industry-year rather than just country-year provides greater precision in identifying a statistical relationship between data localization and economic performance. Since not every industry relies on data equally, not every industry within a country will be equally impacted by its restrictions on data flows. Therefore, the product of a country's DRI with an industry's DIM gives the DRL of that industry within the country. The equation for the DRL of industry i in country c and year t is as follows:

$$DRL_{c,t,i} = DRI_{c,t} * DIM_i$$

The full list of countries and industries in the DRL are shown in table 5 and table 6.

Table 5: Countries included in the dataset

- Algeria
- Armenia
- Australia
- Azerbaijan
- Bangladesh
- Belgium
- Bosnia and Herzegovina
- Brazil
- Bulgaria
- Cote d’Ivoire
- Canada
- Chile
- China
- Cyprus
- Denmark
- Egypt
- Finland
- France
- Georgia
- Germany
- Ghana
- Greece
- Hong Kong
- India
- Indonesia
- Italy
- Kazakhstan
- Kenya
- South Korea
- Luxembourg
- Malaysia
- Malta
- Mexico
- Moldova
- Netherlands
- New Zealand
- Nigeria
- North Macedonia
- Pakistan
- Poland
- Romania
- Russian Federation
- Rwanda
- Saudi Arabia
- Senegal
- Serbia
- South Africa
- Sweden
- Switzerland
- Turkey
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- Uzbekistan
- Venezuela
- Vietnam

Table 6: Industries included in the dataset

- Financial Services
- Telecommunications Equipment
- Mining Products
- Other Business Services
- Insurance and Pension Services
- Fuel
- Telecommunications, Computer, and Information Services
- Pharmaceuticals
- Integrated Circuits and Electronic Components
- Charges for the Use of Intellectual Property N.I.E.
- Automotive Products
- Electronic Data Processing and Office Equipment
- Chemicals
- Textiles
- Food
- Other Transportation Equipment
- Iron and Steel Manufacturing
- Transport
- Personal, Cultural, and Recreational Services
- Clothing
- Construction
- Other Agriculture
- Travel

Country-Level Data Restrictiveness Linkages

This report calculates the effect an increase in DRL has on total trade and imports, where DRL is an industry-specific measure within a country. Therefore, to calculate the effects data localization policies have on total trade and imports at the country level, country-level DRLs are required. This in turn requires computing country-level DIMs as the weighted average of industry DIMs, where the weights are the industries' share of total trade or imports in the country in question. Thus, two DIMs are computed: one to derive the country-level effects on total trade, and another to derive the country-level effects on imports. Specifically, country c's DIM is calculated as

$$DIM_c = \sum_{i=1}^{23} \omega_{c,i} DIM_i$$

where $\omega_{c,i}$ is share of total trade or imports (depending on the DIM being calculated) of industry i in country c. The total trade and import DIMs for each of the five countries are reported in table 7.

Table 7: Total trade and import DIMs

Country	DIM of Total Trade	DIM of Imports
Bangladesh	6.19	6.59
Hong Kong	7.35	7.24
Indonesia	6.73	6.79
Pakistan	6.87	7.21
Vietnam	6.76	6.83

Selection of Response Variables

As prefaced, ITIF designs its regression models based on best practice demonstrated in quantitative literature on data localization as well as on past analysis from ITIF's 2021 report assessing the economic costs of data localization. However, due to the large sample size of countries included in this econometric exercise, new response variables need to be selected. In its previous analysis, ITIF consulted response variable data from the database EU-KLEMS, which reports data for most OECD countries with only a few Asian ones. In seeking alternative response variable data for this exercise, ITIF consulted data from WTO and UNCTAD, which reports extensive data on economic indicators among a wide range of nations, with special attention to developing economies. However, despite using different data sources to collect response variables, this model still aims to make assessments on economic impacts due to data localization in aspects of trade, prices, and productivity. Data on trade volumes is taken from the WTO Stats database on "International Trade Statistics," which has industry level trade data for all 23 industries for which DIM is recorded for more than 200 economies over a panel of 20+ years. Trade volume is taken as the sum of exports and imports for a given country, industry, and year. However, for data on prices and productivity, no such dataset is publicly available that reports industry-level data in a time series for our sample of 57 nations that needs to include Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam. Instead, data on prices is implied through the dataset "import unit value fixed-base indices - annual (2015=100)." This dataset reports an index of real import unit value for more than 200 economies over more than 20 years. Unit value is determined by both price and quality, rather than price alone. Thus, while not a direct measure of price, import unit value data can still be effective in estimating changes in price.

Productivity is measured by labor productivity (GDP per hour of labor). Labor productivity data comes from the Penn World Table 10.0. Unfortunately, this data is only available for 36 of the 57 countries. Therefore, a subsample was constructed and analyzed to estimate the DRI's effect on productivity. However, the 21 countries excluded from the subsample are all non-high-income countries—though Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam are all still included. Thus, the subsample places more weight on developed countries. Moreover, data is available only up to 2019. Finally, the inclusion of China and India complicate the correlations between labor productivity, DRI, and the size of the economy (as measured by PPP-adjusted GDP), and the econometric model must either control for GDP or exclude these two countries to correct for this triple correlation. This version of the model is therefore discussed in more depth and its results reported after discussion of the four primary models.

Primary Regression Models

The purpose of this regression modeling is to estimate the economic effects of data restriction policies. This econometric exercise performs fixed-effects linear regressions with factor variables for country, year, industry, or combination thereof on the natural logs of response variables to estimate percent changes in economic indicators of trade, prices, and productivity associated with increasing data restrictiveness. In all regression models, a one-year time lag is implemented such that measurements of data restrictiveness are assumed to correspond with the response variables in the following year (since these policies' effects likely do not manifest themselves immediately).

Regression for Trade Volume

$$\ln{(Trade\ Volume)_{c,t,i}} = \beta_0 + \beta_1 DRL_{c,t-1,i} + \alpha_c + \gamma_t + \delta_i + \varepsilon_{c,t,i}$$

Trade volume is the sum of exports and imports. β_0 represents the equation's intercept. β_1 represents the coefficient for the predictor variable DRL. α represents country-level fixed effects, which capture variation on unobserved factors specific to the country of a given observation. γ represents year-level fixed effects, which capture variation on unobserved factors changing over time that are unspecific to country or industry. δ represents industry-level fixed effects, which control for unobserved factors specific to industries. This set of controls is added to help isolate all other factors affecting trade volumes so that the estimated coefficient of DRL is an accurate reflection of the index's statistical relationship to trade volume. ε represents the error term for the given observation.

Regression for Unit Import Value

$$\ln{(Unit\ Import\ Value)_{c,t}} = \beta_0 + \beta_1 DRI_{c,t-1} + \beta_2 GDP\ per\ capita_{c,t} + \gamma_t + \varepsilon_{c,t}$$

Unit import value is a real (fixed base year) index that measures the per-unit value of aggregate imports purchased by a country in a given year. Unit import value is both a reflection of the real price of imports as well as of the quality of those purchased imports. For example, unit import value may increase to report an increase in price of purchased imports. However, a positive change in unit import value can also reflect an improvement for the aggregate bundle of imports purchased by the observed country. β_0 represents the model's intercept. β_1 represents the coefficient of DRI. To control for change in unit import value attributable to a change in quality, this model utilizes GDP per capita instead of country-level fixed effects to observe change in country-specific circumstances that are also changing over time—specifically, whether an increase in unit import value is due to a change in the country's wealth that induces it to purchases higher or lower quality imports. Adding in country fixed effects in this model fails variance inflation factor tests with respect to GDP per capita (variance inflation factor (VIF)score on fixed GDP per capita with country fixed effects is well above 5.0). Lastly, this model still maintains yearly fixed effects to control for other unobservable factors changing over time that are nonspecific to individual countries. ε represents the error term for the given observation.

Regression for Imports

$$\ln{(Imports)_{c,t,i}} = \beta_0 + \beta_1 DRL_{c,t-1,i} + \alpha_c + \gamma_t + \delta_i + \varepsilon_{c,t,i}$$

This regression model selects the natural log of imports as the response variable. $\beta_0$represents the model's intercept. β_1 represents the coefficient of DRL. α represents country-level fixed effects, which capture variation on unobserved factors specific to the country of a given observation. γ represents year-level fixed effects, which capture variation on unobserved factors changing over time that are unspecific to country or industry. δ represents industry-level fixed effects, which control for unobserved factors specific to industries. ε represents the error term for the given observation.

Regression for Nontariff Trade Costs

$$\ln{(Nontariff\ Trade\ Cost)_{c,t}} = \beta_0 + \beta_1 DRI_{c,t-1} + \beta_2 GDP\ per\ capita_{c,t} + \alpha_c + \gamma_t + \varepsilon_{c,t}$$

This regression model selects the natural log of country-aggregated nontariff trade costs as reported by the UNESCAP Trade Costs Database in a given year. $\beta_0$represents the model's intercept. β_1 is the coefficient of DRI. β_2 represents the coefficient of GDP per capita. α represents country-level fixed effects. γ represents yearly fixed effects. ε represents the error term for the given observation.

Estimating the Effects of Data Restrictiveness on Productivity

Given the constraints highlighted in the report, the key model results do not include an analysis of the impact on TFP such as in Cory and Dascoli 2021. Results from an analysis using the Penn World data on labor productivity as a substitute for TFP is provided (table 6). With only a subsample of 34 countries (which increases the influence of high-income countries) and excluding China and India, the model estimates that a one-unit increase in DRI is associated with an approximately 0.7 percent decrease in labor productivity the following year. This finding is statistically significant at the 90 percent level. However, due to the listed constraints, these results are not included in the main results of this study.

Data on labor productivity as measured by PPP-adjusted GDP per hour worked comes from the Penn World Table 10.0. Unfortunately, this data is only available for 36 of the 57 countries, and all the countries excluded from the subsample are non-high-income (and therefore more representative of Bangladesh, Indonesia, Pakistan, and Vietnam). Moreover, data is only available up to 2019. Since data is only available at the country level, the relationship between labor productivity and DRI is considered.

The inclusion of China and India especially complicates the relationships between labor productivity, PPP-adjusted GDP, and DRI. China and India are simultaneously the countries with two of the largest PPP-adjusted GDPs, by far the highest DRIs, and the highest labor productivity growth rates in the subsample. Their inclusion therefore results in an estimated positive relationship between DRI and labor productivity growth, using the following model:

$$\ln{(Output\ per\ Hour)}_{c,t} = \beta_0 + \beta_1 DRI_{c,t-1} + \alpha_c + \gamma_t + \varepsilon_{c,t}$$

When including GDP as a control variable to account for this "triple correlation" that results strictly from the inclusion of China and India, the estimated relationship between DRI and labor productivity predictably turns negative and statistically significant. Specifically, a one-unit increase in DRI is associated with a 0.9 percent decrease in labor productivity, and this result is significant at the 95 percent level. However, the inclusion of GDP as a control variable does not pass the VIF test.

Instead, the model is run excluding China and India as high-leverage outliers. Without these two countries, any statistically significant relationship between GDP and DRI vanishes. The original model (i.e., the model without GDP as a control variable) is then tested. The results are presented in table 6. A one-unit increase in DRI is associated with a 0.7 percent decrease in labor productivity, and this result is statistically significant at the 90 percent level. While the model reports an exceptionally high R^2, it should be noted that this is the result of fixed effects themselves being remarkably good predictors of labor productivity and its growth.

Though the analysis is conducted with only a subsample of 34 countries (which increases the influence of high-income countries) and excludes China and India, ITIF estimates that a one-unit increase in DRI is associated with an approximately 0.7 percent decrease in labor productivity the following year. This is consistent with the original hypothesis and is roughly in line with the findings of Cory and Dascoli 2021, which estimated that a one-unit increase in DRI is associated with a 2.9 percent decrease in TFP (a component of labor productivity) in OECD countries. This finding is also statistically significant at the 90 percent level. However, due to the listed constraints, this model is relegated to this appendix.

Table 6: Regression results: DRI and labor productivity

Dependent Variable	Independent Variable	Coefficient Estimate	Pr(>ltl)	Standard Error	Degrees of Freedom	R^2
ln(Output per Hour)	DRI	-0.007	0.094*	0.0043	460	0.99

*Note: Statistically significant at *** p<0.01, ** p<0.05, * p<0.1*

Table 7: Countries included in subsample for labor productivity regression model

- Australia
- Belgium
- Bangladesh
- Bulgaria
- Brazil
- Canada
- Switzerland
- Chile
- Cyprus
- Germany
- Denmark
- Finland
- France
- United Kingdom
- Greece
- Hong Kong
- Indonesia
- Italy
- South Korea
- Luxembourg
- Mexico
- Malta
- Malaysia
- Netherlands
- New Zealand
- Pakistan
- Poland
- Romania
- Russia
- Sweden
- Turkey
- United States
- Vietnam
- South Africa

Acknowledgments

This report was made possible in part by generous support from Meta. The authors also wish to thank Rob Atkinson and Stephen Ezell and the government officials, journalists, private sector representatives, trade associations, and others who helped build the list of data localization measures and to better understand the changing nature and impact of data localization in these countries and territories. Any errors or omissions are the authors' responsibility alone.

About the Authors

Nigel Cory (@NigelCory) is an associate director covering trade policy at ITIF. He focuses on cross-border data flows, data governance, and intellectual property, and how they each relate to digital trade and the broader digital economy.

Luke Dascoli was formerly the economic and technology policy research assistant at ITIF. He was previously a research assistant in the MDI Scholars Program at the McCourt School of Public Policy's Massive Data Institute. He holds a B.A. in Political Economy from Georgetown University.

Ian Clay is a research assistant for ITIF's Global Innovation team. He holds a B.S. in mathematics and economics from the University of Iowa and an M.S. in economics from the University of St. Andrews in the United Kingdom.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit us at itif.org.

ENDNOTES

[1] Hong Kong is obviously not a country. It is a special administrative region of the People's Republic of China. For simplicity, it'll simply be referred as Hong Kong throughout the report.

[2] Maria Monica Wihardja, "Why e-commerce is key to Indonesia's small businesses," World Economic Forum, November 15, 2021, https://www.weforum.org/agenda/2021/11/why-ecommerce-key-to-indonesias-small-businesses.

[3] Elsadig Musa Ahmed and Rahim Ridzuan, "The Impact of ICT on East Asian Economic Growth: Panel Estimation Approach," Journal of the Knowledge Economy, No4 (December 2013): 540–55, http://link.springer.com/article/10.1007%2Fs13132-012-0096-5.; Stephen Ezell and Robert Atkinson, "The Good, the Bad, and the Ugly (and the Self-Destructive) of Innovation Policy: A Policymaker's Guide to Crafting Effective Innovation Policy" (ITIF, October 2010), https://itif.org/publications/2010/10/07/good-bad-and-ugly-innovation-policy/.

[4] Richard Heeks, "ICT and Economic Growth: Evidence From Kenya," ICTs for Development, June 26, 2011, http://ict4dblog.wordpress.com/2011/06/26/ict-and-economic-growth-evidence-from-kenya/.

5. ICT-based services trade has grown quickly as service tasks are increasingly splintered into discreet components that can be performed and sourced remotely. This is considered the “second unbundling” of international trade, following the geographic separation of consumption and production of physical goods that occurred after the reduction in transportation costs in the 1800s. The first unbundling describes the reduction of transportation costs from the late 1800s, where consumption and production can be geographically separated. Richard Baldwin, “Trade and Industrialisation after globalization’s end unbundling: how building and joining a supply chain are different why it matters” (National Bureau of Economic Research Working Paper 17716, December 2011), http://siteresources.worldbank.org/INTRANETTRADE/Resources/Baldwin_NBER_Working_Paper_17716.pdf.
6. Ibid.
7. World Bank, “Digital Dividends,” (Washington DC: World Bank, January, 2016), https://www.worldbank.org/en/publication/wdr2016.
8. United Nations Conference on Trade and Development, *Digital trade: Opportunities and actions for developing countries* (Geneva: UNCTAD, January, 2022), https://unctad.org/webflyer/digital-trade-opportunities-and-actions-developing-countries.
9. International Telecommunications Union, ICT Development Index 2017 (accessed October 27, 2022), https://www.itu.int/net4/ITU-D/idi/2017/; UNCTAD, “The UNCTAD B2C E-Commerce Index 2020,” https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf; WEF, “Network Readiness Index 2021,” https://networkreadinessindex.org/countries/.
10. “Bangladesh creates fertile ground for e-commerce growth,” UNCTAD, July 25, 2019, https://unctad.org/fr/node/2222.
11. UNCTAD, “Bangladesh Poised to Benefit from E-Commerce Boost after Laying “Exemplary” Digital Foundation,” news release, April 1, 2019, https://unctad.org/press-material/bangladesh-poised-benefit-e-commerce-boost-after-laying-exemplary-digital-foundation.
12. Dr. Abdur Razzaque et al., “Impact of Cross-Border Data Flows Restrictions on Bangladesh Economy” (Research and Policy Integration for Development (RAPID) and CUTS International, July, 2022), https://www.rapidbd.org/wp-content/uploads/2022/07/Impact-of-Cross-Border-Data-Flow-Restrictions-on-Bangladesh-Economy-Report-Two.pdf.
13. Ibid.
14. “Bangladesh creates fertile ground for e-commerce growth,” UNCTAD, July 25, 2019, https://unctad.org/fr/node/2222.
15. UNCTAD, “Bangladesh Poised to Benefit from E-Commerce Boost after Laying ‘Exemplary’ Digital Foundation,” news release, April 1, 2019, https://unctad.org/press-material/bangladesh-poised-benefit-e-commerce-boost-after-laying-exemplary-digital-foundation.
16. Pwc, “Explore opportunities in Hong Kong’s digital ecosystem,” 2022, https://www.pwchk.com/en/services/consulting/publications/explore-opportunities-in-hongkong-digital-ecosystem.html.
17. “LCQ13: Development of digital economy,” news release, February 23, 2022, https://www.info.gov.hk/gia/general/202202/23/P2022022300241.htm.
18. (Translation) “Outline of the People’s Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035” (Translation by the Center for Security and Emerging Technology, March 12, 2021), https://cset.georgetown.edu/publication/china-14th-five-year-plan/; (Translation) “Outline Development Plan for the Guangdong-Hong Kong-Macao Greater Bay Area,” Greater Bay Area Initiative, https://www.bayarea.gov.hk/filemanager/en/share/pdf/Outline_Development_Plan.pdf.

19. Cannix Yau, "Budget 2022-23: more than HK$16 billion earmarked to turn Hong Kong into international innovation and technology hub," *South China Morning Post,* February 23, 2022, https://www.scmp.com/news/hong-kong/hong-kong-economy/article/3168129/budget-2022-23-more-hk16-billion-earmarked-turn.

20. "President Jokowi: Indonesia Has Promising Potential for Digital Economy," Cabinet Secretariat of the Republic of Indonesia, March 1, 2022, https://setkab.go.id/en/president-jokowi-indonesia-has-promising-potential-for-digital-economy/; "Indonesia highly potential to develop digital economy: Jokowi," *Antara News Agency,* September 27, 2016, https://en.antaranews.com/news/106929/indonesia-highly-potential-to-develop-digital-economy-jokowi.

21. Sharon Lam, "Tokopedia neatly channels Indonesia's potential," *Reuters,* January 4, 2021, https://www.reuters.com/article/us-tokopedia-ipo-breakingviews/breakingviews-tokopedia-neatly-channels-indonesias-potential-idUSKBN29A0E8.

22. Florian Hoppe, "e-Conomy SEA Report 2021: Southeast Asia enters its 'digital decade' as the internet economy is expected to reach US$1 trillion in Gross Merchandise Value (GMV) by 2030," news release Bain and Company, November 10, 2021, https://www.bain.com/about/media-center/press-releases/2021/sea-economy-report-2021/.

23. World Bank, "Digital Economy in Indonesia," October 28, 2021, https://www.worldbank.org/en/news/infographic/2021/10/28/digital-economy-in-indonesia; World Bank, *Beyond Unicorns: Harnessing Digital Technologies for Inclusion in Indonesia* (Washington DC: World Bank, July 29, 2021), https://www.worldbank.org/en/country/indonesia/publication/beyond-unicorns-harnessing-digital-technologies-for-inclusion-in-indonesia.

24. In 2019, 62 percent of Indonesian adults in urban areas were connected to the internet compared with 36 percent in rural areas, while it was 20 percent and 6 percent, respectively, in 2011. Indonesians in the top 10 percent of the income distribution were five times more likely to be connected than those in the bottom 10 percent. Ibid.

25. Ibid.

26. alphaBeta, "Unlocking Pakistan's digital potential: The economic opportunities of digital transformation and Google's contribution" (consultancy paper, October, 2021), https://alphabeta.com/our-research/unlocking-pakistans-pkr97-trillion-digital-potential-by-2030/.

27. Mutaher Khan, "Pakistan's startup boom has triggered a "war for talent," *Rest of World,* June, 7, 2022, https://restofworld.org/2022/pakistans-startup-boom-war-for-talent/.

28. From 2005 to 2018, the country's share of ICT services within total services exports increased by around 80 percent. World Bank (2020), Pakistan: Economic Policy for Export Competitiveness. Available at: https://openknowledge.worldbank.org/bitstream/handle/10986/33880/Digital-PakistanEconomic-Policy-for-Export-Competitiveness-A-Business-and-Trade-Assessment.pdf; IT-enabled Services (ITeS) include services that leverage IT to improve or provide business operations. The Pakistani Government specifically includes the following services as ITeS: inbound or outbound call centers, medical transcription, remote monitoring, graphics design, accounting services, HR services, telemedicine centers, data entry operations, locally produced television programs and insurance claims processing. The World Bank (2020), Digital Pakistan: A Business and Trade Assessment, https://openknowledge.worldbank.org/bitstream/handle/10986/33880/Digital-Pakistan-Economic-Policy-for-Export-Competitiveness-A-Business-and-Trade-Assessment.pdf.

29. "Pakistan Telecommunications Authority indicators," accessed November 18, 2022, https://www.pta.gov.pk/en/telecom-indicators.

30. The cost of Internet access has fallen, but high taxes and regulatory restrictions have kept prices relatively high. For example, data usage in Pakistan is subject to a provincial sales tax and federal excise duty at a rate of 19.5 percent and 18.5 percent, respectively. Usage of mobile services is

further charged an additional 14 percent ad valorem tax, bringing the total burden from ad valorem taxes up to 33.5 percent. European Centre for International Political Economy (2019), "Digital Trade Restrictiveness Index," https://globalgovernanceprogramme.eui.eu/wp-content/uploads/2019/09/Digital-Trade-Restrictiveness-Index.pdf; "Concept Project Information Document (PID) - Pakistan: Digital Economy Enhancement Project - P174402 (English)," World Bank, October 20, 2020, http://documents.worldbank.org/curated/en/474421603223324570/Concept-Project-Information-Document-PID-Pakistan-Digital-Economy-Enhancement-Project-P174402.

31. Dan Kopf, "Vietnam is the most globalized populous country in modern history," World Economic Forum, October 15, 2018, https://www.weforum.org/agenda/2018/10/vietnam-is-the-most-globalized-populous-country-in-modern-history/.

32. Pritesh Samuel, "Vietnam's Digital Transformation Plan Through 2025," Dezan Shira and Associates, September 16, 2021, https://www.vietnam-briefing.com/news/vietnams-digital-transformation-plan-through-2025.html/.

33. Lien Hoang, "Vietnam's battle to climb the global value chain," *Nikkei Asia Review,* September 21, 2022, https://asia.nikkei.com/Spotlight/The-Big-Story/Vietnam-s-battle-to-climb-the-global-value-chain.

34. Kevin McSpadden, "Tech startups in Vietnam emerge as beneficiaries of U.S.-China trade war," *NBC News,* September 23, 2019, https://www.nbcnews.com/tech/tech-news/tech-startups-vietnam-emerge-beneficiaries-u-s-china-trade-war-n1057781.

35. "ASEAN Digital Masterplan 2025," https://asean.org/book/asean-digital-masterplan-2025/; "Da Nang declaration: "Creating new dynamism, fostering a shared future," *VOV World,* November 11, 2017, https://vovworld.vn/en-US/news/da-nang-declaration-creating-new-dynamism-fostering-a-shared-future-593565.vov.

36. Pritesh Samuel, "Vietnam's Digital Transformation Plan Through 2025," Dezan Shira and Associates, September 16, 2021, https://www.vietnam-briefing.com/news/vietnams-digital-transformation-plan-through-2025.html/.

37. Fabian Stephany, Otto Kässi, and Vili Lehdonvirta, Online Labour Index 2020: New ways to measure the world's remote freelancing market. Big Data & Society, 8(2). https://doi.org/10.1177/20539517211043240.

38. Dr. Abdur Razzaque et al., "Impact of Cross-Border Data Flows Restrictions on Bangladesh Economy" (Research and Policy Integration for Development (RAPID) and CUTS International, July, 2022), https://www.rapidbd.org/wp-content/uploads/2022/07/Impact-of-Cross-Border-Data-Flow-Restrictions-on-Bangladesh-Economy-Report-Two.pdf.

39. "Concept Project Information Document (PID) - Pakistan: Digital Economy Enhancement Project - P174402 (English)," World Bank, October 20, 2020, http://documents.worldbank.org/curated/en/474421603223324570/Concept-Project-Information-Document-PID-Pakistan-Digital-Economy-Enhancement-Project-P174402.

40. Stephany, Kässi, and Lehdonvirta, Online Labour Index 2020.

41. Ibid. Job categories: Clerical and data entry—customer service, data entry, transcription etc.; creative and multimedia—animation, graphic design, photography; professional services—accounting, legal, project management; sales and marketing support—lead generation, posting ads, search engine optimisation; software development and technology—data science, game development, mobile application development etc.; writing and translation – article writing, copywriting, translation.

42. Ibid. At the moment, they're underrepresented in international gig work in Bangladesh, Indonesia, and Pakistan, only representing 16.9 percent, 35 percent, and 14.6 percent, respectively, of gig workers. And as in Bangladesh, jobs in the information communication sector tend to pay better

than many other sectors. For example, the average monthly earnings of entry level workers in the ICT/ITeS sector varies in the range of BDT 20,000-40,000, according to the IT-ITES Industry Statistics of Bangladesh 2019.

43. Bangladeshi officials engaged several times with counterparts in China (also with the those in United States) as they've developed their draft data protection act.

44. The draft Data Protection Act has used many good components from EU, Singapore, APEC, and OECD. For example, its approach to consent, the lawful bases for processing personal data, recognition of the accountability principle for data controllers, and the approach to data breach notifications. However, at the heart of it are sections 42 and 43 include broad data localization and other cross-border data flow restrictions (e.g., user consent).

45. Data storage: Companies will be required to store sensitive data, user created or generated data, and classified data within Bangladesh territories. Francesco Saturnino, "Bangladesh: Draft Data Protection Act 2022 - what you need to know," October, 2022, https://www.dataguidance.com/opinion/bangladesh-draft-data-protection-act-2022-what-you.

46. M S Siddiqui, "Evaluation of Bangladesh's Data Protection Bill," *The Business Post,* August 31, 2022, https://businesspostbd.com/editorial/2022-08-31/evaluation-of-bangladeshs-data-protection-bill; Zara Rahman, "Bangladesh's upcoming Data Protection Act may suppress, not protect, citizens rights," *Global Voices,* October 23, 2021, https://globalvoices.org/2021/10/23/bangladeshs-upcoming-data-protection-act-may-suppress-not-protect-citizens-rights/.

47. Bangladesh's draft data protection act states (confusingly) that part of the reason for this is to ensure it can be access by Bangladeshi government agencies (such as law enforcement) and to protect it from being accessed by foreign governments.

48. U.S. Department of the Treasury, "Treasury Sanctions Perpetrators of Serious Human Rights Abuse on International Human Rights Day," news release, December 10, 2021, https://home.treasury.gov/news/press-releases/jy0526.

49.. Daniel Castro, "The False Promise of Data Nationalism" (ITIF, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

50. Joshua New, "Sorry, Data Is Not the New Oil," Innovation Files, January 10, 2018, https://itif.org/publications/2018/01/10/sorry-data-not-new-oil/; David Moschella, "Your Data Isn't Gold; It's Not Even Yours" (ITIF, April 1, 2022), https://itif.org/publications/2022/04/01/your-data-isnt-gold-its-not-even-yours/; Robert Atkinson, "IP Protection in the Data Economy: Getting the Balance Right on 13 Critical Issues" (ITIF, January 22, 2019), https://itif.org/publications/2019/01/22/ip-protection-data-economy-getting-balance-right-13-critical-issues/.

51. China is the world leader in data localization. It has dozens of laws and regulations that impact data transfers. See the appendix A of: Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" (ITIF, July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

52. This article is indicative but also doesn't cover the full scale of the shift: Yuan Yang et al., "Silicon Valley weighs whether to leave Hong Kong," *Financial Times,* July 8, 2020, https://www.ft.com/content/9c06e9df-0ca2-485b-8afe-98e51f529373.

53. Xinmei Shen, "Hong Kong saw itself as Asia's data hub, but Beijing's strict cybersecurity rules threaten that status," *South China Morning Post,* November 16, 2021, https://www.scmp.com/tech/policy/article/3156151/hong-kong-saw-itself-asias-data-hub-beijings-strict-cybersecurity-rules; Bingna Guo and Bob Li, "China Issued New Measures for Cybersecurity Review in 2022," White and Case, February 8, 2022,

https://www.whitecase.com/publications/alert/china-issued-new-measures-cybersecurity-review-2022.

54. Zhao Yuning, "English translation of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region," *ECNS.CN,* July 1, 2020, http://www.ecns.cn/news/politics/2020-07-01/detail-ifzxrvxc0874078.shtml.

55. (accessed via the Wayback Machine Internet Archive) Charles Mok, "Council question: Requests made to information and communication technology companies for disclosure and removal of information," May 6, 2020, https://www.charlesmok.hk/legco/council-question-requests-made-to-information-and-communication-technology-companies-for-disclosure-and-removal-of-information/.

56. Bill Bishop, "One country, one Internet?; TikTok; Gaokao; Floods in China; US FBI head on China," Sinocism, July 7, 2020, https://sinocism.com/p/one-country-one-internet-tiktok-gaokao.

57. Indonesia's new data protection bill did not include any data localization provisions. Indonesia also agreed to revise and reduce the impact of potentially restrictive payment data and services regulations. Gayatri Suroyo, Aditya Kalra, and Fanny Potkin, "Exclusive: U.S. helps Mastercard, Visa score victory in Indonesia in global lobbying effort," *Reuters,* October 4, 2019, https://www.reuters.com/article/us-mastercard-usa-lobbying-exclusive/exclusive-u-s-helps-mastercard-visa-score-victory-in-indonesia-in-global-lobbying-effort-idUSKBN1WJ0IX.

58. This attraction is both strategic and tactical. For example, there is also evidence that China has had some rhetorical success in pushing its version of cyberspace governance in Indonesia. Beijing's preferred cyberspace governance language was inserted into a memorandum of understanding between Indonesia's National Cyber and Crypto Agency and the Cybersecurity Administration of China. Plus there is the success that Chinese tech firms have had in Indonesia. Gatra Priyandita, Dirk van der Kley, and Benjamin Herscovitch, "Localization and China's Tech Success in Indonesia" (Carnegie Endowment for International Peace, July, 2022), https://carnegieendowment.org/2022/07/11/localization-and-china-s-tech-success-in-indonesia-pub-87477.

59. "Regulation of Bank Indonesia No. 19/8/PBI/2017 on National Payment Gateway," Bank Indonesia website, November 1, 2017, https://www.bi.go.id/en/peraturan/sistem-pembayaran/Pages/pbi_190817.aspx; "U.S. trade officials, at the request of card networks Mastercard MA.N and Visa V.N, convinced Indonesia late last year to loosen rules governing its new domestic payment network, according to Indonesian government and industry sources, and emails reviewed by Reuters." https://www.reuters.com/article/us-mastercard-usa-lobbying-exclusive/exclusive-u-s-helps-mastercard-visa-score-victory-in-indonesia-in-global-lobbying-effort-idUSKBN1WJ0IX.

60. In a joint press release, providers warned that not only would the revision threaten national data sovereignty; it would tip the balance in favor of international service providers, to the detriment of Indonesian companies that have so far been sheltered from competition. Tanwen Dawn-Hiscox, "Indonesia's data center industry protests data localization reform," *Data Center Dynamics,* November 9, 2018, https://www.datacenterdynamics.com/en/news/indonesias-data-center-industry-protests-data-localization-reform/; "MASTEL Tentang Revisi PP 82/2012," news release, November 6, 2018, https://mastel.id/press-release-mastel-tentang-revisi-pp-82-2012/.

61. Deloitte, "Financial Services Authority and Banking Regulations Update KM No. 4/April/2021), April 22, 2021, https://www2.deloitte.com/content/dam/Deloitte/id/Documents/audit/id-aud-ojk-banking-regulations-updates-apr2021.pdf.

62. Catalin Cimpanu, "Indonesian intelligence agency compromised in suspected Chinese hack," *The Record,* September 10, 2021, https://therecord.media/indonesian-intelligence-agency-compromised-in-suspected-chinese-hack/; For example, in 2021, Indonesia's Ministry of Communication and Information Technology issued Ministerial Circular No. 3/2021 on the use of third-party cloud services for central government agencies for FY2021. The circular sets out 13 security criteria for

third party cloud providers that public agencies can use, among others: they must have at least 2 (two) availability zones at different data center locations in Indonesia; and they must store encryption keys within Indonesia; Government Directive 82 of 2012: Mandates that all electronic system operators who provide "public services" must establish a data center in Indonesia. "Regulation Number 82 of 2012," http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html; Regulation 71 of 2019: Limited the data localization requirements to "public electronic system operators" including public bodies (central or regional executive, legislatures, judicial and any other body set up pursuant to a statute), public entities in banking and financial sectors, and entities that are operating electronic systems on their behalf.

63. Pakistan is in the process of finalizing its draft Personal Data Protection Bill. "IT Ministry to Re-Draft Personal Data Protection Bill," *ProPakistani,* October 13, 2022, https://propakistani.pk/2022/10/13/it-ministry-to-re-draft-personal-data-protection-bill/

64. Pakistan resisted making the draft laws and regulations public. It shows that the process can be just as important as the policies in considering what the government's actual intent is with a data localization and other restrictive policies government officials circulated outdated versions—even among parliamentarians—and then try and bulldoze these through parliamentary committees and the lower house of parliament to avoid debate and scrutiny. Farieha Aziz, "Pakistan's cybercrime law: boon or bane?" Heinrich Boll Stiftung, February 14, 2018, https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane.

65. Riazul Haq, "Cabinet approves amendments to controversial social media rules," *Dawn*, September 29, 2021, https://www.dawn.com/news/1649144.

66. "Pakistan's ISI Snoops On Its Own Citizens In Bid To Control Social Media," *AFP,* May 11, 2019, https://www.ndtv.com/world-news/pakistans-isi-snoops-on-its-own-citizens-in-bid-to-control-social-media-2036085.

67. U.S. Department of State, "2019 Report on International Religious Freedom: Pakistan," https://www.state.gov/reports/2019-report-on-international-religious-freedom/pakistan/; Farieha Azia, "Pakistan's cybercrime law: boon or bane?" (Heinrich Boll Stigtung, the Green Political Foundation, February 14, 2018), https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane

68. Ramsha Jahangir, "Govt's revised internet rules fuel tension with tech firms," *Dawn,* June 29, 2021, https://www.dawn.com/news/1632070.

69. Government of Pakistan, Ministry of Commerce and Textile, *E-commerce Policy Framework of Pakistan* (Islamabad, August, 2019), https://www.commerce.gov.pk/wp-content/uploads/2019/08/Draft-E-Commerce-Policy-Framework-Final-23-8-19.pdf.

70. Ibid.

71. Nigel Cory, "The False Appeal of Data Nationalism: Why the Value of Data Comes From How It's Used, Not Where It's Stored" (ITIF, April 1, 2019), https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where/.

72. Upon completion of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) trade agreement, Vietnam got a transition period to come into compliance. Vietnam has until 2023 to ensure its data localization and governance arrangements are in line with its trade law commitments under the CPTPP, after which other members could initiate a case against it on the basis that it has broken its commitment to not stop cross-border data flow

73. As part of its Draft Decree on Personal Data Protection.

74. In Aug 2022, Decree 53 was issued, giving Vietnam's MPS the authority to request firms to localize data and and set up a local branch or rep office (Article 26) to ensure cooperation with MPA's Cyber Security and Hi-Tech Crime Prevention Department under the Law on Cyber Security. The final Decree in force on Oct 2022, states "[I]n case the service(s) provided is/are used to commit act(s)

that violate(s) the law on cyber security, which has been notified by the Department of Cybersecurity and Hi-Tech Crime Prevention under the Ministry of Public Security and the foreign enterprises have been requested in writing for coordination, prevention, investigations and handling of the same but failed to comply, incompletely complied or prevented, obstructed, disabled or invalidated the effect of the cybersecurity protection measures taken by the cybersecurity task force."

75. In July 2022, Vietnam's Politburo considered a draft personal data protection law that proposed an impact assessment and notification scheme for data exports under the control of MPS. However, there has not been an update since. But prior to this, in November 2021, MPS issued a draft decree stipulating penalties for administrative violations that referenced transfers of personal data out of Vietnam on three conditions: (1) consent of the data subject; (2) records of assessment impact of cross border data transfers of personal data; and (3) a legally binding agreement. Having to meet all three requirements is onerous.

76. It requires all credit and debit payment transactions be processed by a government-owned monopoly "National Payment Corporation of Vietnam," Banking Vietnam website, http://banking.org.vn/2016/national-payment-corporation-of-vietnam/.

77. "Vietnam: Withdraw Problematic Cyber Security Law," Human Rights Watch, June 7, 2018, https://www.hrw.org/news/2018/06/07/vietnam-withdraw-problematic-cyber-security-law; Human Rights Watch, "Viet Nam: New Cybersecurity law a devastating blow for freedom of expression," news release, June 12, 2018, https://www.amnesty.org/en/latest/news/2018/06/viet-nam-cybersecurity-law-devastating-blow-freedom-of-expression/.

78. Article 2 of Vietnam's Cybersecurity law defines "network espionage" as the act of knowingly bypassing a firewall among other things to illegally acquire information, which users may well do to avoid censorship. Article 8 and 15 prohibit "the use of cyberspace" to "prepare, post, and spread information" that "has the content of propaganda opposing the State of the Socialist Republic of Vietnam," or "offends the nation, the national flag, the national emblem, the national anthem, great people, leaders, notable people, and national heroes."

79. Article 2 of Vietnam's Cybersecurity law defines "network espionage" as the act of knowingly bypassing a firewall among other things to illegally acquire information, which users may well do to avoid censorship.

80. Nigel Cory, "Vietnam's cybersecurity law threatens free trade," *Nikkei Asian Review,* August 15, 2018, https://asia.nikkei.com/Opinion/Vietnam-s-cybersecurity-law-threatens-free-trade.

81. Wayne Ma, "Facebook and Google Balance Booming Business with Censorship Pressure in Vietnam," *The Information,* December 10, 2019, https://www.theinformation.com/articles/facebook-and-google-balance-booming-business-with-censorship-pressure-in-vietnam.

82. Ben Shepherd, "Services Trade Policies and Economic Integration: New Evidence for Developing Countries," CEPR Discussion Paper 14181(2019), https://cepr.org/publications/dp14181

83. Ibid.

84. For example: Avi Goldfarb and Daniel Trefler, "AI and International Trade" (National Bureau of Economic Research, working paper No24254, 2018), https://www.nber.org/papers/w24254; Jack Triplett and Barry Bosworth, "Productivity Measurement Issues in Services Industries: Baumol's Disease Has Been Cured," Economic Policy Review, 2003, 9(3): 23–33, https://ssrn.com/abstract=789545.

85. Bert Verschelde, "The Impact of Data Localisation on Vietnam's Economy" (The European Center for International Political Economy, June 2014), https://ecipe.org/publications/impact-data-localisation-vietnams-economy/.

86. Dr. Abdur Razzaque et al., "Impact of Cross-Border Data Flows Restrictions on Bangladesh Economy" (Research and Policy Integration for Development (RAPID) and CUTS International, July,

2022), https://www.rapidbd.org/wp-content/uploads/2022/07/Impact-of-Cross-Border-Data-Flow-Restrictions-on-Bangladesh-Economy-Report-Two.pdf.

87. Nigel Cory and Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them” (ITIF, July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

88. World Bank, *World Development Report* (Washington DC; 2020), https://www.worldbank.org/en/publication/wdr2020.

89. Organization for Economic Cooperation and Development (OECD), *Digital Trade and Market Openness* (Paris: OECD Trade Policy Papers, No217, 2018), https://doi.org/10.1787/1bd89c9a-en.

90. Ibid.

91. Nigel Cory and Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them” (ITIF, July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

92. ITIF’s past modeling used sub-indicators from the OECD PMR Indicators database to develop a proxy measurement of how restrictive a nation’s rules are for cross-border data transfers.

93. Nigel Cory and Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them” (ITIF, July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

94. Cory and Dascoli, “How Barriers to Cross-Border Data Flows are Spreading Globally, What They Cost, and How to Address Them” (Appendix A); Authors’ calculations.

95.. United States Census Bureau, 2013 Information and Communication Technology Survey (Table 3a; accessed February 15, 2022), https://www.census.gov/data/tables/2013/econ/icts/2013-icts.html.

96.. United States Bureau of Labor Statistics, Quarterly Census of Employment and Wages (accessed February 15, 2022), https://data.bls.gov/cew/apps/data_views/data_views.htm#tab=Tables.

97. This is because an industry’s share of imports in a country may not equal its share of total trade (imports plus exports).

98.. World Trade Organization (WTO), International trade statistics, https://stats.wto.org/.

99.. WTO, International trade statistics (Merchandise import unit value fixed-base indices – annual (2015=100); accessed March 30, 2022), https://stats.wto.org/.

100.. UNESCAP, ESCAP-World Bank trade cost database (accessed March 30, 2022), https://www.unescap.org/resources/escap-world-bank-trade-cost-database.

101.. University of Groningen Growth and Development Center, Penn World Table 10.0 (TFP at constant national prices; accessed August 28, 2022), https://www.rug.nl/ggdc/productivity/pwt/?lang=en.

102. “Unofficial 1st Draft English Text of Proposed Data Protection Bill, 2022” July 16, 2022, https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/6c9773a2_7556_4395_bbec_f132b9d819f0/Data%20Protection%20Bill%20en%20V13%20Unofficial%20Working%20Draft%2016.07.22.pdf.

103. Nigel Cory, “The False Appeal of Data Nationalism: Why the Value of Data Comes From How It’s Used, Not Where It’s Stored” (ITIF, April 1, 2019), https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where/; UNCTAD, *Digital trade: Opportunities and actions for developing countries* (Geneva: January 7, 2022), https://unctad.org/webflyer/digital-trade-opportunities-and-actions-developing-countries.

104. For example, "[F]irms in Pakistan and Bangladesh cite connectivity and IT backbone a significant hurdles for cross-border e-commerce." Sanjay Kathuria, Arti Grover, Viviana Maria Eugenia Perego, Aaditya Mattoo, and Pritam Banerjee, *Unleashing E-Commerce for South Asian Integration* (Washington, DC: 2019), https://elibrary.worldbank.org/doi/abs/10.1596/978-1-4648-1519-5.

105. Robert Atkinson, "How ICT Can Drive Growth in Emerging Economies," Innovation Files, August 10, 2015, https://www.innovationfiles.org/ict-can-drive-growth-emerging-economies/; Jason Dedrick, ViJay Gurbaxani, and Kenneth LKraemer, "Information Technology and Economic Performance: A Critical Review of the Empirical Evidence," ACM Computing Surveys 35, no. 1 (March 2003), 1; For several of the numerous literature surveys, see: Mirko Draca, Raffaella Sadun, and John van Reenen, "Productivity and ICT: A Review of the Evidence" (discussion paper no749, Centre for Economic Performance, August 2006), http://eprints.lse.ac.uk/4561/; Tobias Kretschmer, "Information and Communication Technologies and Productivity Growth: A Survey of the Literature," OECD Digital Economy Papers, no. 195 (2012), http://dx.doi.org/10.1787/5k9bh3jllgs7-en; M. Cardona, T. Kretschmer, and T. Strobel, "ICT and Productivity: Conclusions from the Empirical Literature," Information Economics and Policy 25, no. 3 (September 2013): 109–125, doi:10.1016/j.infoecopol.2012.12.002.

106. Nick Wallace, "Double Consent Rule for Sharing Data Would Be Useless" (Center for Data Innovation, October 31, 2016), https://www.datainnovation.org/2016/10/double-consent-rule-for-sharing-datauseless/.

107. Daniel Castro and Travis Korte, "Open Data in the G8: A Review of Progress on the G8 Open Data Charter" (Information Technology and Innovation Foundation, Center for Open Data, March 17, 2015), http://www2.datainnovation.org/2015-open-data-g8.pdf.

108. Robert Atkinson, "IP Protection in the Data Economy: Getting the Balance Right on 13 Critical Issues" (Information Technology and Innovation Foundation, January, 2019), /publications/2019/01/22/ip-protection-data-economy-getting-balance-right-13-critical-issues

109. Nick Wallace and Daniel Castro, "The State of Data Innovation in the EU" (Center for Data Innovation, October 9, 2017), https://www.datainnovation.org/2017/10/the-state-of-data-innovation-in-the-eu-2/; Daniel Castro, Joshua New, and John Wu, "The Best States for Data Innovation" (Center for Data Innovation, July 31, 2017), https://www.datainnovation.org/2017/07/the-best-states-for-data-innovation/.

110. Also, Recital 23 of the EU's GDPR mentions that factors such as the use of a language or a currency generally used in the jurisdiction will be taken into consideration in determining legal nexus.

111. ISO 27001/27002 are widely adopted global security standards that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments appropriate to ever-changing threat scenarios. ISO27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002. It also provides a set of additional controls and associated guidance intended to address public cloud personal data protection requirements not addressed by the existing ISO 27002 control set.

112. Introduced in 2020 by the Australian Cyber Security Centre (ACSC), the Information Security Registered Assessors Program (IRAP) forms the basis for government entities to conduct a risk-based review to determine if the cloud service provider (CSP) and its cloud services are suitable for handling its data. It is a voluntary process and IRAP assessments are not mandatory for agencies. Different protocols apply depending on the security rating of an agencies systems. "IRAP Policy and Procedures 11/2020, Australian Signals Directorate Information Security Registered Assessors Program," https://www.cyber.gov.au/sites/default/files/2020-12/IRAP%20Policy%20and%20Procedures.pdf.

113. "Kuwait, Bahrain sign cloud computing MOU," Kuwait News Agency, October 5, 2018, https://www.kuna.net.kw/ArticleDetails.aspx?id=2749760&language=en.

114. “European Commission: e-evidence,” https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime/e-evidence_en; Vanessa Franssen, “The European Commission’s E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?” European Law Blog, October 12, 2018, https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/.

115. “Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences,” December 10, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN; U.S. Department of Justice, “Joint US-EU Statement on Electronic Evidence Sharing Negotiations,” news release, September 26, 2019, https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations.

116. A good review of issues in many of countries in the report. ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance in Asia and the Pacific: Experiences in 31 Jurisdictions* (Manila: 2017), https://www.oecd.org/corruption/ADB-OECD-Mutual-Legal-Assistance-Corruption-2017.pdf.

117. “Toolkit: Cross-Border Access to Electronic Evidence,” Internet Jurisdiction Policy Network, March, 2021, https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-21-103-Toolkit-Cross-border-Access-to-Electronic-Evidence-2021.pdf.

118. Brad Wiegmann, “Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights” (testimony to the Subcommittee on Crime and Terrorism Committee on the Judiciary United States Senate, May 24, 2017), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf.

119. ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance in Asia and the Pacific: Experiences in 31 Jurisdictions* (Manila: 2017), https://www.oecd.org/corruption/ADB-OECD-Mutual-Legal-Assistance-Corruption-2017.pdf.

120. Pakistan’s Ministry of Information Technology and Telecommunication, “Ministry of Information Technology and Telecommunication has approached the Interior Ministry to finalize viewpoint on the matter of signing Mutual Legal Assistance Treaty and Budapest Convention with the United States of America,” news release, https://moitt.gov.pk/NewsDetail/YWIzMTgxZGItMmM3NS00ZGI4LTljNTEtNzlmNDljNGE1Njll.

121. U.S. Department of State, “Treaties and Agreements,” March 7, 2012, https://2009-2017.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm.

122. Panitia Khusus, “Mutual Legal Assistance Treaty between Indonesia-Swiss Approved,” The House of Representatives of the Republic of Indonesia, March 7, 2020, https://www.dpr.go.id/en/berita/detail/id/29280/t/javascript.

123. “Treaty on Mutual Legal Assistance in Criminal Matters,” https://asean.org/our-communities/asean-political-security-community/rules-based-people-oriented-people-centred/treaty-on-mutual-legal-assistance-in-criminal-matters/.

124. “Cybercrime: Towards a Protocol on evidence in the cloud,” Council of Europe, June 8, 2017, https://www.coe.int/en/web/cybercrime/-/cybercrime-towards-a-protocol-on-evidence-in-the-cloud.

125. “Council of Europe: Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY,” https://www.coe.int/en/web/cybercrime/parties-observers.

126. Mike Gallaher and Nigel Cory, “4 key steps to support cross-border payments and digital trade growth,” World Economic Forum, June 4, 2020, https://www.weforum.org/agenda/2020/06/action-on-cross-border-payments-will-support-digital-trade-growth; “Connecting Digital Economies: Policy Recommendations for Cross-Border Payments,” World Economic Forum, June, 2020,

https://itif.org/publications/2020/06/02/connecting-digital-economies-policy-recommendations-cross-border-payments/.

127. Monetary Authority of Singapore, “MAS Establishes Payments Council,” Press release, 2 August 2017.
128. World Economic Forum, “Digital ASEAN,” 2018, https://www.weforum.org/projects/digital-asean.
129. “Bangladesh: Country Report,” Telenor, March, 2017, https://www.telenor.com/binaries/sustainability/responsible-business/handling-access-requests-from-authorities/Authority-Request-Legal-Overview_March-2017-bangladesh.pdf;
130. Bangladesh Bank Company Act, (1991), https://www.findevgateway.org/paper/1991/01/bank-company-act-bangladesh-1991
131. “Unofficial 1st Draft English Text of Proposed Data Protection Bill, 2022” July 16, 2022, https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/6c9773a2_7556_4395_bbec_f132b9d819f0/Data%20Protection%20Bill%20en%20V13%20Unofficial%20Working%20Draft%2016.07.22.pdf.
132. Global Data Alliance, “Comments to the People’s Republic of Bangladesh on The Cross-Border Policy Implications of the Draft Data Protection Act of 2022” (industry submission, September 2022), https://globaldataalliance.org/wp-content/uploads/2022/09/09072022gdabgdpa.pdf.
133. “Draft Personal Data Protection Act 2020,” October, 2020, https://mcusercontent.com/3db897db1506081dc74dd704d/files/d7abfc5b-3035-4fea-9ae8-6095e92c7c5f/_DRAFT_Personal_Data_Protection_Act_2020.pdf.
134. Global Data Alliance, “Comments to the People’s Republic of Bangladesh on The Draft Cloud Computing Policy,” (industry submission, May 2021), https://www.globaldataalliance.org/downloads/05122021gdabdcloudpol.pdf.
135. Bangladesh Draft Cloud Computing Policy.
136. Office of the Privacy Commissioner for Personal Data Hong Kong, “Guidance on Personal Data Protection in Cross-border Data Transfer,” https://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_crossborder_e.pdf; Richard Bates and Nicholas Blackmore, “Insurance Connect: Data privacy challenges for Hong Kong insurers setting up Greater Bay Area Service Desks,” Kennedys, October 7, 2020, https://kennedyslaw.com/pt/thought-leadership/article/insurance-connect-data-privacy-challenges-for-hong-kong-insurers-setting-up-greater-bay-area-service-desks/.
137. Alun John, “Hong Kong regulator considers easing strict data storage rules – sources,” *Reuters,* March 10, 2020, https://www.reuters.com/article/hongkong-regulators-cloud/hong-kong-regulator-considers-easing-strict-data-storage-rules-sources-idUSL3N2AQ1XA.
138. Selina Cheng, “Hong Kong Policy Address: New cybersecurity law to protect ‘critical infrastructure,’” Hong Kong Free press, October 6, 2021, https://hongkongfp.com/2021/10/06/hong-kong-policy-address-new-cybersecurity-law-to-protect-critical-infrastructure/.
139. Arjun Kharpal, “China to make some firms undergo a data security review before listing overseas,” *CNBC,* January 4, 2022, https://www.cnbc.com/2022/01/04/china-to-require-data-security-review-on-some-firms-before-ipo-abroad.html.
140. Xiaomeng Lu, “What Does Hong Kong’s National Security Law Mean for Tech Companies?,” *The Diplomat,* June 12, 2020, https://thediplomat.com/2020/06/what-does-hong-kongs-national-security-law-mean-for-tech-companies/.
141. Angeli Datt, “The Impact of the National Security Law on Media and Internet Freedom in Hong Kong,” Freedom House, September 8, 2021, https://freedomhouse.org/article/impact-national-security-law-media-and-internet-freedom-hong-kong.

142. Government of the Hong Kong SAR, “Implementation Rules for Article 43 of the Law of the People’s Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region gazette,” July 6, 2020 https://www.info.gov.hk/gia/general/202007/06/P2020070600784.htm; Patrick Frater, “National Security Law Expands Online Reach of Hong Kong Police,” Variety, July 7, 2020, https://variety.com/2020/digital/asia/national-security-law-online-hong-kong-police-1234699833/.

143. For example: Adam Au, “What Hong Kong can learn from the European Union to enable better data sharing in the Greater Bay Area,” *South China Morning Post,* January 20, 2021, https://www.scmp.com/comment/opinion/article/3118273/what-hong-kong-can-learn-european-union-enable-better-data-sharing.

144. Xinmei Shen, “Hong Kong in talks with Beijing to ease cross-border data flow as new rules threaten city’s gateway status,” *South China Morning Post,* July 24, 2022, https://www.scmp.com/tech/policy/article/3186094/hong-kong-talks-beijing-ease-cross-border-data-flow-new-rules-threaten; Xiaomeng Lu, “Is China Changing Its Thinking on Data Localization?,” *The Diplomat,* June 4, 2020, https://thediplomat.com/2020/06/is-china-changing-its-thinking-on-data-localization/.

145. Indonesia – Asia Internet Coalition, submission, https://aicasia.org/category/regions/indonesia.

146. Asia Internet Coalition, “Letter: Follow-up on the Government Regulation No. 71/2019 on Electronic System and Transaction (“GR 71”) and Industry Request for Amended Regulation,” October 1, 2020, https://aicasia.org/wp-content/uploads/2020/10/AIC-letter-to-Kominfo_Government-Regulation_01102020.pdf.

147. “Indonesia Now Has a Specific E-commerce Regulation,” HHP Law Firm, December 2019, https://www.bakermckenzie.com/en-/media/files/insight/publications/2019/12/ma-taxtrad--indonesia-now-has-a-specific-ecommerce-regulation-dece-2019.pdf.

148. “Regulation of Bank Indonesia No. 19/8/PBI/2017 on National Payment Gateway,” Bank Indonesia website, November 1, 2017, https://www.bi.go.id/en/peraturan/sistem-pembayaran/Pages/pbi_190817.aspx.

149. Gayatri Suroyo, Aditya Kalra, and Fanny Potkin, “Exclusive: U.S. helps Mastercard, Visa score victory in Indonesia in global lobbying effort,” *Reuters,* October 4, 2019, https://www.reuters.com/article/us-mastercard-usa-lobbying-exclusive/exclusive-u-s-helps-mastercard-visa-score-victory-in-indonesia-in-global-lobbying-effort-idUSKBN1WJ0IX.

150. “Indonesia sets new rules on payments systems,” *Reuters,* January 8, 2021, https://www.reuters.com/article/indonesia-economy-payments/indonesia-sets-new-rules-on-payments-systems-idUSL4N2JJ1HN.

151. Indonesia’s Regulation on Information Technology Risk Management requires foreign banks and payments networks to locate data centers and process payments in the economy “Comments in Response to Executive Order Regarding Trade Agreements Violations and Abuses,” The Information Technology Industry Council, 2017, https://www.itic.org/dotAsset/9d22f0e2-90cb-467d-81c8-ecc87e8dbd2b.pdf.

152. Deloitte, “Financial Services Authority and Banking Regulations Update KM No. 4/April/2021,” https://www2.deloitte.com/content/dam/Deloitte/id/Documents/audit/id-aud-ojk-banking-regulations-updates-apr2021.pdf; (Translation) “Implementation of Risk Management in Use of IT by Non-Bank Financial Service Institutions,” 2021, https://www.ojk.go.id/id/regulasi/Documents/Pages/Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-oleh-Lembaga-Jasa-Keuangan-Nonbank/pojk%204-2021.pdf.

153. Government of Pakistan, Ministry of Commerce and Textile, E-commerce Policy Framework of Pakistan (Islamabad, August, 2019), https://www.commerce.gov.pk/wp-content/uploads/2019/08/Draft-E-Commerce-Policy-Framework-Final-23-8-19.pdf.

154. Government of Pakistan, ‘Pakistan Cloud First Policy,” February 25, 2022, https://moitt.gov.pk/SiteImage/Misc/files/Pakistan%20Cloud%20First%20Policy-Final-25-02-2022.pdf.

155. Kalbe Ali, “Federal cabinet approves Cloud First Policy, Personal Data Protection Bill,” February 16, 2022, https://www.dawn.com/news/1675330; “Pakistan: Federal Cabinet approves Draft Personal Data Protection Bill,” February 28, 2022, https://www.dataguidance.com/news/pakistan-federal-cabinet-approves-draft-personal-data.

156. “Personal Data Protection Bill 2021,” https://moitt.gov.pk/SiteImage/Misc/files/25821%20DPA%20Bill%20Consultation%20Draft_docx.pdf; Asian Internet Coalition, “Submission on Pakistan’s Data Protection Bill 2021,” September 22, 2021, https://aicasia.org/wp-content/uploads/2021/10/Pakistans-Personal-Data-Protection-Bill-2021-9-22.pdf.

157. Ibid.

158. Ibid.

159. Ibid.

160. Farieha Aziz, “Pakistan’s cybercrime law: boon or bane?,” Heinrich Boll Stifung, February 14, 2018, https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane.

161. “President passes ordinance to regulate social media, as Naseem warns against spreading ‘fake news’,” February 20, 2022, https://www.pakistantoday.com.pk/2022/02/20/president-passes-ordinance-to-regulate-social-media-as-naseem-warns-against-spreading-fake-news/; Asia Internet Coalition, “Letter: Industry comments on the Amendment - Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules,” June 28, 2021, https://aicasia.org/wp-content/uploads/2021/06/Asia-Internet-Coalition-AIC-Industry-comments-on-the-Amendment-Removal-and-Blocking-of-Unlawful-Online-Content-Procedure-Oversight-and-Safeguards-Rules_28-June-2021.pdf.

162. Riazul Haq, “Cabinet approves amendments to controversial social media rules,” *Dawn,* September 29, 2021, https://www.dawn.com/news/1649144.

163. Ramsha Jahangir, “Govt’s revised internet rules fuel tension with tech firms,” *Dawn,* June 29, 2021, https://www.dawn.com/news/1632070.

164. Asia Internet Coalition, “Joint industry letter on Decree No. 53/2022/ND-CP detailing the implementation of a number of articles of the Law on Cybersecurity (LOCS),” September 2022, https://aicasia.org/2022/09/09/vietnam-asia-internet-coalition-aic-submits-joint-industry-letter-on-decree-no-53-2022-nd-cp-detailing-the-implementation-of-a-number-of-articles-of-the-law-on-cybersecurity-locs-sept-2022/.

165. Ibid.

166. Asia Internet Coalition, “Letter:) Comments and Recommendations on the draft decree amending Decree 72 on Management, Provision, and Use of Internet Services and Online Information (“Decree 72 or Draft Decree”),” January 3, 2022, https://aicasia.org/wp-content/uploads/2022/01/Asia-Internet-Coalition-AIC-Comments-and-Recommendations-on-Amended-Decree-on-Management-Provision-and-Use-of-Internet-Services-and-Information-Content-Online-22Decree-7222_English-updated.pdf.

167. Ibid.

168. “Vietnam Issues New Draft Decree on Personal Data Protection,” Tilleke and Gibbons, February 25, 2021, https://www.tilleke.com/insights/vietnam-issues-new-draft-decree-on-personal-data-protection/.

169. “National Payment Corporation of Vietnam,” Banking Vietnam website, http://banking.org.vn/2016/national-payment-corporation-of-vietnam/.

170.. Organization for Economic Cooperation and Development (OECD), “Digital Services Trade Restrictiveness Index,” (OECD, 2022), https://stats.oecd.org/Index.aspx?DataSetCode=STRI. Martina F. Ferracane and Erik van der Marel, “Do Data Policy Restrictions Inhibit Trade in Services?” (European Center for International Political Economy (ECIPE), 2018), https://ecipe.org/publications/do-data-policy-restrictions-inhibit-trade-in-services/. Bauer et al., “Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization” (Global Commission on Internet Governance, 2016), https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf.

171. Nigel Cory and Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them” (ITIF, July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

172.. ECIPE, Digital Trade Estimates (Data policies; accessed February 23, 2022), https://ecipe.org/dte/database/.

173. Nigel Cory and Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them” (ITIF, July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.