ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

700 K Street NW Suite 600
Washington, DC 20001

COMMENTS OF ITIF

Before the

U.S. House Committee on Ways and Means, Subcommittee on Trade

Washington, D.C.

In the Matter of:	)	Reforming the Generalized System of Preferences to Safeguard U.S. Supply Chains and Combat China

September 20, 2023

CONTENTS

Forward 1
Introduction 1
The Many and Growing Types of Digital Trade Barriers 3
Digital Trade Barriers Impact U.S. Competitiveness, Exports, and Workers, Especially for SMEs 5
Data Localization Enables Digital Authoritarianism 6
Trade Data Show GSP Provides the United States With Critical Leverage to Roll Back Digital Trade Barriers 7
U.S. Digital Trade with GSP Countries is Growing. Digital Trade Restrictions Would Prevent Future Growth in Large, Growing Digital Economies 8
Current and Potential Legislative Proposals: Add an Explicit Digital Trade Criterion and New Transparency and Reporting Requirements to Ensure GSP Becomes an Effective Digital Trade Tool 9
- Congressman LaHood's Digital Trade for Development Act 10
- The Senate's Trade Preferences and American Manufacturing Competitiveness Act of 2021 10
- Reform GSP to Ensure a Clearer and Stronger Role for Congress in GSP Oversight 11

Conclusion 12
Appendix: Case Studies of GSP Recipients and Digital Trade Barriers 13
- Algeria 13
- Brazil 13
- Cambodia 13
- Cote-d'Ivoire 14
- Egypt 14
- Ghana 14
- Indonesia 14
- Kazakhstan 17
- Kenya 18
- Nigeria 18
- Pakistan 19
- The Philippines 20
- Rwanda 20
- Senegal 20
- Sri Lanka 20
- South Africa 21
- Thailand 21
- Uganda 21
- Uzbekistan 21

Endnotes 22

FORWARD

The Information Technology and Innovation Foundation (ITIF) appreciates the House Ways and Means Trade Subcommittee's invitation to testify regarding the proposal to add a criterion for digital trade barriers to the Generalized System of Preferences program and the importance of digital trade to the U.S. economy. ITIF is a nonpartisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity internationally, in Washington, and the states. Recognizing the vital role of technology in ensuring prosperity, ITIF focuses on innovation, productivity, and digital economy issues. We have long been involved in the digital trade debate, advocating for policies that support the free flow of data across borders as essential to global trade and commerce.

INTRODUCTION

At the heart of the United States' Generalized System of Preferences (GSP) lies a recognition that free trade supports economic growth in developing countries, and such trade can be mutually beneficial. However, several developing countries that benefit from GSP have enacted (with many more considering) digital trade barriers that hurt U.S. firms and workers and contravene the GSP's requirement that they provide reasonable and fair market access to U.S. firms and their goods and services. Many countries enact digital trade barriers that specifically target U.S. firms and their digital goods and services. Congress should update the GSP by creating an explicit criterion for assessing digital trade barriers and use this criterion to evaluate and, if needed, revoke GSP status. In 2018, ITIF first proposed this change in "Time to Restrict GSP Benefits to Fight Trade Mercantilism."[1]

Global trade is increasingly digital, and the U.S. is home to many of the world's leading firms that depend on the ability to transfer data and use digital technologies to engage in digital trade to support and grow their U.S. operations, workforce, and research and development programs. Digital trade—the cross-border transfer of data, products, or services by electronic means—involves firms of all sizes in every sector, not just big tech—in 2021, the digital economy accounted for an estimated 10.3 percent of U.S. GDP).[2] U.S. exports of all services that can be delivered digitally, including business services, were $594 billion in 2021 (75 percent of total U.S. services exports), an increase of 33 percent since 2016.[3]

Just as global digital trade has grown, so have barriers to it. As policymakers in a growing number of countries realize there is a global race for innovation advantage, they're turning to new behind-the-border barriers to disadvantage U.S. firms and their digital products in favor of local ones. For example, the number of forced local data storage/residency requirements (a concept known as data-localization) has more than doubled in four years. In 2017, 35 countries had implemented 67 such barriers. Now, 62 countries have imposed 144 restrictions—and dozens more are under consideration.4 Data localization is a common barrier, but there are many more (explained below), so digital protectionism is spreading in many ways. However, data localization is not only a trade barrier, but it also can be a human rights issue as it enables China-like digital authoritarianism by making it easier for governments to access and control data for social and political purposes.

Digital protectionism is spreading as current global trade rules at the World Trade Organization (WTO) are largely from the pre-Internet era and thus don't apply or were written in such a way that it's uncertain as to whether they apply. Countries have taken advantage of this vacuum and uncertainty to enact barriers to

digital trade. China is the world leader in digital protectionism, enacting dozens of different data localization and other restrictions. There are ongoing e-commerce negotiations at the WTO; however, it's highly uncertain whether these will lead to ambitious and enforceable rules against digital protectionism. Bilateral and regional trade agreements among like-minded countries are the main effort to help build new norms, rules, and agreements that support digital trade. However, new trade agreements are not the only way to push back against digital protectionism. The United States has considerable leverage in using GSP as a tool to ensure a range of important trading partners do not succumb to digital protectionism; at least not while also benefiting from tariff-free access to the U.S. market.

While the GSP only applies to a subset of developing countries, its duty-free access to U.S. markets represents a major benefit to many trading partners that clearly do not provide fair and reasonable market access or treatment of U.S. firms and their goods and services. For example, in 2019, $2.7 billion of Indonesia's exports (13.6 percent of total exports) benefited from GSP duty-free access. Yet, it has enacted, and is considering further, digital trade restrictions that disadvantage U.S. firms and products. Similarly, in 2019, $346 million of Pakistan's exports (8.8 percent of total exports) to the United States benefited from GSP tariff-free market access, yet it, too, is considering a range of restrictive digital trade barriers. While U.S. digital exports to both countries (e.g., U.S. digital trade exports to Indonesia were worth $222 million in 2021) are not comparable to major U.S. trading partners, their potential to tap into these large, growing markets will be cut off if these countries are allowed to enact barriers to digital trade. All the while, these countries continue to increase their GSP-eligible exports. From 2000 to 2019, Indonesia's GSP-eligible exports increased by nearly 100 percent, while Pakistan's increased by 271 percent.

The United States should use updated GSP criteria as another tool to force these countries to roll back digital trade barriers. In doing so, the goal is not the punitive removal of these benefits for developing countries but to fully enact the rules already clearly set out as part of the GSP program, which the beneficiary countries have long been aware of, as they have enjoyed the corresponding benefits without fulfilling their accompanying obligations. Ultimately, GSP aims to convince these countries that abandoning mercantilist-oriented practices will produce stronger economic growth outcomes for these countries over the long term, which, after all, is the core goal of the GSP program anyway.

Adding an explicit digital trade criterion would build on past reforms to keep GSP relevant. After the GSP's creation in 1974, the Trade and Tariff Act of 1984 linked intellectual property rights enforcement and trade by making them actionable under Section 301 of the 1974 Trade Act, which meant the U.S. government could unilaterally raise tariffs against trading partners that maintain "unjustifiable or unreasonable" restrictions against U.S. trade. More recently, the Trade Facilitation and Trade Enforcement Act of 2015 required the USTR to develop an action plan and set of benchmarks for countries with the most serious intellectual property rights deficiencies on the Section 301 Priority Watch List. A year after an action plan is developed, USTR can report to the U.S. president that a country has not substantially complied with the benchmarks and recommend appropriate action. The United States still has much more to do to fully enforce GSP's intellectual property criterion, given the long and detailed list of countries that the United States lists in its annual Special 301 report on global intellectual property protection and enforcement.

This written testimony proceeds as follows. Firstly, it analyzes the many and growing types of digital trade barriers. Secondly, it analyzes the economic impact digital trade barriers have on the U.S. economy. Thirdly,

it analyzes how digital protectionism often enables China-like digital authoritarianism, which relates to proposals to add a GSP human rights criteria. Fourth, it reviews and builds on existing congressional proposals to reform GSP by adding a digital trade criterion and changes to GSP transparency and reporting to help ensure the U.S. government uses GSP to support digital trade. Fifth, it analyzes trade statistics that show how GSP countries benefit from its tariff-free market access and how this provides critical leverage to encourage them to live up to the GSP's criterion. It also analyzes U.S. digital trade with GSP countries (where data exists). Finally, it provides a detailed (but not exhaustive) list of digital trade barriers in GSP beneficiary countries.

THE MANY AND GROWING TYPES OF DIGITAL TRADE BARRIERS

Data for legal goods and services will naturally flow across borders when needed, unless nations erect digital barriers that impede it. Unfortunately, despite the vast benefits to companies, workers, consumers, and economies that arise from the ability to easily share data across borders, dozens of developing countries have erected a wide slate of barriers to digital trade.

Countries that enact such barriers proffer a few main types of "justifications" for these policies: privacy and security concerns, national security and law enforcement concerns, censorship and surveillance, and aspirations for domestic economic growth (i.e. digital protectionism). In almost all cases, though, multiple motivations play a role. Also, none of these justifications validate the digital trade barriers all too many countries are increasingly erecting.

For example, misguided data privacy and protection and cybersecurity are common motivations. As more countries enact updated data protection frameworks, it is nearly inevitable that some policymakers will propose data localization as they reflexively and mistakenly believe that storing data within a country's borders is the best way to protect data. This misunderstanding remains at the core of many data-localization policies. However, the security of data does not depend on where it is stored.[5] This is misguided, as organizations cannot escape from complying with a nation's laws by transferring data abroad. Most companies doing business in a nation, including all domestic and most foreign companies, have a "legal nexus," which puts them in that country's jurisdiction.

Likewise, many policymakers try to justify data localization and other restrictions on the basis of cybersecurity. However, the security of data depends primarily on the logical and physical controls used to protect it, such as strong encryption on devices and perimeter security for data centers. Policymakers misunderstand that the confidentiality of data does not generally depend on which country the information is stored in, only on the measures used to store it securely. A secure server in Malaysia is no different from a secure server in the United Kingdom.

A growing number of countries are resorting to digital protectionism—a strategy that uses trade-distorting policies to advantage local technology firms and production activities. While modern forms of protectionism typically rely on behind-the-border regulations, not tariffs, to protect local firms, the objective and impact remain the same—to either replace foreign goods and services with local ones, unfairly promote exports, or both. Behind-the-border barriers cover various differential health, technical, product, labor, and environmental standards, internal taxes and charges, licensing and qualification recognition, and other administrative processes. These behind-the-border measures can be further differentiated by whether they

apply to the establishment of a firm versus affecting its provision of services after establishment and measures that are discriminatory against foreign firms (to the advantage of local firms) versus non-discriminatory (meaning the regulation affects domestic and foreign firms alike).

There are several common types of digital trade barriers:

- **Forced local data-residency requirements that confine data within a country's borders, a concept known as "data localization":** This disadvantages foreign firms that rely on centralized IT services to operate and otherwise need to set up or contract local data centers and services to enter and serve a market with data localization requirements. Local firms benefit as they're more likely to already use local data centers and service providers.
- **Discriminatory licensing, approval, and certification processes:** A growing number of countries are using licensing, approval, and certification policies to discriminate against U.S. payment, financial, cloud, and other services, as well as U.S. digital content (e.g., movies, TV shows, and video games).
- **Discriminatory and unwarranted digital service taxes (DSTs) and other similar tax measures, such as significant economic presence (SEP) taxes apply only to non-resident companies:** The first generation of DSTs (France, the United Kingdom, etc.) included scoping to target mainly U.S. firms through covered activities and dual revenue thresholds, but the second generation (Kenya, India, etc.) and third generation (SEPs) have generally applied to non-resident companies engaging with the market and do not include a global revenue threshold or narrowly defined activities as part of scoping. Countries worldwide have agreed to a moratorium on enacting digital service taxes given their agreement to the Organization for Economic Cooperation and Development's (OECD) ongoing work on a new multilateral tax convention. More than 140 governments have participated in the negotiations. Despite this global agreement, some countries are considering or enacting digital service taxes and other similar taxation measures that discriminate against U.S. firms and products.
- **Use of censorship as a non-tariff barrier to trade:** As in China (but spreading to other countries like Vietnam), complicated and often opaque legal, political, and bureaucratic censorship processes for blocking "illegal" and objectionable content are used as a non-tariff barrier to trade. Whether it's movies, TV shows, video games, or other digital content, countries can use inconsistent, vague, and non-transparent criteria to create an unpredictable and burdensome market access restriction.[6]
- **Discriminatory and onerous technical reviews and certifications:** This includes requirements to meet onerous and unnecessary security standards and requirements to disclose encryption algorithms or other proprietary source code.
- **Duties on imports of digital products:** Some countries (namely, Indonesia, India, and South Africa) want to end a decades-long World Trade Organization agreement not to enact duties on imports of digital content, which could include movies, TV shows, music, and software.
- **Digital local content requirements:** Some countries force over-the-top video streaming services to include a certain level of local content as part of a mandatory quota.

- **Weak or non-existent intellectual property protections:** To be effective, digital trade requires robust IP protections because without them, producers will be less able to sell their products and services across borders.
- **Foreign equity limitations (disallows or limits foreign participation in which foreign capital is restricted):** Such restrictions remain a significant barrier to ICT-based services trade as many ICT firms need to establish a local presence to better serve clients. Examples include measures on foreign firms that restrict direct equity stakes, requirements for foreign investment only through joint ventures, and limitations on mergers and acquisitions activity.
- **Market access limitations through requirements for citizenship or residency:** Also, countries are forcing foreign firms to set up a local physical office and designate a local official. This local presence is often used alongside data localization as countries essentially want a firm representative to be held accountable if the firm does not abide by local (often restrictive and problematic) laws and regulations regarding content and access to data.

DIGITAL TRADE BARRIERS IMPACT U.S. COMPETITIVENESS, EXPORTS, AND WORKERS, ESPECIALLY FOR SMES

Digital trade fosters U.S. economic competitiveness, job creation, and innovation. Modern trade is increasingly about services and data. In 2020, the total services supplied by U.S.-based firms to foreign persons through both trade and sales by foreign affiliates of U.S. MNEs was $2.25 trillion. The United States has a clear comparative advantage in services trade, with a trade surplus of $245 billion in 2021.[7] Similarly, in 2021, U.S. exports of ICT services (a core measure of digital trade) were $89.4 billion, with a surplus of $38.3 billion.[8]

Moreover, the United States realizes far more leverage from services exports than imports. Comparing production with the international purchases of services, the U.S. Department of Commerce shows that U.S. parent companies involved in international trade contributed nearly $21 of value-added to the U.S. economy for every dollar of services they imported. This led to U.S. parent companies exporting about $10,000 of services and importing nearly $5,000 of services per employee.[9] Likewise, U.S. exporting firms pay higher wages than their non-exporting counterparts. The U.S. Census Bureau estimates the difference in wages to be as high as 18 percent.[10]

Digital trade democratizes access to markets as U.S. small businesses rely on digital tools to expand their reach and export goods and digital services to customers around the world. More than 97 percent of U.S. exporters are SMEs.[11] Small and medium-sized firms gain the most from the impact that the Internet and digital technologies (like global services and global marketplace platforms) have in removing geography as a barrier to trade. In essence, the Internet and digital technologies enable SMEs to be born global rather than go through the traditional growth path of first having to grow before exporting. New U.S. Small Business Administration (SBA) survey data shows time and again a correlation between e-commerce use, digitization, and exporting.[12] Exporting SMEs are more likely to not only survive but thrive, given trade provides them with greater economies of scale. SBA survey data shows the importance of getting more SMEs to use digital tools to export as exporting SMEs tend to outperform—they are more productive, profitable, capital-intensive, pay higher wages, and employ more skilled workers than non-exporters.[13]

Individuals, startups, and SMEs rely on the power of digital technologies and platforms to succeed in global markets. These tools level the playing field by making access to global markets easy and low-cost. For example, research reveals that 97 percent of women-owned eBay-enabled small businesses are exporters compared to less than 1 percent of traditional businesses. Additionally, they reach an average of 15 international markets with their goods, nearly 4 times that of traditional businesses.[14] Similarly, a survey of 336,000 SMEs on Facebook found that they are more likely to export (6.75 percent) than other firms (only 4.3 percent of which export). Likewise, PayPal states that 79 percent of U.S. SMEs on PayPal sell to foreign markets and that these firms experienced higher growth rates: small business exporters on PayPal grew 32.8 percent from 2015 to 2016 compared to 22.9 percent growth for small businesses in general.[15] This is to show that measures that specifically impact larger U.S. tech firms also have a direct and major impact on the many SMEs that depend on them to find and serve customers in foreign markets.

Conversely, digital trade barriers undermine U.S. economic interests. Many, if not most, digital trade barriers are purposely designed to disadvantage American firms, given the United States is a world leader in digital technologies. If U.S. firms lose market share to unfairly competing firms supported by their innovation mercantilist governments, it means two things. First, sales fall. This is true because global sales are largely fixed, and if a mercantilist-supported competitor (unfairly) gains market share, then the market-based competitor loses share. Second, because profits decline more than sales, it becomes more difficult for the market-based innovator to reinvest revenues in the next generation of products or services, meaning that the mercantilist-supported entrant has an advantage in creating the next generation of products. Studies show that barriers to trade in digital services, including data localization, decrease services trade.[16]

Digital trade barriers disproportionately disadvantage individual traders, startups, and SMEs as they do not have the resources or expertise to try and adjust to them. These operators depend on centralized IT systems to take advantage of global markets. These operators can't afford to set up local data centers, cloud services, or core digital platforms and services (payments, marketplaces, etc.) in each and every market they sell into. Likewise, digital trade restrictions that impact the leading U.S. digital services and platforms that individuals, startups, and SMEs rely on inevitably affect their ability to help them find, communicate, service, deliver to, and process payments from customers around the world. The same applies to some DSTs, which have an outsized effect on U.S. SMEs because, in some of these measures, a company is liable for the DST starting with its first dollar of revenue in a market. For example, Uganda adopted a DST earlier in 2023 that imposes a 5 percent tax on revenue derived by non-residents providing digital services to customers in Uganda. This also applies to Kenya's DST.

DATA LOCALIZATION ENABLES DIGITAL AUTHORITARIANISM

Digital authoritarianism—which can be generally defined as the governmental misuse of digital tools to repress civil and economic freedoms—often relies on data localization as it provides governments with easy access to data and content for surveillance and control purposes. As Congress considers stronger enforcement of the GSP's human rights-related criteria, it should recognize the cross-over with some digital trade restrictions, especially data localization. In this sense, an explicit digital trade criterion helps address two GSP criteria simultaneously.

Not every use of data localization is used for digital authoritarianism. However, many authoritarian countries use localization for exactly this reason. These countries don't publicly say this. Policymakers often take a "dual-use" approach with an official and seemingly legitimate objective, such as data privacy or cybersecurity, when their primary (hidden) motivation is censorship and surveillance. Countries use data localization as a cudgel to force foreign firms to provide easier access to data for surveillance and political purposes and force compliance with censorship requirements. Commonly mixed into this rationale is the specter—real and imagined—of foreign surveillance as a rationale for data localization when it actually enables their own surveillance.

Digital authoritarian governments—led by China and Russia—see physical access to data centers as a critical enabler of surveillance and political control. Data localization enables political oppression by bringing information under government control and allowing the government to identify and threaten individuals, impacting privacy, data protection, and freedom of expression.[17] China retains broad and vague legal authority in its laws to potentially access data for national security, public interest, and political purposes.[18] The lack of an independent judiciary and the opaque nature of these laws make it hard to judge how China uses these broad powers.[19] Yet, this doesn't stop these countries from referring to "data privacy" as a motivation for localization.[20]

Recent laws introduced in Pakistan and Vietnam highlight how data localization does not lead to greater data privacy—but the exact opposite in making it easier for governments to access a small number of servers. Related but different from this authoritarian motivation is when countries like India enact short deadlines for firms to respond to content takedown requests that create a de facto localization requirement. Firms have to do this; otherwise, they would not be able to comply (and thus avoid fines and other legal consequences).[21]

Pakistan is using data localization to support censorship and surveillance. Pakistan's "Removal and Blocking of Unlawful Online Content" includes broad data localization requirements. It also allows the government to force companies to block content critical of the government and facilitate access to user data. It allows the Pakistan Telecommunication Authority to avoid existing data access and privacy safeguards, allowing it to intervene on behalf of law enforcement agencies to ask social media companies to provide user data.[22] It also makes it mandatory for firms to retain information, including traffic data linked to blocked content and decrypted information about subscribers and their activity.

TRADE DATA SHOW GSP PROVIDES THE UNITED STATES WITH CRITICAL LEVERAGE TO ROLL BACK DIGITAL TRADE BARRIERS

The GSP's duty-free access provides critical leverage for the United States in its engagement with a range of countries where USTR has reported a plethora of trade and market-access issues. The size, significance, and growth of the GSP's duty-free access is considerable for several GSP beneficiaries. In 2000, products valued at $12.7 billion entered the United States duty-free under the program. In 2006, this figure peaked (before the global financial crisis) at $28.4 billion, after which it fell to $17.8 billion in 2009, before gradually increasing to $21.2 billion in 2017.[23] In 2020, products valued at $16.9 billion (imports for consumption) entered the United States duty-free under the program out of $152.0 billion worth of total imports from GSP-eligible countries.[24]

Table 1 lists major GSP beneficiaries that have also enacted or are considering significant digital trade barriers. Indonesia is the most significant beneficiary country with the most concerning digital trade restrictions. In 2019, $2.7 billion of Indonesia's exports to the United States benefited from GSP's tariff-free market access, which represented 13.6 percent of Indonesia's total exports to the United States. While Thailand's GSP-related exports to the United States represent a higher share of its total exports, it does not have nearly as many enacted or proposed digital trade restrictions as Indonesia. Similarly, Pakistan is another major beneficiary of GSP tariff-free market access that has also enacted (or is considering) a series of digital trade restrictions (that also raise human rights concerns in terms of privacy and freedom of speech). In 2019, $346 million of Pakistan's exports to the United States benefited from GSP tariff-free market access, which represented 8.8 percent of Pakistan's total exports to the United States. It's also worth noting that exports from all these GSP-eligible countries that have digital trade barriers have grown considerably over time. From 2000 to 2017, Indonesia's GSP-eligible exports increased by nearly 200 percent, while Pakistan's increased by 371 percent.

Table 1: Imports of GSP-eligible goods by countries with digital trade barriers[25]

Country	GSP Imports in 2019 ($Millions)	Growth, 2000–2019	U.S. General Imports in 2019 ($Millions)	GSP as % of Total Imports
Thailand	$4,861.0	120.5%	$33,442.6	14.5%
Indonesia	$2,730.6	99.5%	$20,104.6	13.6%
South Africa	$756.8	29.8%	$7,794.5	9.7%
Pakistan	$346.2	271.1%	$3,920.2	8.8%
Brazil	$2,322.1	11.3%	$30,934.1	7.5%
India	$2,902.6	155.0%	$57,879.0	5.0%
Kenya	$5.8	47.5%	$667.1	0.9%
Nigeria	$8.3	11,618.8%	$4,609.5	0.2%

U.S. DIGITAL TRADE WITH GSP COUNTRIES IS GROWING. DIGITAL TRADE RESTRICTIONS WOULD PREVENT FUTURE GROWTH IN LARGE, GROWING DIGITAL ECONOMIES

Table 2 shows that U.S exports of information communication technology (ICT) and potential ICT-enabled services (the statistic the U.S. Department of Commerce uses to measure digital trade) to some GSP countries are significant, increasing, and most importantly, hold the potential for significant future growth that would otherwise be cut off if these countries are allowed to enact digital trade barriers. Table 1 is a snapshot as the U.S. Department of Commerce does not have digital trade statistics for all GSP beneficiaries. For example, U.S. digital trade exports to Brazil were worth $4.4 billion in 2021, an increase of 75 percent from 2010. U.S. digital trade exports to South Africa, the Philippines, Indonesia, and Nigeria are relatively low compared to other major trading partners, but in all cases, the future potential for their respective digital economies is enormous and worth preserving access to via updated GSP criteria and other trade tools.

Table 2: ICT and ICT-enabled exports from the United States[26]

Country	ICT Exports from United States in 2010 ($Millions)	ICT Exports from United States in 2021 ($Millions)	Growth, 2010–2021
Brazil	$4,407	$3,342	-24.2%
South Africa	$389	$371	-4.6%
Philippines	$189	$253	33.9%
Indonesia	$117	$222	89.7%
Nigeria	$87	$97	11.5%

CURRENT AND POTENTIAL LEGISLATIVE PROPOSALS: ADD AN EXPLICIT DIGITAL TRADE CRITERION AND NEW TRANSPARENCY AND REPORTING REQUIREMENTS TO ENSURE GSP BECOMES AN EFFECTIVE DIGITAL TRADE TOOL

Congress should build on past bipartisan support to finally create an explicit digital trade criterion for GSP eligibility. Senate and House legislative proposals (both detailed below) have already considered (largely overlapping) legislative proposals that add an explicit criterion for digital trade barriers (along with other changes). Congress should finally add digital trade to GSP and make reporting and transparency reforms (detailed below) to GSP to ensure the current and future administrations use it to support digital free trade. These latter reforms are important given part of the Biden administration's reluctance (or aversion) to actually advocating for U.S. digital trade interests.

The Trump administration showed the advantages of making digital trade barriers a central feature of GSP reviews. Former USTR Lighthizer took several steps in the right direction in considering digital trade barriers in GSP reviews of India, Indonesia, and Kazakhstan. In October 2017, USTR Lighthizer announced his agency would step up GSP enforcement:

> Countries receiving U.S. trade benefits must meet the eligibility criteria established by Congress.… By creating a more proactive process to assess beneficiary countries' eligibility, the United States can ensure that countries not playing by the rules do not receive U.S. trade preferences. This sets the correct balance for a system that helps incentivize economic reform in developing countries and achieve[s] a level playing field for American businesses.[27]

USTR Lighthizer asked USTR officials to conduct a broad triennial review of the GSP, starting with members in Asia (the administration has already initiated reviews of India, Indonesia, and Thailand). In particular, the U.S. threat of removing GSP benefits was one of the useful tools used to help convince Indonesia and Thailand from enacting data localization. This is why Congress should make digital trade barriers a clear and consistent feature of GSP reviews henceforth.

Congressman LaHood's Digital Trade for Development Act

In May 2021, Congressman Darin LaHood (IL-18) introduced the Digital Trade for Development Act (DTDA) to modernize the Generalized System of Preferences (GSP) to support open digital trade policies.[28] DTDA's provisions would be a valuable addition to GSP criteria.

DTDA would add the new provisions:

- ''The President, acting through the United States Trade Representative, determines that such country restricts digital trade to the detriment of United States development goals, strategic interests, or competitiveness.''
- "The extent to which, in the determination 3 of the President acting through the United States 4 Trade Representative, such country—
  - (A) has refrained from imposing, or has eliminated, digital trade barriers, including unnecessary data transfer restrictions and data localization mandates; and '
  - (B) has taken steps to support consumer protections and the privacy of personal information online and to extend the benefits of digital trade to all.''[29]

The Senate's Trade Preferences and American Manufacturing Competitiveness Act of 2021

In May 2021, Senator Rob Wyden (D-Ore) announced the Trade Preferences and American Manufacturing Competitiveness Act of 2021 to extend duty-free access to the U.S. market for certain developing countries under GSP until 2027, with important updates to eligibility rules that ensure trade policy rewards advances in human rights, women's economic empowerment, labor, environment, the rule of law and digital trade, among others.[30]

This bill would add several important digital trade, transparency, and reporting provisions:

- (A) has refrained from imposing, or has eliminated, digital trade barriers, including unnecessary or discriminatory data localization or data transfer restrictions; and
- (B) has taken steps in the digital environment to support consumer protections, the privacy of personal information, and open digital ecosystems.
- Publication of determinations relating to petitions for review—The United States Trade Representative shall publish in the Federal Register a notice of, and the rationale for, any determination of the Trade Representative with respect to a petition for review of the eligibility of a country for designation as a beneficiary developing country, including a determination—
  - (1) to accept or deny such a petition;
  - (2) to continue to review the eligibility of the country; or
  - (3) to withdraw, suspend, or limit the application of duty-free treatment under this title with respect to the country.
- In General—The President shall—

- (A) on an annual basis—
    - (i) conduct assessments of the compliance of an appropriate number of countries designated as beneficiary developing countries for purposes of this title in meeting or continuing to meet the eligibility requirements under this title; and
    - (ii) make determinations with respect to whether to initiate full reviews of the practices of those countries to assess the continued eligibility of those countries 6 for designation as beneficiary developing countries under this title; and
- (B) submit to Congress a report consisting of the results of such assessments and determinations.
    - Frequency—The President shall conduct an assessment described in clause (i) of paragraph (1)(A) and make a determination described in clause (ii) of that paragraph with respect to each country designated as a beneficiary developing country for purposes of this title not less frequently than once every 3 years.'

Reform GSP to Ensure a Clearer and Stronger Role for Congress in GSP Oversight

The Biden administration's unnecessarily reluctant approach to supporting digital trade and pushing back against digital protectionism points towards the need for GSP to have improved transparency and reporting requirements (akin to the Senate bill) to ensure Congress has clearer and stronger oversight of USTR's use of GSP reviews.

USTR Tai and senior staff are ideologically opposed to fully, forcefully, and publicly advocating for new, stronger, and binding digital trade rules and pushing back against existing and proposed digital trade barriers, as they don't want to do anything that they think helps "big tech."[31] Even if it comes at the cost of U.S. jobs and economic, trade, technology, and strategic interests. So, it is important for the administration and bipartisan supporters of digital trade in Congress to understand why USTR Tai's approach is misguided and to push back by making it clear in GSP reforms that Congress wants USTR to advocate for digital free trade.

USTR has the necessary rules and tools in place to turn the GSP into an effective mechanism to confront the mercantilist trade policies of many beneficiaries. But it's an increasingly important question as to whether it uses it effectively. Congress should ensure GSP has improved transparency, reporting, and feedback mechanisms built into it to ensure that USTR consistently and effectively reviews whether countries meet all of the GSP criteria.

During the GSP review process, U.S. and foreign firms and foreign governments can petition the Trade Policy Staff Committee (the interagency committee chaired by USTR that manages the GSP review) about whether certain goods and countries should be eligible for GSP benefits. At the end of the review process, the GSP subcommittee provides advice to the U.S. president, who has the discretion to act accordingly. The key question is whether USTR uses the triennial review to reboot the GSP's role in addressing mercantilist trade policies. Most of the time, USTR's own reporting has all the evidence they should need to identify GSP beneficiaries who are not living up to the criteria and, therefore should have access suspended or revoked.

Greater congressional oversight would ensure USTR avoids its past practice of ad hoc GSP enforcement, as this is ineffective in encouraging countries to address digital trade barriers and other GSP criteria. Thus far,

USTR has only withdrawn GSP benefits in a very limited number of instances based on intellectual property and workers' rights issues (even though the GSP's criteria are broader than these two explicitly listed criteria). For example, due to intellectual property issues, Argentina, Lebanon, Russia, and Ukraine have been cited and denied GSP benefits. Workers' rights were the most prominent issue in the most recent GSP annual review, with six countries cited (based on petitions from the AFL-CIO, the International Labor Rights Forum (ILRF), and USTR itself). Intellectual property concerns were the second-most prominent category, with the International Intellectual Property Alliance (IIPA) citing concerns with Indonesia, Ukraine, and Uzbekistan.[32] Ad hoc scrutiny and enforcement do not send the much-needed signal that, in the future, participants will only be able to reap the rewards if they truly live up to the program's free-trade principles and provide fair and reasonable market access and treatment to U.S. firms and their goods, services, and intellectual property.

CONCLUSION

The United States needs to ramp up its use of existing trade enforcement tools—including GSP eligibility—to contest growing digital protectionism. The GSP's duty-free access provides USTR with significant leverage that should be applied more forcefully to push trading partners—especially Brazil, Indonesia, Kenya, and Pakistan—to address various digital trade barriers. While more proactive and forceful enforcement of updated GSP's trade criteria would only cover a subset of U.S. trading partners, it would still help a great deal in addressing some emerging trade issues in some key markets. In doing so, it would also send a message to other GSP countries that if they want to continue enjoying the program's benefits, they should not follow the lead of countries using innovation mercantilist policies and enacting unwarranted barriers to trade.

Nigel Cory
Associate Director, Trade Policy

APPENDIX: CASE STUDIES OF GSP RECIPIENTS AND DIGITAL TRADE BARRIERS

The list below details many (but by no means all) digital trade barriers in GSP beneficiary countries. It mainly focuses on explicit data localization measures. It also details a few proposed (but not enacted) localization requirements to highlight the spread of restrictions among GSP beneficiary countries. In these cases, it highlights the potential value of U.S. officials being able to point towards the withdrawal of GSP benefits in engagements with these countries to encourage them to reconsider.

In the case of Indonesia, the below also highlights preparations to enact duties on digital products, which could become another major barrier to digital trade around the world if the World Trade Organization's moratorium on such digital duties is not renewed in 2024.

The list also details digital service taxes and similar taxation measures (often called significant economic presence taxes) in Indonesia and Nigeria. Both Indonesia and Nigeria are involved with the Inclusive Framework. However, Nigeria did not agree to the October 2021 "Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalization of the Economy," which included the standstill on newly enacted DSTs and similar measures (other non-joinees for the October 2021 Statement are Kenya, Sri Lanka, and Pakistan).

Algeria

2018: Algeria signed into law legislation requiring electronic commerce platforms conducting business in Algeria to register with the government and to host their websites from a data center located in Algeria.[33]

Brazil

2018: Brazil's Ministry of Planning released guidelines for government contracts related to information and communications, which may include encryption methods, firewalls, and other measures. Confidential data or information produced or safeguarded by the Federal Public Administration, including backup data, shall receive a security risk assessment and potentially be prohibited from being processed in a cloud computer software if deemed sufficiently sensitive. This data shall also be physically located in Brazil.[34]

2020: Brazil's General Law for the Protection of Personal Data (LGPD) took effect on September 18, 2020. The LGPD includes provisions concerning restrictions on the transfer of personal data outside of Brazil that will be implemented after promulgation of regulations required for international transfers of personal data.

2020: Brazil is considering various digital tax initiatives, including the introduction of a DST through an expansion of its existing CIDE (contribuição de intervenção no domínio econômico) regime. The CIDE-Digital tax (PL 2,358/2020) would apply progressively from 1 percent to 5 percent on gross revenues derived from (1) digital advertising; (2) operating a digital service that permits users to interact with each other for the sale of goods and services; and (3) collection of user-generated data in the operation of a digital platform.[35]

Cambodia

2020: Cambodia's Law on Electronic Commerce mandates that personal data transfers can only take place based on certain conditions.[36] Furthermore, Cambodia's National Assembly passed a sub-decree in February 2021 to establish a National Internet Gateway that would require Internet providers to route all online traffic

through a single node regulated by a government-appointed operator. Cambodia's implementation of the National Internet Gateway has been delayed but not canceled. Both the private sector and human rights organizations continue to express concerns over the National Internet Gateway's effect on internet freedom in Cambodia. Separate laws governing cybersecurity, cybercrime, and data privacy are in draft form.[37] The law was set to go into effect in February 2022 but has been postponed to an undetermined date due to the pandemic.[38]

2022: (Proposed) Cambodia has considered a draft Cybercrime bill that includes data localization.[39]

Cote-d'Ivoire

2013: Cote-d'Ivoire enacted privacy laws that required firms to get pre-approval from the regulator before processing personal data outside of the Economic Community of West African States (ECOWAS, which includes 15 member countries, ranging from Benin, Ghana, Liberia, Mali, Niger, Nigeria, and Senegal).[40]

Egypt

2018: Egypt's Law No. 180/2018 Regulating the Press, Media, and the Supreme Council for Media Regulation (SCMR) requires media outlets to pay a fee of 50,000 Egyptian Pounds (approximately $1,636) to obtain a license from the SCMR and gain legal status. The law broadly defines "media outlet" to include any social media account with at least 5,000 subscribers. The Egyptian Government has used this and other laws as grounds to limit cross-border services.[41]

2020: Egypt enacted the Personal Data Protection Act (Law No. 151/2020), which requires licenses for cross-border data transfers.[42]

Ghana

2019: Ghana enacted the Ghana Payment Systems Bill & Guidelines, which, among many other things, set out the requirements to obtain a payment systems operator license.[43] In particular, it calls for firms to establish a local entity, at least 30 percent local ownership, and for a board of directors that includes at least three Ghanaians, one of which must be the CEO. In July 2018, Ghana issued draft regulation that required all domestic transactions to be processed by the Ghana Interbank Payment and Settlement Systems Limited (GhiPPS, which the Central Bank of Ghana wholly owns). However, there were significant industry concerns, so the final implementing directive has not yet been issued.

Indonesia

2016: OJK's Regulation 69/POJK.05/2016 mandates insurers/reinsurers to establish data centers and disaster recovery centers in Indonesia. Indonesia is considering national legislation and additional regulations on personal data protection, which could expand requirements for data localization.[44]

2018: Digital duties. In 2018, Indonesia's Ministry of Finance (MOF) issued Regulation 17/2018, which established five HS lines at the eight-digit level for digital products transmitted electronically, including applications, software, and video and audio content. The regulation sets import duty rates at zero percent. On January 14, 2023, the MOF issued Regulation No. 190/PMK.04/2022, which requires entities importing

digital products covered by the five harmonized schedule (HS) lines to file a customs declaration within 30 days of receiving payment for the digital products.

Despite the zero percent duty rate, U.S. firms and other stakeholders have expressed concern over these new reporting requirements. It could potentially apply to a wide range of entities, including SMEs, that transmit files through the Internet to entities within Indonesia. Since no other country has taken similar steps to attempt to apply to digital products on electronic networks the rules and processes for the collection of customs duties on physical goods at the physical border, there are significant unanswered questions concerning how Indonesia will define the "border" on electronic networks and what steps Indonesia would take to "inspect" digital products.[45]

2019: Regulation 71 on Organization of Electronic Systems and Transactions 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.[46] 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.[47] Foreign firms have lost, and continue to lose, business in Indonesia due to the ambiguity in these data localization requirements.

GR 71 also requires private sector ESPs to facilitate government agencies' supervision, including granting access to electronic systems and data for monitoring and law enforcement purposes. Indonesia's Ministry of Communications and Information Technology (MCIT) issued implementing regulations for GR 71, Regulation 5/2020 and Regulation 10/2021, which require private sector ESPs, including those providing services on a cross-border basis, to register with MCIT by July 20, 2022 or be subject to blocking. Failure to comply with government takedown orders for a potentially broad category of "prohibited electronic information" can also result in blocking.[48]

2019 (Proposed). 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.[49] 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.[50] 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. Indonesians, individuals, or entities must own at least 51 percent of shares with voting rights.[51]

2020: Under Law 2/2020, Indonesia introduced a series of changes to its tax code, including an expansion of the definition of permanent establishment for purposes of Indonesia's corporate income tax, and a new electronic transaction tax (ETT) that targets cross-border transactions where tax treaties (such as the U.S.-Indonesia tax treaty) prohibit Indonesia from taxing corporate income from the transaction. The MOF would need to issue additional legal measures for these new taxes to go into effect.[52] USTR launched and subsequently closed a Section 301 investigation into Indonesia's new tax measures.

While structurally different from DSTs in European countries, the tax is similarly concerning insofar as it looks to increase U.S. firms' tax payments in the region by departing from longstanding international taxation norms. U.S. companies were cited as targets of these tax measures. Implementation details are still uncertain, even as Indonesian officials have stated that they would align politics with the OECD consensus reached in October 2021. A new VAT on digital goods and services went into effect on April 1, 2022. The VAT will be collected on all goods and services that are taxable and delivered to Indonesia via electronic systems at a rate of 11 percent (which will rise to 12 percent starting in 2025).[53]

Indonesia joined the October 2021 "Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy," but it had already adopted its measure before October 2021. The October 2021 Statement commits jurisdictions to not imposing any newly enacted measures on any company from October 7, 2021, until the earlier of the coming into force of the framework agreement or December 31, 2023. Again, Indonesia hasn't put forward implementing regulations, so while the SEP/ETT is on the books, it is not being imposed.

2020: Indonesia's Ministry of Communications and Information Technology (KOMINFO) issued the "Regulation on Governance of Private Scope Electronic System Administrators (ESA)," which is very vague and broad and contains de facto localization requirements that contravene existing regulations (GR71) which allow firms to store data offshore. The definition of what a private scope ESA is not clear and could cover a broad range of digital activity. It requires all ESAs to register (whether foreign or domestic) with KOMINFO. Those who fail to register face sanctions, such as having their website/service blocked. Article 6 on the management, processing, and/or retention of data requires all ESAs to have approval from the minister, who must take into account the requirements and consideration of "national interests," such as to ensure effective regulatory supervision and law enforcement access to data. It doesn't specify the requirements and criteria to obtain approval to maintain data outside Indonesia. It also only provides firms with 12 hours to remove illegal content after notification, which would create a de facto localization requirement as it'd be technically impossible for firms to abide by such a requirement. It requires private ESAs to provide access to their systems

and data to government ministries and law enforcement within 24 hours after receiving a request. Further, Article 99 of GR 71 states that institutions holding "Strategic Electronic Data" must hold archives and must be connected to a specific data center (presumably one that is managed by the Government). Included in sectors stipulated as holders of "Strategic Electronic Data" are energy, transportation, financial, health care, ICT, food, defense, and any other sectors stipulated by the Government.[54]

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.[55]

2021: Indonesia's overall approach to financial data governance is 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.[56] 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.[57]

Kazakhstan

2021: Kazakhstan adopted new rules as part of its personal data protection framework, which specified that all personal data should be stored locally.[58]

2015: Kazakhstan enacted a law (No. 418-V) on informatization that reaffirmed that organizations store electronic databases containing personal data in the country.[59]

2013: Kazakhstan enacted an amendment to its personal data protection law that requires owners and operators collecting and using personal data to keep such data in-country. The requirement for localization of personal data applies to companies established in Kazakhstan and individual proprietors in Kazakhstan, including branches and representative offices of foreign companies.[60]

2010: Kazakhstan enacted a regulation on telecommunication subscriber information, which prohibits the storage of subscriber information outside the country.[61]

2005: (reinforced in a revised regulation in 2018), Kazakhstan has required that all domestically registered domain names (i.e., those on the ".kz" top-level domain) operate on physical servers within the country).[62]

2004: Kazakhstan enacted a communications law that requires certain communication services to store data in the country.[63]

Kenya

2016: (Proposed) Kenya's Communications Authority considered including data localization provisions within Kenya Information Communications (Cyber-Security) Regulations (2016). Article 10(1) required the hosting and storage of "public information" within Kenya.[64]

2019: Kenya Data Protection Act excluded explicit data localization provisions from earlier drafts but still included unclear and potentially restrictive provisions governing the cross-border transfer of personal information, such as explicit consent for transfers of "sensitive personal data" (a broad category) and that data controllers provide unspecified proof that personal data transferred abroad receives the same protection as if stored at home. Furthermore, it empowers a political official to prohibit the cross-border transfer of certain categories of data, creating uncertainty for businesses.[65] The 2021 Data Protection (General) Regulations require the processing of personal data "for the purposes of actualizing a public good" to be processed through a server and data center located in Kenya or that at least one copy of the personal data be stored in a data center located in Kenya.

2021: (Proposed) Kenya's released draft data protection regulations (to implement the Data Protection Bill) require firms to store data (a copy) and process data locally if the data processing is done "for the purpose of actualizing a public good." This apparently includes managing an electronic payment system licensed under the National Payment Systems Act; processing health data for any other purpose other than providing health care directly to a data subject; managing personal data to facilitate access of primary and secondary education: and management of a system designated as a protected computer system under the Computer Misuse and Cybercrime Act, 2018.[66]

2021: The 2021 Finance Act includes a 1.5 percent digital services tax for non-resident businesses. The DST taxes gross revenue accrued through any "digital marketplace," defined as "an online platform which enables users to sell or provide services, goods, or other property to other users." Kenya has engaged in discussions with the Organization for Economic Cooperation and Development (OECD) and other partners on the OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting but has not endorsed or adopted it and continues to apply its unilateral DST.[67]

Nigeria

2011: The Central Bank of Nigeria enacted a de facto local storage and processing requirement for entities engaging in point-of-sale (POS) card services. Domestic transactions cannot be routed outside Nigeria for switching between Nigerian issuers and acquirers.[68]

2015: Nigeria enacted broad data localization requirements as part of the Guidelines for Nigerian Content Development in ICT. Nigeria wants ICT companies to "host all subscriber and consumer data" and all government data inside the country.[69]

2020: Nigeria's 2020 Finance Act introduces income tax obligations for non-resident companies providing digital goods and services in Nigeria.[70] While the law applies to all non-resident companies earning above a certain threshold, extensive media coverage and analysis by experts has repeatedly mentioned the targeting of US multinationals.[71] The law specifically references non-resident companies with a 'significant economic presence' in the country which is defined by a number of factors including: a minimum amount of revenue

generated from users in Nigeria, transmitting data about Nigerian users, or the availability of local websites or local payment options. Exceptions have been built into the law for companies that are covered by a multilateral agreement to which the Nigerian government is a party.[72] This policy was eventually signed into law as the Finance Act of 2021 on December 31, 2021, which captured U.S. tech firms under revisions to its Value Added Tax code policies and resulted in a knock-on 7.5 percent VAT rate for tech firms such as Google. Non-resident digital services firms are also required to pay 6 percent of their yearly turnover as well.[73]

Pakistan

2020–Present: (Proposed) Pakistan's Cabinet approved a draft data protection bill that includes a range of data localization and processing requirements (including for "critical personal data" (which is not clearly defined)).[74] The PDP Bill in Pakistan is expected to be introduced in parliament shortly and is expected to be passed soon thereafter. The exact date is unknown. The Pakistani government has not shared a copy of the latest version of the PDP bill, so there has not been an opportunity for the public and other countries to submit feedback.

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."[75] 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. Furthermore, the Authority has the power to impose data mirroring requirements that would require a copy of the data to be stored in Pakistan.[76] 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.[77]

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."[78]

2016: Pakistan enacted PECA (commonly known as the Cyber Crimes Law).[79] 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 Article 19 of the constitution guarantees. 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 the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2020.[80] Pakistan considered and enacted amendments to this legislation in 2021, but most problematic provisions remain unchanged, including data localization and a local office/staff.[81] 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 than 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.[82]

The Philippines

2023: (Proposed) A draft presidential executive order calls for explicit and broad data localization and local data processing. The proposed rule would extend to "cloud service providers, intermediaries, and other private entities with transactions, contracts, or data related to, in connection with, or arising from the rendition of cloud computing services i.) for the Philippine government; ii) for private entities processing sensitive personal information as defined in Republic Act No 10173; iii) private entities processing subscriber's information as defined in Republic Act No. 11223… and v) private entities processing personal information declared to be confidential in nature under existing laws."

Rwanda

2012: Rwanda enacted a regulation that all critical information data within the government (website hosting, email hosting, shared applications such as Document Management and e-archiving, and enterprise applications) should be hosted in their national data center.[83]

Senegal

2021: Senegal announced that it would move all government data and digital platforms from foreign servers to a new national data centre in hopes of strengthening its digital sovereignty.[84]

Sri Lanka

2023: Sri Lanka's Data Protection Bill only allows public authorities (who may be using a foreign cloud provider) who are processing personal data as a controller or processor to only process this data within Sri

Lanka. The public authority can only process this data in another country if it is listed as an "adequate" country by the government.

South Africa

2018: The South African Reserve Bank imposed a moratorium prohibiting the migration of domestic transaction volumes from Bankserv (South Africa's bank-owned domestic payment switch) to international payment schemes. The South African Reserve Bank enacted the moratorium after it found out that domestic South African banks planned to move more of their transactions to global payment service networks. The moratorium was to be in place until a new policy was developed and enacted.[85]

2021: (Proposed) South Africa's "Draft National Policy on Data and Cloud" recommends data localization and local data processing for all data related to "critical information infrastructure" and data mirroring for personal data (for the purposes of law enforcement). It also states that all data generated in South Africa shall be the property of South Africa, regardless of the nationality of the firm involved in collecting it.[86]

Thailand

2022: Thailand's Personal Data Protection Act (PDPA) was enacted in 2022. In September 2022, the Thai Office of the Personal Data Protection Committee released draft regulations to dictate rules for transferring personal data outside of Thailand under the PDPA, called the "Notification of the personal data protection committee on rules and principles of appropriate personal data protection for international transfer."[87] The rules governing the export of data from Thailand include a provision that could lead to companies needing to obtain consent from customers if they opt to change business partnerships surrounding the sub-processing of data. If enacted, this could prove restrictive for businesses that would be obligated to wait for consent from each of its customers in Thailand to approve what is usually seen as a standard business decision requiring swift movement.[88]

Uganda

2023: Uganda adopted a DST that imposes a 5 percent tax on revenue derived by non-residents providing digital services to customers in Uganda.[89] Digital services covered by this tax include online advertising services; data services; services delivered through an online marketplace or intermediation platform, including an accommodation online marketplace, a vehicle hire online market place and any other transport online marketplace; digital content services, including access and downloading of digital content; online gaming services; cloud computing services; data warehousing; and other services delivered through a social media platform or an Internet search engine. The legislation does not establish thresholds for in-market activity, so a U.S. company would be liable for the DST from the first dollar of revenue.[90]

Uzbekistan

2019: Uzbekistan's revised personal data law requires explicit local personal data storage and processing.[91]

ENDNOTES

1. Nigel Cory and Rob Atkinson, "Time to Restrict GSP Benefits to Fight Trade Mercantilism" (ITIF, 2018), https://itif.org/publications/2018/08/20/time-restrict-gsp-benefits-fight-trade-mercantilism/.
2. Nigel Cory, "Explainer: Understanding Digital Trade," *Real Clear Policy,* March 13, 2019, https://www.realclearpolicy.com/articles/2019/03/13/explainer_understanding_digital_trade_111113.html.
3. Global Innovation Forum, "Making Small Business Mighty: The Digital Trade Opportunity for Small Businesses in the Indo-Pacific," https://globalinnovationforum.com/reports/us-apac-small-business-digital-trade/; Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries" (ITIF, 2015), https://itif.org/publications/2015/02/24/cross-border-data-flows-enable-growth-all-industries/; Tina Highfill and Christopher Surfeld, "New and Revised Statistics of the U.S. Digital Economy, 2005–2021," U.S. Bureau of Economic Analysis, https://www.bea.gov/system/files/2022-11/new-and-revised-statistics-of-the-us-digital-economy-2005-2021.pdf; Danielle Trachtenberg, "Digital Trade and Data Policy: Select Key Issues," (Congressional Research Service, 2023), https://crsreports.congress.gov/product/pdf/IF/IF12347.
4. Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" (ITIF, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.
5. Daniel Castro, "The False Promise of Data Nationalism" (ITIF, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.
6. Nigel Cory, "Testimony to the U.S. Senate Subcommittee on Trade Regarding Censorship as a Non-Tariff Barrier to Trade" (ITIF, 2020), https://itif.org/publications/2020/06/30/testimony-us-senate-subcommittee-trade-regarding-censorship-non-tariff/.
7. Shari Allen and Maryam Fatima, "U.S. International Services: Trade in Services in 2021 and Services Supplied Through Affiliates in 2020," U.S. Department of Commerce, October 19, 2022, https://apps.bea.gov/scb/issues/2022/10-october/1022-international-services.htm.
8. Ibid.
9. Kevin Barefoot and Jennifer Koncz-Bruner, "A Profile of U.S. Exporters and Importers of Services" (Washington, DC: International Trade Administration, June 2012), http://www.bea.gov/scb/pdf/2012/06%20June/0612_MNC.pdf.
10. U.S. International Trade Commission (USITC), *Economic Impact of Trade Agreements Implemented under Trade Authorities Procedures, 2021 Report* (USITC, June, 2021), https://www.usitc.gov/publications/332/pub5199.pdf.
11. "ITA's Exporter Database," U.S. International Trade Administration, https://www.trade.gov/ita-us-exporters-database-home.
12. U.S. Small Business Administration (SBA), Report with Eight Deliverables for Project to Support Small Business Administration (SBA) to Identify the Total Addressable Market of Small Business Exporters (SBA, 2023), https://www.sba.gov/sites/sbagov/files/2023-02/SBA%20Total%20Addressable%20Market%20Study%20FINAL-508%20%281%29.pdf.
13. Ibid; See for example: "State of MSME Ecommerce Around the World," Nextrade Group, https://www.nextradegroupllc.com/nextrade-ecommerce-diagnostics; The World Bank, *World Development Report 2016: Digital Dividends* (Washington, D.C. 2016), https://www.worldbank.org/en/publication/wdr2016; Sanjay Kathuria, Arti Grover, Viviana Maria Eugenia Perego, Aaditya Mattoo, and Pritam Banerjee, *Unleashing E-Commerce for South Asian Integration,* (Washington, D.C., 2020),

https://openknowledge.worldbank.org/bitstream/handle/10986/32718/9781464815195.pdf?sequence=4&isAllowed=y.

14. "US Women-Owned Small Online Business Export Report," eBay, October, 2022, https://www.ebaymainstreet.com/news-events/ebay-publishes-us-women-owned-small-online-business-export-report.
15. Christine McDaniel and Daniele Parks, "Businesses on Facebook and Propensity to Export: The United States" (Mercatus Center, George Mason University, February, 2019), https://www.mercatus.org/media/69441/download.
16. Eric van der Marel and Martina Ferracane, "Do data policy restrictions inhibit trade in services?" *Review of World Economics*, 157, 727-776. doi: https://doi.org/10.1007/s10290-021-00417-2.
17. Erica Fraser, "Data Localisation and the Balkanisation of the Internet," *SCRIPTed*, 2016, Vol. 13, p. 359, https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/.
18. Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare blog post, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense; Samm Sacks, Qiheng Chen, and Graham Webster, "Five Important Takeaways From China's Draft Data Security Law," DigiChina Project blog post, July 9, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/five-important-take-aways-chinas-draft-data-security-law/.
19. Bill Bishop, "One country, one Internet?; TikTok; Gaokao; Floods in China; US FBI head on China," Sinocism newsletter, July 7, 2020, https://sinocism.com/p/one-country-one-internet-tiktok-gaokao.
20. For example, Russia stated that its personal data localization requirement (enacted in 2015) was to "provide extra protection for Russian citizens both from misuse of their personal data by foreign companies and surveillance of foreign governments." Alexander Savelyev, "Russia's new personal data localization regulations: A step forward or a self-imposed sanction?" Computer Law & Security Review, 32 (2016) 128–145, https://doi.org/10.1016/j.clsr.2015.12.003; "Russia's security service tells internet firms to hand over user data: The Bell," *Reuters,* February 12, 2020, https://www.reuters.com/article/us-russia-internet/russias-security-service-tells-internet-firms-to-hand-over-user-data-the-bell-idUSKBN2060UV.
21. Daniel Castro, "India's Intermediary Liability Law Out of Step With Global Norms," Innovation Files blog post, May 11, 2021, https://itif.org/publications/2021/05/11/indias-intermediary-liability-law-out-step-global-norms.
22. "PTA empowered to block online speech critical of government & public officers; gets power to block entire online systems," Digital Rights Monitor, November 18, 2020, https://www.digitalrightsmonitor.pk/pta-empowered-to-block-online-speech-critical-of-government-gets-power-to-block-entire-online-systems/; Sadaf Khan, Zoya Rehman, and Salwa Rana, "The Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2020: A legal analysis" (Media Matters for Democracy, 2020), https://www.digitalrightsmonitor.pk/wp-content/uploads/2021/01/Social-Media-Rules-2020-Legal-Analysis.pdf; "Media Matters for Democracy conducts an initial analysis of the new social media rules and their potential impact on digital rights and economy in Pakistan," Media Matters for Democracy blog post, November 23, 2020, https://mediamatters.pk/media-matters-for-democracy-conducts-an-initial-analysis-of-the-new-social-media-rules-and-their-potential-impact-on-digital-rights-and-economy-in-pakistan/.
23. U.S. International Trade Commission Interactive Trade DataWeb (USITC DataWeb), using data retrieved from the U.S. Bureau of the Census, accessed June 4, 2018, https://dataweb.usitc.gov/.
24. Liana Wong, "Generalized System of Preferences (GSP): Overview and Issues for Congress" (Congressional Research Service, 2022), https://sgp.fas.org/crs/misc/RL33663.pdf.
25. U.S. International Trade Commission Interactive Trade DataWeb (USITC DataWeb), using data retrieved from the U.S. Bureau of the Census, accessed September 12, 2023, https://dataweb.usitc.gov/.

26. Bureau of Economic Analysis, Table 3.3. U.S. Trade in ICT and Potentially ICT-Enabled Services, by Country or Affiliation (Exports; accessed September 13, 2023), https://apps.bea.gov/iTable/?reqid=62&step=9&isuri=1&6210=4#eyJhcHBpZCI6NjIsInN0ZXBzIjpbMSw5LDZdLCJkYXRhIjpbWyJQcm9kdWN0IiwiNCJdLFsiVGFibGVMaXN0IiwiMzU5Il1dfQ==.
27. Jack Caporal, "USTR announces new, beefed-up GSP enforcement scheme," *Inside U.S. Trade,* June 11, 2018, https://insidetrade.com/daily-news/ustr-announces-new-beefed-gsp-enforcement-scheme.
28. "The Digital Trade for Development Act," https://lahood.house.gov/index.cfm?a=Files.serve&file_id=0026F552-DD54-4AFE-9743-46F95E48D76B.
29. Ibid.
30. "Trade Preferences and American Manufacturing Competitiveness Act of 2021," https://www.finance.senate.gov/chairmans-news/wyden-announces-legislation-to-extend-trade-preferences-and-tariff-relief; https://www.finance.senate.gov/download/legislative-text-of-the-trade-preferences-and-american-manufacturing-competitiveness-act-of-2021.
31. Nigel Cory and Rob Atkinson, "The Administration Should Disregard Progressives' Unfair Attacks on Its Digital Trade Agenda" (ITIF, 2023), https://itif.org/publications/2023/05/25/the-administration-should-disregard-progressives-unfair-attacks-on-its-digital-trade-agenda/.
32. "Public Hearings: Initiation of the 2017 Annual Generalized System of Preferences Product and Country Practices Review; Deadlines for Filing Petitions," Regulations.gov, accessed June 11, 2018, https://www.regulations.gov/document?D=USTR-2017-0014-0001; "Active and Recently Completed GSP Eligibility and Country Practices Reviews," United States Trade Representative website, accessed June 111, 2018, https://ustr.gov/issue-areas/trade-development/preference-programs/generalized-system-preference-gsp/current-review-0.
33. Law No. 18-05 of 24 Chaâbane 1439 (corresponding to May 10, 2018); International Trade Administration (ITA), "Algeria -- Country Commercial Guide," (September 14, 2019), https://www.trade.gov/knowledge-product/algeria-ecommerce; United States Trade Representative (USTR), 2021 National Trade Estimate Report on foreign Trade Barriers, (Washington, DC: USTR, 2021), https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf; Algerian Law No. 18-07 of 25 Ramadhan 1439 (Corresponding to June 10, 2018) Relating to the Protection of Individuals in the Processing of Personal Data, available at https://www.dataguidance.com/jurisdiction/algeria.
34. See: GSI/PR Supplementary Norms no. 4 and 19; MP/STI Ordinance no. 20/2016; and Ordinance No. 9, 2018."
35. Brazil Congressman Proposed Digital Services Tax, EY (May 8, 2020), https://taxnews.ey.com/news/2020-1246-brazilian-congressman-proposes-digital-services-tax.
36. Som Sothea, "Law on Electronic Commerce of Kingdom of Cambodia," June 13, 2021, https://commerce-cambodia.com/2021/06/13/law-on-electronic-commerce-of-kingdom-of-cambodia/.
37. USTR, "2023 National Trade Estimate Report on Foreign Trade Barriers," https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf.
38. United National Human Rights Office of the High Commissioner, State of Press Freedom in Cambodia (Aug. 2022), https://www.ohchr.org/sites/default/files/2022-08/press-freedom-cambodia-en.pdf#page=11.
39. Activists: Cambodia's Draft Cybercrime Law, VOA (Oct. 11, 2020) https://www.voanews.com/a/eastasia-pacific_activists-cambodias-draft-cybercrime-law-imperils-free-expression-privacy/6196959.html; Cyberlaw to Address Security Concerns, KHMER TIMES (May 24, 2022), https://www.khmertimeskh.com/501080863/cyberlaw-to-address-security-concerns/; Draft Cybercrime Law

Nearing Completion, PHNOM PENH POST (Sept. 7, 2022), https://www.phnompenhpost.com/national/draft-cybercrime-law-nearing-completion.

40. "African Union National Data Protection Act," UNODC website, https://www.unodc.org/res/cld/document/civ/loi-no-2013-450-relative-a-la-protection-des-donnees-a-caractere-personnel_html/06192013_loi_donne_es_personnelles.pdf.
41. USTR, "2023 National Trade Estimate Report on Foreign Trade Barriers," https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf.
42. Clyde & Co, "Egypt's Data Protection Law enters into force," Clyde & Co, October 19, 2020, https://www.clydeco.com/en/insights/2020/10/egypt-s-data-protection-law-enters-into-force.
43. "Public Notices: Payment Systems and Services Act, 2019," Bank of Ghana website, June 12, 2019, https://www.bog.gov.gh/public-notices/4231-payment-systems-and-services-bill-2019.
44. Global Business Guide, "The OJK Issues Regulation on Implementation of Insurance and Reinsurance Companies," January 2017, http://www.gbgindonesia.com/en/main/legal_updates/the_ojk_issues_regulation_on_implementation_of_insurance_and_reinsurance_companies.php.
45. USTR, "2023 National Trade Estimate Report on Foreign Trade Barriers," https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf.
46. Indonesia, Asia Internet Coalition, submission, https://aicasia.org/category/regions/indonesia.
47. 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.
48. USTR, "2023 National Trade Estimate Report on Foreign Trade Barriers," https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf.
49. "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.
50. 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.
51. "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.
52. USTR, "2023 National Trade Estimate Report on Foreign Trade Barriers," https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf.
53. "Computer and Communication Industry Association (CCIA) Submission to the 2023 National Trade Estimate Report on Foreign Trade Barriers," October, 2022, https://ccianet.org/wp-content/uploads/2022/10/CCIA-Comments-2023-National-Trade-Estimate-Reporting.pdf.
54. Jeff Paine, " Asia Internet Coalition Submission on Regulation on Governance of Private Scope Electronic System Administrator," (Asia Internet Coalition, March 2020), https://aicasia.org/wp-content/uploads/2020/04/AIC-Submission-on-Regulation-on-Governance-of-Private-Scope-Electronic-System-Administrator_26032020_English.pdf; Baker McKenzie, "Indonesia: Indonesia Regulates Foreign Private

Electronic System Operators," Lexology, December 2020, https://www.lexology.com/library/detail.aspx?g=237ba0a4-2616-4106-af25-f26ddbfafc0e.

55. Asia Internet Coalition, translation of Kominfo Circular 3/2021 on the Use of Cloud for the Public Sector.
56. 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.
57. 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.
58. Aliya Seitova and Victoria Simonova, "Kazakhstan strengthens personal data protection by gradually moving toward GDPR standards," JD Spura, January 28, 2021, https://www.jdsupra.com/legalnews/kazakhstan-strengthens-personal-data-9616681/.
59. "Law of the Republic of Kazakhstan dated 24 November 2015 No. 418-V," https://adilet.zan.kz/eng/docs/Z1500000418.
60. Ravil Kassilgov, "Kazakhstan—Localization of Personal Data," Lexology, January 12, 2016, http://www.lexology.com/library/detail.aspx?g=303621d9-e5b7-4115-9d8c-2a5d1d40ed2c; https://adilet.zan.kz/eng/docs/Z1300000094; Aset Shyngyssov et al., "Data Localization Laws: Overview (Kazakhstan)," *Thomson Reuters*, 2019, https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2019/datalocalizationlawsoverviewkazakhstan.ashx?la=en&hash=CAAEA6B82869DD66B3BA8D3E62D05DDE8CBCC7EE.
61. "Resolution of the Government of the Republic of Kazakhstan dated March 30, 2010 No. 246," https://adilet.zan.kz/rus/docs/P100000246_.
62. Anupam Chander and Uyên P. Lê, *Data Nationalism,* 64 Emory Law Journal 677 (2015), https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/; "Order of the Minister of Defense and Aerospace Industry of the Republic of Kazakhstan dated March 13, 2018 No. 38 / НҚ," https://adilet.zan.kz/rus/docs/V1800016654.
63. "The Law of the Republic of Kazakhstan dated 5 July 2004 No. 567," a https://adilet.zan.kz/eng/docs/Z040000567_.
64. "Kenya: Information Communications (Cybersecurity) and (Electronic Transactions) Draft Regulations," (Article 19 working paper, April 2016), https://www.article19.org/data/files/medialibrary/38413/Kenya-Cyber-Security-and-Electronic-Transactions-Legal-Analysis-21-April-2016.pdf.
65. Joseph Kaguru, Dean Wanjala, and Daniel Wanjau, "Recent developments on data privacy and protection in Kenya," *JDSpura*, March, 2021, https://www.jdsupra.com/legalnews/recent-developments-on-data-privacy-and-1051513/.
66. Ibid.
67. USTR, "2023 National Trade Estimate Report on Foreign Trade Barriers," https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf.
68. Jumoke Lambo, "Data Localization Laws: Nigeria," Practical Law, https://www.uubo.org/media/1795/data-localization-laws-nigeria-w-022-1015.pdf.

69. PwC Nigeria, *NITDA Has Issued a Final Notice of Local Content Compliance for ICT Companies*, (accessed December 11, 2015), https://nlipw.com/wp-content/uploads/Guidelines-for-Nigerian-Content-Development-in-Information-and-Communications-Technology-ICT.pdf.
70. KPMG, Nigeria: Tax Provisions in Finance Act, 2019, https://home.kpmg/us/en/home/insights/2020/01/tnf-nigeria-tax-provisions-in-finance-act-2020.html.
71. "Computer and Communication Industry Association (CCIA) Submission to the 2023 National Trade Estimate Report on Foreign Trade Barriers," October, 2022, https://ccianet.org/wp-content/uploads/2022/10/CCIA-Comments-2023-National-Trade-Estimate-Reporting.pdf.
72. Ibid.
73. "Finance Act 2021," Federal Republic of Nigeria Official Gazette, https://www.firs.gov.ng/wp-content/uploads/2022/04/Finance-Act-2021-Gazetted.pdf and https://pwcnigeria.typepad.com/files/finance-act-2021-gazette.pdf; Google, Meta, and Others Raise Nigeria Prices Due to Digital Tax, *QZ* (Mar. 4, 2022), https://qz.com/africa/2137660/google-meta-and-others-raise-nigeria-prices-due-to-digital-tax/.
74. 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; Asia Internet Coalition (AIC), Industry Submission by AIC on Pakistan's Personal Data Protection Bill 2020; Tahir Amin, "Ministry finalizes 'Personal Data Protection Bill'," *Business Recorder,* January 15, 2021, https://www.brecorder.com/news/40051791.
75. "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.
76. Ibid.
77. Ibid.
78. Ibid.
79. 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.
80. "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.
81. Riazul Haq, "Cabinet approves amendments to controversial social media rules," *Dawn,* September 29, 2021, https://www.dawn.com/news/1649144.
82. Ramsha Jahangir, "Govt's revised internet rules fuel tension with tech firms," *Dawn,* June 29, 2021, https://www.dawn.com/news/1632070.
83. International Bank for Reconstruction and Development/The World Bank, "A Single Digital Market for East Africa," (World Bank, 2018), http://documents1.worldbank.org/curated/en/809911557382027900/pdf/A-Single-Digital-Market-for-East-Africa-Presenting-Vision-Strategic-Framework-Implementation-Roadmap-and-Impact-

Assessment.pdf; "Ministerial order N°001/MINICT/2012 of 12/03/2012," https://businessprocedures.rdb.rw/media/Ministerial%20order%20Number%2013-2012%20of%2020-02-2012%20determining%20licence%20fees%20for%20Special%20Economic%20Zones%20developers%20-%20operators%20in%20Rwanda.pdf.

84. Dan Swinhoe, "Senegal to migrate all government data and applications to new government data center," *Data Center Dynamics,* June 23, 2021, https://www.datacenterdynamics.com/en/news/senegal-to-migrate-all-government-data-and-applications-to-new-government-data-center/.
85. "Consultation Paper Processing of Payments in South Africa," South African Reserve Bank, https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Documents%20for%20Comment/Domestic%20Processing%20-%2014%20Nov%202018%20-publication.pdf.
86. "Electronic Communications Act, 2005," https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf.
87. "Thailand: PDPC launches consultation period on rules for cross-border transfer of personal data," One Trust Data Guidance, October, 2022, https://www.dataguidance.com/news/thailand-pdpc-launches-consultation-period-rules-cross.
88. "Computer and Communication Industry Association (CCIA) Submission to the 2023 National Trade Estimate Report on Foreign Trade Barriers," October, 2022, https://ccianet.org/wp-content/uploads/2022/10/CCIA-Comments-2023-National-Trade-Estimate-Reporting.pdf.
89. "The Income Tax (Amendment) Bill of 2023," The Uganda Gazette, March 30, 2023, https://www.parliament.go.ug/sites/default/files/Income%20Tax%20%28Amendment%29%20Bill%2C%202023%20Edited.pdf.
90. "Access Alert: Uganda follows growing trend, implements digital services tax law," Access Partnership, July 20, 2023, https://accesspartnership.com/access-alert-uganda-follows-growing-trend-implements-digital-services-tax-law/.
91. Ulugbek Abdullaev and Eldor Mannopov, "Uzbekistan: Data localization requirement to be effective in April 2021," JD Spura, January 25, 2021, https://www.jdsupra.com/legalnews/uzbekistan-data-localization-3000241/.