ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them

NIGEL CORY AND LUKE DASCOLI | JULY 2021

Data-localization policies are spreading rapidly around the world. This measurably reduces trade, slows productivity, and increases prices for affected industries. Like-minded nations must work together to stem the tide and build an open, rules-based, and innovative digital economy.

KEY TAKEAWAYS

- The number of data-localization measures in force around the world 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.
- Restricting data flows has a statistically significant impact on a nation's economy—sharply reducing its total volume of trade, lowering its productivity, and increasing prices for downstream industries that increasingly rely on data.
- Using a scale based on OECD market-regulation data, ITIF finds that a 1-point increase in a nation's data restrictiveness cuts its gross trade output 7 percent, slows its productivity 2.9 percent, and hikes downstream prices 1.5 percent over five years.
- China is the most data-restrictive country in the world, followed by Indonesia, Russia, and South Africa. Their economies will all suffer for it.
- Policymakers should update laws to address legitimate data-related concerns, but they should ensure people, firms, and governments can maximize the enormous societal and economic benefits of data and digital technologies.
- To build an open, rules-based, and innovative digital economy, countries like Australia, Canada, Chile, Japan, Singapore, New Zealand, the United States, and the United Kingdom must collaborate on constructive alternatives to data localization.

INTRODUCTION

For centuries information has flowed around the world, steadily increasing with the rise of international mail, the first transatlantic cables in the 1850s, and the first transatlantic telephone cable in the 1950s. What is different now is that the Internet creates the potential to send large amounts of data quickly and at virtually no cost to almost any part of the world. Moreover, on this global network, sending data abroad costs no more than sending data domestically. COVID-19 has made clear that data flows are critical to the global economy, enabling both economic responses (e.g., data sharing for medical research, the monitoring and automated control of vaccine production facilities, and the adoption of digital services for business continuity) and societal responses (e.g., family video calls, contact tracing, streaming content for entertainment, and online shopping). Data flows will only continue to rise as more countries and sectors embrace digital transformation.

Data will flow across borders unless governments enact restrictions. While some countries allow data to flow easily around the world—recognizing that legal protections can accompany the data—many more have enacted new barriers to data transfers that make it more expensive and time-consuming, if not illegal, to transfer data overseas. Forced local data-residency requirements that confine data within a country's borders, a concept known as "data localization," have evolved and spread in the four years since the Information Technology and Innovation Foundation's (ITIF) last major report on data flows and localization.[1] Data localization targets a growing range of specific data types and broad categories of data deemed "important" or "sensitive" or related to national security. The justifications policymakers use have also evolved. Misguided data privacy and cybersecurity concerns remain common, but cybersovereignty and censorship are newer, and in many ways, more-troubling motivations given they are broader and more ideologically driven. Some policymakers—especially those in Europe and India—openly call for data localization as part of digital protectionism, while others disguise localization and protectionism by burying them in technical regulations.

The spread of data localization to more countries and data types poses a growing threat to the potential for an open, rules-based, and innovative global digital economy. Data localization makes the Internet less accessible and secure, more costly and complicated, and less innovative. Businesses use data to create value, and many can only maximize that value when data can flow freely across borders. Hence, data localization undermines the impact data-intensive services can have on economic productivity and innovation.[2] For example, a 2018 Organization for Economic Cooperation and Development (OECD) report notes that digitalization is linked with greater trade openness, selling more products to more markets, and that a 10 percent increase in bilateral digital connectivity increased trade in services by over 3.1 percent.[3] The opposite is also true. ITIF's econometric modeling estimates that a one-unit increase in a country's data restrictiveness index (DRI) results (cumulatively, over a five-year period) in a 7 percent decrease in its volume of gross output traded, a 1.5 percent increase in its prices of goods and services among downstream industries, and a 2.9 percent decrease in its economy-wide productivity. The report finds that China, Indonesia, Russia, and South Africa are countries for which their increasing data restrictiveness is leading to their economies experiencing higher prices, lower trade, and reduced productivity.

Forced data localization also undermines the potential for shared governance. Countries can work together to address legitimate concerns about data transfers, such as to prevent espionage, to maintain financial oversight, and to conduct law enforcement investigations, while still allowing data to flow freely. Of course, countries should create robust data privacy frameworks that protect consumers and address national security concerns, but policymakers should do so in a transparent, targeted, and balanced way to avoid unnecessarily costly and restrictive policies given their economic and trade impacts. Many common data protection laws—such as those based on OECD's guidelines on the protection of privacy and cross-border flows of personal data—do not constitute a restriction on digital trade.[4] It is entirely acceptable for ex post accountability for the data exporter if data sent abroad is misused. The cost of abiding by these data protection laws is a typical cost of doing business.[5] This is a crucial distinction to differentiate policymakers in those countries that try to misuse data localization as a legitimate data protection tool when it is not.

The spread of data localization to more countries and data types poses a growing threat to the potential for an open, rules-based, and innovative global digital economy.

As the world emerges from COVID-19, policymakers need to do more to ensure that the global digital economy remains an engine of economic growth and recovery. Thankfully, some countries are bringing this concept to life via new mechanisms, agreements, and frameworks for data flows and governance and digital trade. The first section of this report provides an updated analysis of data localization's use and application and the five main motivations used to justify it. The second section provides a quantitative assessment as to its growing impact. The final section combines analysis and recommendations relating to mechanisms to support data flows and global digital trade and data governance.

The report offers several general recommendations for policymakers:

- Global data governance: Policymakers should provide multiple mechanisms to transfer personal data, encourage firms to improve consumer trust through greater transparency about how they manage data, support the development of global data-related standards, and provide more assistance to developing countries to help with digital economy policy.
- Digital free trade: Policymakers should support rules that protect data flows, prohibit data localization, and only allow narrow exceptions to these provisions at e-commerce negotiations at the World Trade Organization (WTO). Policymakers should also create new tools to enact retaliatory measures against countries that enact data localization and other digital protectionist rules. Policymakers should encourage national and global bodies to conduct surveys about the firm-level impact of data localization. Trade negotiators should develop transparency and good regulatory practices provisions to ensure opaque regulatory rulemaking can't be used to enact barriers to data flows and digital trade.

Specific recommendations make the case that policymakers should:

- Focus on the overarching concept of building "interoperability" between different regulatory systems;

- Pursue new digital economy agreements and mechanisms for cooperation, such as those negotiated by Australia, Chile, New Zealand, and Singapore;
- Work with like-minded countries to create interoperable health data-sharing frameworks. This would support the responsible and ethical cross-border sharing of health and genomic data;
- Make the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) a global model for data governance by opening it up to non-APEC members;
- Support efforts by like-minded, value-sharing democratic countries working together to develop a "Geneva Convention for Data" to establish common principles, processes, and safeguards to govern government access data;
- Develop a targeted strategy to support the adoption of financial oversight frameworks that focus on regulatory access to data rather than the location of data storage; and
- Improve existing, and build new, mechanisms to improve cross-border requests for data related to law enforcement investigations, such as CLOUD (Clarifying Lawful Overseas Use of Data) Act agreements and updated mutual legal assistance treaties (MLATs) to provide timely assistance.

THE EVOLUTION AND SPREAD OF DATA LOCALIZATION CONTINUES TO DEGRADE THE GLOBAL INTERNET ECONOMY

Data localization has evolved to target a growing range of data in more countries. The number of countries that have enacted data localization requirements has nearly doubled from 35 in 2017 to 62 in 2021. The total number of data localization policies (both explicit and de facto) has more than doubled from 67 in 2017 to 144 in 2021. Another 38 data localization policies have been proposed or considered in countries around the world. China (29), India (12), Russia (9), and Turkey (7) are world leaders in requiring forced data localization. Appendix A is a comprehensive and detailed list of explicit, de facto, and proposed or draft data localization measures around the world.

There are three main kinds of data localization. First, some governments restrict the transfer of particular types of data outside their borders. These include personal data; health and genomic data; mapping and geospatial data; government data; banking, credit reporting, financial, payment, tax, insurance, and accounting data; the internal company data of publicly listed companies; data related to user-generated content on social media and Internet service platforms; subscriber data and communications content and metadata for traditional telecommunications and Internet-based communication services; and e-commerce operator data.

Second, countries are increasingly restricting data in broad and vague categories involving data deemed "sensitive," "important," "core," or related to national security, which often impacts a wide range of commercial data.[6] Similarly, the EU and India are moving toward extending restrictions to a broad framework targeting nonpersonal data.[7]

Third, de facto localization is also growing. By making data transfers so complicated, costly, and uncertain, firms basically have no other option but to store the data locally, especially in the face of massive fines. For example, the European Union's removal of data transfer mechanisms,

failure to add new certifications and other new legal tools for data transfers, and ever-ratcheting up of restrictions and conditions for those remaining mechanisms (such as standard contractual clauses) have the potential to make the General Data Protection Regime (GDPR) the world's largest de facto localization framework.[8] Other examples include explicit consent requirements for personal data transfers and the need to submit data transfers for opaque and ad hoc authorization.

Governments enforce these requirements with at least five different types of rules. All these rules are bad, but their impact varies by their design, moving along a sliding scale of restrictiveness (from bad to worst):

- **Local data mirroring.** Firms must first store a copy of data locally before transferring a copy out of the country. This may also involve keeping the most updated version of the data locally.
- **Explicit local data storage.** Firms must physically locate data in the country where it originates. Some cases allow foreign processing of data (after which data must be stored locally).
- **De facto local storage and processing.** Firms store data locally as stringent data transfer requirements (such as getting pre-approval for transfers and explicit consent) and legal uncertainty about data transfers, which, when combined with hefty fines and arbitrary enforcement, create unacceptable risk for firms.
- **Explicit local data storage and processing.** Countries prohibit transfer to other countries.
- **Explicit local—and discriminatory—data processing, routing, and storage.** Some countries use discriminatory licensing, certification, and other regulatory restrictions to require local data storage and exclude foreign firms entirely from managing and processing local data.

THE FIVE RATIONALES FOR DATA LOCALIZATION

Justifications for data localization have evolved. Some policymakers still inadvertently support localization, as they do not understand how firms manage data on a global basis while complying with local laws. However, more policymakers openly support localization as a form of protectionism. More policymakers (such as in France, India, and South Korea) are being creative in using arbitrary and opaque licensing, certification, and other regulatory restrictions to indirectly require data localization (and exclude foreign firms and products). These policymakers seek to avoid scrutiny from trading partners by pushing restrictions deeper into technical and administrative regulations.

Nearly all data localization proposals involve mixed motivations. 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 protectionism, national security, greater control over the Internet, or some combination of these. In some cases, such as India, they use all of them.[9] A telltale sign of hidden motivations is a lack of evidence, transparency, debate, and engagement around a data localization proposal.

This section analyzes the five key motivations policymakers use to justify data localization policies.

Misguided Data Privacy, Protection, and Cybersecurity

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 the best way to protect data is to store it within a country's borders. This misunderstanding remains at the core of many data-localization policies. However, the security of data does not depend on where it is stored.[10]

First, organizations cannot escape from complying with a nation's laws by transferring data abroad. As a result, data localization is not necessary to force an organization to comply with domestic data laws. For example, if a county requires businesses to disclose data breaches, they would have to make this report whether the data breach occurs domestically or abroad. Similarly, businesses cannot circumvent data protection laws by transferring data abroad—laws and contracts can still hold them accountable for how they use data. Most companies doing business in a nation, including all domestic companies and most foreign ones, have "legal nexus," which puts them in that country's jurisdiction. This is crystal clear for firms in financial, payment, and other heavily regulated sectors, given their need to apply for licenses to operate.

It is nearly inevitable that some policymakers will propose data localization as they reflexively and mistakenly believe that the best way to protect data is to store it within a country's borders.

Second, 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. The nationality of who owns or controls servers or which country these devices are located in, has little to do with how secure they are. For example, one of the most notorious hacks occurred against domestic, on-premise servers of the U.S. government in the U.S. Office of Budget and Management data breach.[11]

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. Data security depends on the technical, physical, and administrative controls implemented by the service provider, which can be strong or weak, regardless of where the data is stored.

Policymakers focus on the location of data storage, in part, because they do not want to tackle the more challenging factors that actually contribute to good cybersecurity, such as building greater cybersecurity awareness by users and firms and encouraging firms and government agencies to adopt and remain committed to best-in-class cybersecurity practices and services. Good cybersecurity is just as much about the people involved in managing, protecting, and accessing the data as it is about the data itself, as they are central to most cybersecurity incidents, such as the failure to update vulnerable systems or credentials being lost via phishing attacks.

Data localization actually undermines cybersecurity. First, it prevents the sharing of data to identify IT system vulnerabilities and help firms detect and respond to cyberattacks. For

example, in 2020, India's Securities and Exchange Board released a cybersecurity circular that requires financial firms to localize a broad range of data that would do just this.[12] Firms need to share data to reconcile if cyberattacks (such as those in China, India, Russia, or elsewhere) are new or known. Sharing system vulnerability information also allows cybersecurity providers to identify vulnerabilities.

Second, data localization precludes cloud service providers from using cybersecurity best practices, such as through "sharding," wherein data is spread over multiple data centers. This gets to the broader point: While cloud computing does not guarantee security, it will likely lead to better security because implementing a robust security program requires resources and expertise, which many organizations (especially small and medium-sized ones) lack. But large-scale cloud computing providers are better positioned to offer this protection. For example, certain cloud providers offer their users advanced encryption tools to allow them to retain and use encryption keys before data is uploaded, thereby preventing third parties, including the cloud companies themselves, from accessing their data.[13]

"Data Sovereignty" Subsumes Digital Protectionism as a Leading Motivator

Digital protectionism remains a key motivation behind many countries enacting data localization practices, but it has been subsumed into a broader narrative around cybersovereignty (also called data sovereignty or digital sovereignty) and control.

Data localization's use for protectionism has evolved in recent years. More and more policymakers look to use it to favor local firms as they realize that data-driven innovation is at the heart of modern competitiveness and they haven't made the long-term investments in education, infrastructure, and other enabling factors that actually help firms and economies become more competitive.[14] For example, India's Non-Personal Data Governance Framework initially included a proposal to force firms to share anonymized datasets (undoubtedly to help local firms). Europe, India, South Africa, and others use localization to target U.S. firms explicitly.[15] Proponents often call for "policy space" for developing countries to enact protectionist-based, state-directed digital industrial policy strategies.[16]

Policymakers commonly portray cybersovereignty as a strong yet nebulous concept, usually referring to the assertion of state control over data, data flows, and digital technologies.[17] That it helps countries "take back control" and "sovereignty" from foreign technology firms and trading partners (mainly the United States, but increasingly China as well) offers added appeal to them.[18] Misconceptions about data and cybersovereignty miss the point that a complex interplay of economic, governance, social, and political factors determines a country's position on digital issues. Policymakers deliberately—and deceptively—use these concepts to condense complex phenomena into catchy phrases.

Proponents think that forcing firms to store data locally enhances the state's agency and that of their own firms and people. At best, the agency gained by data localization is illusory. In many cases, it is counterproductive. And in the case of authoritarian countries, it is predatory given the agencies data localization supports are those involved in surveillance and social and political control. So it's no surprise that authoritarian countries such as China and Russia are the most significant users of these concepts (and data localization) as they align with their main political interests—maintaining power through access and control over data. Both countries frequently cite sovereignty as part of advocacy to create a top-down, state-directed global Internet (as

opposed to the open, multistakeholder-based approach favored by democratic countries). The push for cybersovereignty among countries that are not inherently authoritarian gives cover to countries like China and Russia.

Europe is a leading offender. European leaders such as German chancellor Merkel and French president Macron explicitly call for both digital protectionism and data sovereignty.[19] The fact that senior European policymakers think that data stored on a foreign cloud service represents lost sovereignty shows how little some understand how firms manage data, and how much they prioritize this misguided sense of control.[20] Europe tries to position itself as a moral leader of digital regulation, using concerns over data protection and artificial intelligence (AI) to cloak their discriminatory and restrictive policies. Europe's protectionist intent appears in nearly every digital policy proposal. Europe's GDPR is evolving into the world's most significant de facto data localization framework. Europe's draft data strategy pushes for data localization and asserts that the EU needs cloud providers owned and operated in Europe.[21] Likewise, Europe's white paper on AI advocates data localization precepts.[22] It is also evident in the proposal for a European cloud via GAIA-X.

At best, the agency gained by data localization is illusory. In many cases, it is counterproductive. And in the case of authoritarian countries, it is predatory.

Policymakers, academics, civil society advocates, and business leaders in many developing countries have turned to the related concept of "digital colonialism" to use data localization as part of broader efforts to disadvantage or block foreign tech firms.[23] It's most frequently used in the outdated and ideologically driven narrative about the "global north" and "global south."[24] It's popular in India, South Africa, and the United Nations Conference on Trade and Development (UNCTAD). Many proponents are ideologically driven, opposing capitalism, big businesses, the United States, and, in some cases, the use of data and digital technology itself.[25] Local tech firms often try to take advantage. India's richest man told India's prime minister to take steps to end "data colonization" by global firms, saying Indians (presumably meaning his e-commerce operations) should own and control data.[26]

Data Localization for 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—both 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, thereby impacting privacy, data protection, and freedom of expression.[27] China retains broad and vague legal authority in its laws to potentially access data for national security, public interest, and political purposes.[28] The lack of an independent judiciary and the opaque nature of these laws make it hard to judge how China uses these broad powers.[29] Yet, this doesn't stop these countries from referring to "data privacy" as a motivation for localization.[30]

Recent laws introduced in Pakistan and Vietnam highlight how data localization does not lead to greater data privacy—but rather 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, such as 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).[31]

Data localization is central to Vietnam's evolving online censorship and surveillance regime. Vietnam's Law on Cybersecurity requires online firms to store personal and other data types locally and establish a local office in Vietnam. Its motivation is broad and vague: to protect national security, social order and safety, social ethics, and the health of the community.[32] Firms must have a license and at least one server in Vietnam for inspection at any time, store detailed information about users and their activities, and remove illegal content within three hours of notice.[33] Concerns about how Vietnam could use this to facilitate government access to data are real given the country does not have a dedicated, independent data protection agency; the responsible agency is the Ministry of Public Security.[34]

Digital authoritarian governments—led by China and Russia—see physical access to data centers as a critical enabler of surveillance and political control.

Pakistan is also 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, and to intervene on behalf of law enforcement agencies to ask social media companies to provide user data.[35] 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.

Data Localization for Law Enforcement and Regulatory Oversight

Countries continue to use law enforcement and regulatory concerns about cross-border access to data, both to justify data localization and as an excuse for digital protectionism. Some policymakers say data localization is the only way to get local and foreign firms to respond to requests for data from law enforcement and financial regulators. This reflects the mistaken belief that firms can avoid oversight and requests for data by simply transferring data out of a country, and that firms can pursue some form of regulatory or legal arbitrage in terms of picking and choosing which country's laws they follow and which they don't.[36] Data localization requirements do not change who is responsible for the data, regardless of where it is stored.

Some countries support data localization due to the lack of effective cross-border law enforcement legal tools and treaties. If data is stored locally, the thinking goes, foreign governments will not be able to halt investigations by stopping providers from fulfilling government requests. This mistaken belief was central to proposed localization elements in India's draft data protection law.[37] However, policymakers in India fail to acknowledge all the contributing factors. For example, Indian law enforcement often files MLAT requests that are incomplete, poorly drafted, or inappropriate (or requests that aren't related to criminal activity).[38]

For example, after the Department of Justice (DOJ) advised an Indian prosecutor to fill out an MLAT in 2012 to obtain U.S.-stored information, the court instead issued a summons for several U.S. tech firms for not cooperating.[39] Other policymakers use this law enforcement motivation to support localization as a disguise for different goals, such as surveillance and protectionism.

Law enforcement-motivated data localization often stems from the fact that policymakers do not want to address the underlying issues with existing legal mechanisms to improve the process of making cross-border requests for data. The transnational nature of crime and digital services means that countries will inevitably need other countries' help—even if they have localization policies in place. For example, a European Union report states that electronic evidence in some form is relevant in around 85 percent of total criminal investigations and that 55 percent of investigations require cross-border access to electronic evidence.[40] Current legal tools definitely need upgrading. For example, conflicting laws can put firms in a "catch 22" scenario wherein they face lawful requests for access to data from one country the release of which may be legally prohibited in another.[41] Governments also have mismatched legal-assistance treaties and laws.

Data localization requirements do not change who is responsible for the data, regardless of where it is stored.

Financial regulatory oversight agencies use localization to target publicly listed companies, payment services, banks, and other financial firms, as they think it's the only way to access data they need for their oversight responsibilities. U.S. financial regulators initially sought the option for data localization (before, thankfully, backtracking) for financial oversight.[42] The Reserve Bank of India cited the need for "unfettered" access to data for monitoring purposes in trying to justify its payments data localization requirement. Yet, policymakers in China, India, Turkey, and elsewhere that use this motivation for localization routinely fail to provide evidence that they face genuine cross-border issues related to financial oversight.[43] The false promise of "unfettered" access is made clear by the fact that even with local storage, regulators will still have to request firms to decrypt the data, in line with relevant legal checks and balances, before the data can be viewed.

Whether it is law enforcement or regulatory related, data localization is not the silver bullet policymakers think it is for improving access to data. The self-defeating nature of localization becomes clear given the scenario in which every country requires localization, thus preventing the cooperation that will still inevitably be needed given the interconnected nature of the Internet, such as emails between two people and providers in different jurisdictions. But the potential for regulatory-motivated digital fragmentation is much broader. For example, medical labs must disclose confidential data about infectious diseases, firms must share clinical trial data with medical authorities, banks must disclose data on suspicious transactions, and accountants and their clients must share data for tax audits. It's up to rule-of-law and rights-respecting countries to set up appropriate mechanisms to improve these processes.

Data Localization Motivated by Geopolitical Risks and Financial Sanctions

Some countries use data localization, alongside other policies, in preparation for largely hypothetical (and unlikely) international financial sanctions. Some see the national payments system as part of the country's critical infrastructure and that the use of global payment networks

represents a systemic, geopolitical, and sovereign risk, as these payment services are not locally owned.

Russia is the lead example. Russia required payments data localization as part of an initiative to create a Russian payment system (called MIR) after international sanctions in 2014 targeted Crimea-based services (forcing Visa and Mastercard to end services there). These sanctions raised the hypothetical risk of it being cut off from the global financial system.[44] Russia also forced its banks to accept and issue MIR credit cards and use MIR for government-related payments.[45] This motivation is thus closely tied to Internet sovereignty, but again showing the overlap, also relates to protectionism, given it represents (digital services) import substitution. However, Russia is unique, as its disregard for international law and norms makes it a frequent target of sanctions. The vast majority of countries will never face international financial sanctions.

Despite the extraordinarily low probability of sanctions, Indonesia, Mexico, South Africa, and Vietnam have all misused national security and sovereign risk to justify payment services-related restrictions, including data localization. For example, in 2018, the South African Reserve Bank imposed a moratorium prohibiting the migration of domestic transaction volumes from BankservAfrica (South Africa's bank-owned domestic payment switch) to international payment schemes. It stated that "there are potential sovereign/geopolitical and financial stability risks to SA from sole reliance on offshore processing of domestic transactions."[46] Mexico's financial regulators released draft rules requiring payments services to use local computing services as part of their license application.[47]

ESTIMATING THE COST OF RESTRICTIONS ON DATA FLOWS

Maximizing the value of data means enabling it to move. Innovation and economic growth are increasingly supported by how firms collect, transfer, analyze, and act on data. This section provides a quantitative analysis of the effects of restrictions given the relationship between data flows and economic performance. While econometric analysis provides an indicative estimate of the economic impact (given challenges with measurement and specificity), it is still important to do to reinforce to policymakers the negative effects of restrictions on data flows.

Estimating the Impact That Data Restrictiveness Has on Prices, Trade, and Productivity

ITIF's model calculates a composite index—the data restrictiveness linkage (DRL)—to estimate the linkage of downstream industries with national data restrictiveness (based on the data intensity of those industries). We further examine the impacts that changes in data restrictions have on total factor productivity (TFP), value-added price indices (PVA), and gross output volumes (GOVs) at the industry level in each country (through the EU-KLEMS database). The model runs separate log-linear regression models between DRL and these three economic indicators to approximate the percentage changes in productivity, prices, and trade volumes incited by changes in a country's restrictions on data transfers (table 1). It is based on econometric best practices as demonstrated by OECD and European Center for International Political Economy (ECIPE).[48] However, it differs in that it benefits from updated data from the U.S. Census ICT Survey, the OECD Product Market Regulation (PMR) database, it covers countries not covered in past models, and compares trade volumes.[49] Appendix B details the data and methodology.

Data Restrictiveness Index

ITIF uses sub-indicators from the OECD PMR Indicators database to develop a proxy measurement of how restrictive a nation's rules are for cross-border data transfers. By taking the unweighted averages of select PMR sub-indicators, ITIF computes the data restrictiveness index (DRI) of 46 countries that OECD has PMR data available for in between 1998 and 2018. Since PMR data updates are published every 5 years, DRI of these 46 available countries is only calculated every five years (2018, 2013, 2008, 2003, and 1998). DRI is resultantly measured on a scale between 0 and 6, with 6 indicating the most data restrictive. As countries impose additional data regulations such as localization, and other government barriers and administrative requirements that limit the movement of data, their DRI increases.

PMR data is central to our model as it captures several regulations that countries use to restrict the use and transfer of data, such as explicit localization measures and restrictions related to administrative costs like requiring data protection impact assessments or data protection officers. Our selection of sub-indicators used to calculate DRI between countries over time is informed by best-practice modeling data restrictiveness via PMR proxy data as performed by a 2016 study by CIGI & Chatham House.[50]

While the PMR Indicators database reports on a wide range of regulatory activity beyond just those that determine data restrictiveness within countries, the database also provides several PMR sub-indicators that more narrowly capture restrictions on data flows. PMR "medium-level" sub-indicators distinguish more specific types of regulation. "Low-level" indicators refer to the narrowest ranges of regulatory activity observed, further breaking down OECD's medium level indicators of PMR into more specific subjects. Pre-2018, DRI is calculated using the two medium-level indicators "Administrative Barriers to Startups" and "Administrative and Regulatory Opacity." For 2018, DRI is calculated using five low-level PMR sub-indicators: "Assessment of Impact on Competition," "Interaction with Interest Groups," "Complexity of Regulatory Procedures," "Barriers in Service Sectors," and "Barriers in Network Sectors." These five fully comprise the two medium-level indicators, "Simplifications and Evaluations of Regulations," and "Barriers in Service and Network Sectors," which are preferred due to their correlations with pre-2018 data and overlap of regulatory activity.

ITIF's method of calculating DRI for 2018 had to adjust for a change in how the OECD reported the PMR index and sub-indicators. This was necessary to ensure the model's use of PMR data was consistent with pre-2018 data and measurements. To do this, our model selected several PMR sub-indicators based on correlation trends between the pre-2018 years of DRI and between DRI and overall PMR of the same year, as well as by the content of sub-indicators that most specifically relate to regulations that restriction data flows. (Appendix B, equation 1 provides the details of the calculation to form DRI measurements pre-2018, whereas equation 2 provides the calculation used for 2018 DRI. Table 1 presents correlation trends that further justify the selection of sub-indicators).

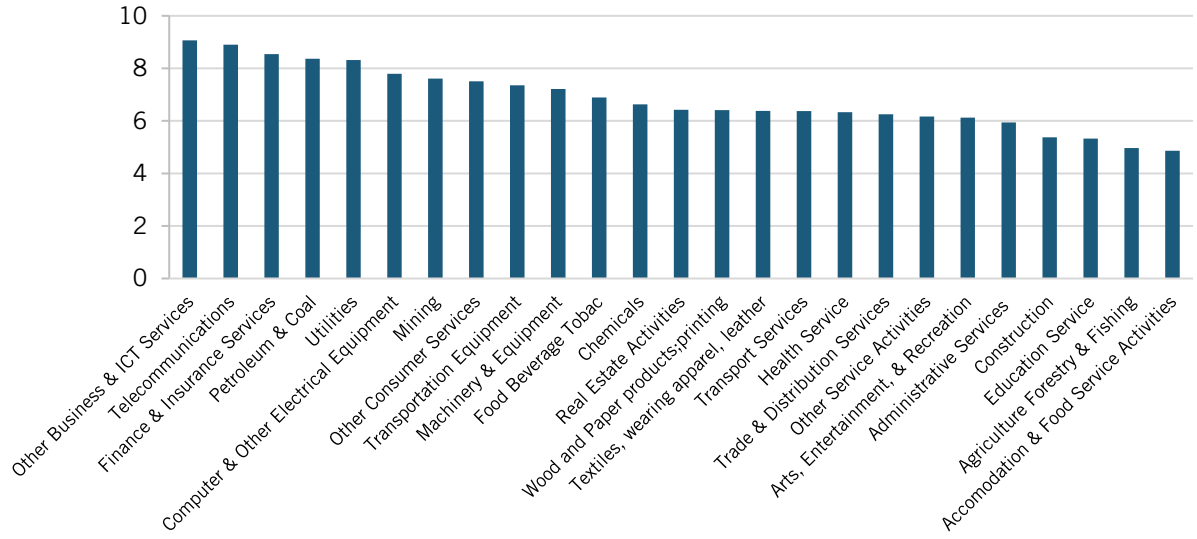
Data-Intensity Modifier

ITIF's model assumes that data restrictions have greater effects on economic industries that are more reliant on data and data-related tools and services. 2018 studies by ECIPE provide best practices for calculating the data intensity of industries and using those scores to estimate industry-level.[51] A data-intensity modifier (DIM) following this methodology is calculated by

selecting a country exogenous to the model, the United States, for a given reference year. For each industry noted in the KLEMS categorization, we calculate a DIM using 2013 U.S. Census ICT Survey data on noncapitalized software expenditure and 2013 Bureau of Labor Statistics (BLS) employment data by industry to calculate the ratios of data-related service expenditures per worker in each industry (figure 1).

DIM ratios (computed in equation 3, Appendix B) measure data intensity between industries and enable us to weigh national DRI measurements in countries over time at the industry level. This allows the model to assess the straightforward point: that more data-intensive industries are more economically impacted by data restrictions than are non-data-intensive ones. And while calculating DIM exogenously helps control for issues of endogeneity within countries' downstream industries, the model further assumes equal technologies between countries. However, that assumption is commonly made among the literature of econometric modeling on this subject and is of less concern when the set of countries within a regression model are all economically developed ones.

Figure 1: Data intensity by KLEMS industry (as log of noncapitalized software expenditure per worker)



Data Restrictiveness Linkage and Regression Modeling

Lastly, the model develops a composite index—the data restrictiveness linkage (DRL)—linking the measurement of national data restrictiveness in a given year to the data-intensity of a given industry to produce observations in terms of country-year-industry. The DRL is the independent variable tested in regression modeling against economic performance observed at the level of country-year-industry. Equation 4 of Appendix B (also below) provides the calculation for a given country-year-industry's DRL, which is simply the product of DRI and DIM.[52]

(4)

$$DRL_{xty} = DRI_{xt} * DIM_{y}$$

The model is used to test three separate regressions modeling trade outputs, prices, and productivity to examine the economic impact national data restrictions have on downstream industries. Dependent variable data at the level of country-year-industry is most widely provided by the EU-KLEMS database, from which we select three measurements to be regressed against DRL: gross output volume (GOV) to indicate trade activity (equation 5), TFP to indicate economic productivity (equation 6), and price index based on value added to indicate prices of goods and services (equation 7).

While OECD PMR data allows 46 countries to be sampled, the constrained availability of data in the EU-KLEMS database means that industry-level trade data is limited to 28 developed OECD member nations. These 28 countries include in both OECD and EU-KLEMS data comprise the set of countries included in regression analysis. The downside is this omits many developing and non-OECD countries. However, the model's core components (DRI and DIM, and the impact they have on trade volumes, prices, and productivity) can be applied to any country, as they are representative estimates of data usage and the effect of restrictions (such as in Russia, China, and Indonesia). Equations 5, 6, and 7 provide the full regression models used to produce results shown in table 2.

(5) [Trade Volume Regression: Volume of Gross Output Traded using 2010 Reference Prices (GOV)]

$$\ln(GOV_{xyt}) = \phi + \theta * DRL_{x\,y\,t-1} + \delta_{xt} + \gamma_{yt} + \varepsilon_{xyt}$$

(6) [Productivity Regression: Total Factor Productivity]

$$\ln(TFP_{xyt}) = \phi + \theta * DRL_{x\,y\,t-1} + \delta_{xt} + \gamma_{yt} + \varepsilon_{xyt}$$

(7) [Prices Regression: Aggregate Price Index for Valued Added on Industry Goods and Services (PVA)]

$$\ln(PVA_{xyt}) = \phi + \theta * DRL_{x\,y\,t-1} + \delta_{xt} + \gamma_{yt} + \varepsilon_{xyt}$$

GOV_{xyt}, PVA_{xyt}, TFP_{xyt} are the economic measurements for a given country-industry-year. ϕ is the equation intercept (β_0 estimate in log-linear regressions). ϑ is the coefficient of DRL (β_1 estimate in log-linear regressions). $DRL_{x\,y\,t-1}$ is the DRL for a given country-industry-previous year. ε_{xyt} represents the equation error term. The model further controls for issues of endogeneity by implementing a time lag, wherein economic indicators in a given year are regressed against the DRL of the previous year. Change in economic performance is also not often immediately observable in the year new policy is enacted, further supporting a time lag. Lastly, this model provides controls so that regression results of DRL's impact on GOV, PVA, and TFP are accurately estimated by providing fixed effects for country-year and industry-year level. Fixed effects are added based on best econometric practice and control for the many country-, time-, and industry-specific factors not able to be accounted for that assuredly affect GOV, PVA, and TFP.

These dependent variables are taken as natural logs to be regressed because log-linear regression coefficients best estimate the percentage changes associated with unit changes in the independent variable of interest.

General Model Results: Data Restrictiveness Has a Significant Impact on Prices, Trade, and Productivity

The model shows that restricting data flows has a statistically significant negative impact on an economy. Table 2 provides greater statistical detail on regression results. All coefficient estimates are statistically significant above the 90 percent confidence level, with PVA having an estimate p-value just above 0.05 (95 percent confidence level). TFP and GOV, however, are both highly statistically significant above the level of 99 percent confidence. Interpreting the coefficient estimates of DRL by the log-linear regression interaction provides the percentage changes in GOV, TFP, and PVA associated with a one unit increase in a country's DRI.

Table 2: Regression results

Dependent Variable	Coefficient Estimates of Data Restrictiveness Linkage	Pr(>|t|)	Standard Error	Number of Observations	R-Squared
ln(TFP)	-0.02918 ***	0.000937	0.0088	1691	0.1165
ln(PVA)	0.01448*	0.063356	0.0078	2351	0.2271
ln(GOV)	-0.07306***	0.00005	0.018	1990	0.9496

Note: Robust standard errors in parentheses, *** p<0.001, ** p<0.05, * p<0.1
Source: Authors.

Restrictions on data flows are most strongly associated with a decrease in GOVs. Gross output measures the total amount of goods and services traded, including both final and intermediate output. By interpreting the regression coefficient -0.073, the model finds that on average, a 1.0 unit increase in a country's DRI (from the sample of 28 OECD member countries) is associated with a 7.05 percent decrease in its gross output traded. This naturally gives a relationship between data restrictions and gross output that is higher than a more traditional measurement of economic growth such as gross domestic product (GDP), which accounts for only final outputs produced. Loss in gross output surely still indicates a loss in GDP, but by a notably smaller proportion given that GDP excludes measurement of intermediate outputs. While the highest data-intensive industries identified in the model would be most affected, such as Telecommunications or Other Business and ICT, nearly every single sector of economic activity requires some usage of data to facilitate trade, from mining to retail to construction.

More significant data restrictions also artificially increase the prices (and reduce the supply) of goods and services that rely on data, such as data analytics, targeted advertising, and software used to manage global workforces, product networks, and supply chains. The model estimates

that countries that restrict data transfers experience lower trade volumes, leading to increased prices of goods due to reduced supply. Data localization may also force a more-innovative and price-competitive service provider from the market, thus allowing a more expensive or inferior product to seize market share.

Over five years, a one-unit increase in a country's DRI is associated with a 7 percent decrease in its gross output traded, a 2.9 percent decrease in productivity in downstream industries, and a 1.5 percent increase in prices among the goods and services those industries provide.

The regression model's results support this intuitive analysis of the trade and economic impact resulting from countries' data localization policies. The model finds that a one-unit increase in a country's DRI is associated with a 1.5 percent increase in the prices of goods and services that downstream industries produce (in aggregate, over five years). This result means that as data becomes more heavily restricted, the remaining output among industries becomes more expensive to consumers than would otherwise be expected in a scenario wherein there exists free flows of data and data-driven goods and services.

Data and data-driven tools are increasingly important determinants of productivity, which is essential to long-run economic growth. Estimating TFP helps policymakers understand how efficient industries are at using their production inputs and how innovative those industries are at utilizing new technologies. Our regression modeling on TFP finds that a one-unit increase in a country's DRI is associated with a 2.9 percent decrease in productivity in downstream industries. This negative productivity shock can cause GDP to decrease, with a 2.9 percent decrease in a country's productivity translating to notable losses in living standards and economic growth. Without access to the most competitive and innovative data-related inputs, firms must use available labor and capital less efficiently, which reduces productivity and, of course, translates into decreased economic growth at the national-economy level.

Specific Model Results: China, Indonesia, Russia, and South Africa All Suffer From Data Restrictiveness

Applying the model's statistically significant relationships on data restrictiveness, lower productivity, less trade, and higher prices allows one to estimate the economic costs in countries of interest beyond the OECD sample set. While the model's findings on the relationships between increased data restrictions and changes in TFP, PVA, and GOV are identified in the context of developed OECD countries, the model's findings still have value in being applied to countries beyond this context, given the degree of statistical significance identified in variable relationships and the lengths of controls placed in the model via multiple fixed effects. Since econometric modeling using a proxy variable (DRI, and in turn, the compositive index DRL) is not an exact measurement of national data restrictions per country, some countries may naturally be underestimated or overestimated. Proxies are further constrained in their extended application by the availability of data for observations outside a studied sample. However, analysis of a proxy variable still identifies significant trends in data on average.

ITIF selected four nations—China, Indonesia, Russia, and South Africa—whose DRI and changes in DRI (between 2013 and 2018) strongly support qualitative findings of expanded data restrictions in this report and are therefore known to be well fitted by the proxy variable used.

The countries listed in table 3 all have data in the OECD's PMR database for both 2013 and 2018 (the most recent years available), allowing us to calculate their changes in DRI over that time (unfortunately, there isn't data for India for both years, otherwise it would also be added). The ranking includes all 46 countries with DRI able to be calculated between 2013 and 2018 (where a rank of first indicates the most data restrictiveness). Figures 2 and 3 of Appendix B details 2013 and 2018 rankings for these 46 countries. By multiplying the changes in DRI observed between 2013 and 2018 by the percentage changes in GOV, TFP, and PVA associated with a unit increase in DRI, the model can estimate the economic costs borne by countries that imposed additional restrictions on data (model produces an aggregate total for 2013 to 2018).

Changes in the DRI ranking align with the report's analysis and listing of data localization measures. China was the most restrictive country in both 2013 and 2018. Over those six years, China's DRI increased by 0.25 points. Our econometric analysis estimates that over five years, these restrictions decrease output by 1.7 percent and productivity by 0.7 percent and leads to a 0.4 percent rise in prices among downstream industries.

Table 3: Economic costs of case studies due to changes in DRI

Country	2013 DRI	2013 DRI Ranking	2018 DRI	2018 DRI Ranking	DRI Difference	Total Cumulative Change in Gross Output Volume (2013–2018)	Total Percent Change in Productivity (2013–2018)	Total Percent Change in Prices (2013–2018)
China	3.88	1st	4.13	1st	0.25	-1.7%	-0.7%	0.4%
Indonesia	2.03	19th	3.14	4th	1.11	-7.8%	-3.2%	1.6%
Russia	1.38	39th	2.08	12th	0.70	-4.9%	-2.0%	1.0%
South Africa	2.17	16th	3.47	2nd	1.30	-9.1%	-3.7%	1.9%

Note: DRI rankings are based out of 46 countries maintained in both 2013 and 2018 within the OECD "Indicators of PMR" database. As a result, this ranking excludes notable countries such as India and Argentina.
Source: Authors.

Indonesia, Russia, and South Africa are all notable cases that reflect their growing interest in enacting barriers to data flows in recent years. Both Indonesia's and South Africa's DRI rankings increased by 1.0 point between 2013 and 2018. These two countries face the most significant marginal losses by changes in data restrictiveness policy over this time span. The model estimates that over five years from 2013 to 2018 (cumulatively), South Africa's volume of gross output fell by 9.1 percent, productivity fell by 3.7 percent, and prices rose by 1.9 percent due to increased restrictions imposed on data flows.

For Indonesia, the model estimates that over the five years, its more-significant data restrictions reduced GOVs by 7.8 percent, lowered productivity by 3.2 percent, and raised prices by 1.6 percent. In the case of Russia, its heightened data restrictions between 2013 and 2018 cost an

estimated 4.9 percent reduction in trade volume, a 2.0 percent reduction in productivity, and a 1.0 percent increase in prices of goods and services on average nationally.

These losses in trade and productivity due to increased data restrictiveness held back these countries' potential economic growth. Had South Africa and other countries not enacted more restrictions on data, their economies would not have suffered the expensive marginal costs of data localization estimated by the model.

RECOMMENDATIONS TO BUILD GLOBAL DATA GOVERNANCE AND CONSTRUCTIVE ALTERNATIVES TO DATA LOCALIZATION

Building an open, rules-based, and innovative global digital economy will depend on a small group of proactive and ambitious countries working together. This path ahead reflects the fact that there is no global forum for cooperation and progress on data issues—and nor should there be at this stage. Former Japanese prime minister Abe deserves a lot of credit for putting data governance and localization on the global agenda with his concept for "data free flow with trust," which is a vision wherein openness and trust exist in symbiosis, not as contradictions.[53] However, it is still conceptual and has not been defined.

Countries that support this goal will need to work together to develop new norms, rules, cooperation mechanisms, and agreements to address legitimate concerns raised by cross-border data flows while supporting the free flow of data. These initiatives can then form the foundation for broader debate, adaptation, and adoption to expand to more issues and countries. It will be challenging to develop a common agenda, even among core countries such as Australia, Canada, Chile, Japan, New Zealand, Singapore, the United Kingdom, and the United States. It will be difficult, if not impossible, to make meaningful progress in any forum that involves China, Russia, and others that support digital protectionism and control. It's hard to include Europe given its inability to genuinely engage and collaborate with counterparts unless its privacy preferences prevail over everyone else's.

This section outlines key recommendations to build global data governance. It starts by providing high-level recommendations.

Recommendations on data governance best practices:

- Governments should provide multiple mechanisms for the cross-border transfer of personal data. These mechanisms should be accessible to firms of all sizes. Countries should explicitly mention acceptable frameworks and standards for transfers.
- Governments should encourage businesses to improve transparency on how they manage data, including on a global basis, such as by regularly disclosing information about government requests for data.
- Governments should support global, market-led, voluntary, and consensus-based efforts to develop and use data and digital technology standards, such as via multistakeholder forums and intergovernmental forums (e.g., OECD).

- Governments should protect cloud-based government data and services by ensuring that cloud providers are audited and certified against national and international standards, sector-specific regulations (such as health care and financial), national certifications (e.g., U.S. FedRAMP, Germany C5, Australia IRAP), and global accreditations (e.g., ISO 27001 and ISO 27018).[54]
- Developed economies should provide technical assistance and capacity-building assistance to developing economies to help them build their data governance framework.

Recommendations to support digital free trade and counter digital protectionism:

- Support an ambitious outcome on data flows at the e-commerce negotiations at the WTO, including an explicit prohibition on data localization and narrow and detailed exceptions. The United States and others should exclude China and Russia and others that do not support ambitious outcomes. A weak result may be worse than no deal at all.
- To create reciprocity, policymakers from digital free-trade countries should develop new countermeasures against countries that enact data localization and other digital protectionist measures. Firms from digital protectionist countries shouldn't benefit from open digital markets.
- Policymakers should encourage national, regional, and global organizations to conduct detailed surveys about the impact of data localization and other barriers to cross-border data transfers.[55]
- Digital free-trade countries should advocate for transparency and good regulatory practices as part of trade agreements, such as allowing parties to request the publication of impact assessments to ensure that digital regulations are appropriate, proportionate, and effective.

Build Interoperability Into Global Data and Digital Economy Governance

Policymakers should put the concept of "digital interoperability" at the center of their strategy for developing rules for the global digital economy. Interoperability means that countries enact laws to address data privacy, cybersecurity, and other issues in broadly similar ways so that they each provides a similar level of protection or similarly addresses a shared objective, even if their specific legal and regulatory frameworks differ. At its most fundamental level, interoperability is the ability for firms to transfer and use data and other information across applications, systems, services, and jurisdictions.[56] Interoperability is the most realistic goal for global data governance. It accounts for the fact that countries have differing legal, political, and social values and systems, and there is no one law for any specific data-related issue.

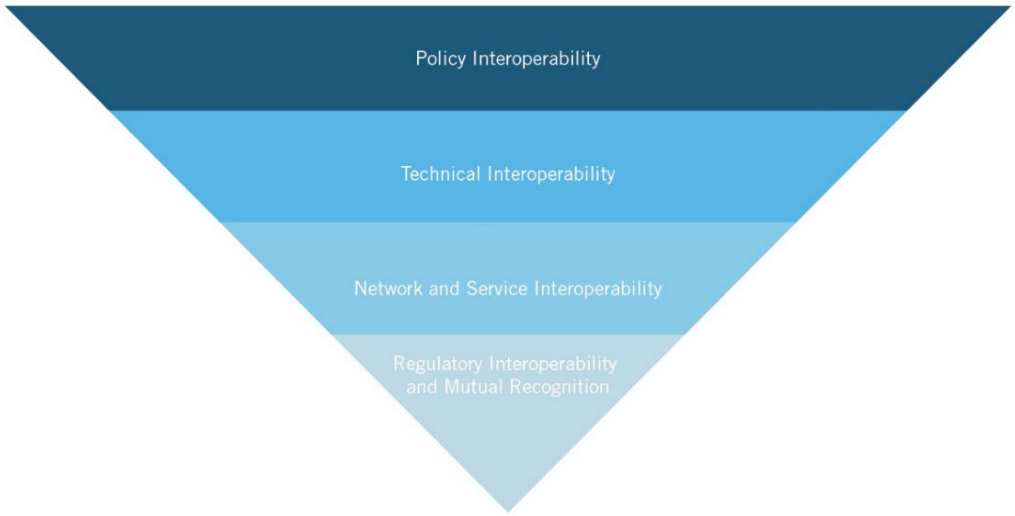
Policymakers should put the concept of "digital interoperability" at the center of their strategy for developing rules for the global digital economy.

Interoperability is central, yet often invisible, to the integration of the global digital economy.[57] Interoperability depends on governments, businesses, and other stakeholders developing common ways to mitigate risks and address shared concerns. Interoperability has many benefits. It supports innovation, competition, and consumer choice as it facilitates access and development of more data and data-driven services, which reduces barriers to market entry.[58] It

improves regulatory outcomes and trust as jurisdictions with similar legal concepts and approaches address issues that arise from cross-border data flows similarly (thus avoiding regulatory conflict, arbitrage, and avoidance). In this way, interoperability supports reciprocity given regulatory compatibility.[59] Interoperability can also build trust between trading partners, as they have some assurance that counterparts won't use data localization to target their firms, and their firms' digital products, unfairly.

While data privacy is a critical focal point for the concept of interoperability, it extends much further to cybersecurity, payment services, financial oversight, and any number of digital processes and services that relate to trade.[60] What interoperability looks like in practice depends on the specific sector and policy concern. Stakeholders working to build interoperability in the global digital economy should look to develop and use different tools at different technological layers and levels of integration (figure 1).

Figure 1: The different layers of global digital interoperability



At the first stage, stakeholders can build policy interoperability by supporting early research and discussions about potential best practices (such as to address bias, violent content online, certain uses of AI, e-identity, e-invoicing, or other issues) and joint pilot projects and regulatory sandboxes to test potential regulations. All stakeholders (government, private sector, academia, and others) should have the opportunity to participate, given these early discussions represent brainstorming and the testing of regulatory ideas.

At the second stage, stakeholders can build technical interoperability so that data and digital services can move across jurisdictions, and between different applications and infrastructure, with straight-through processing—that is, processing data and digital services without additional human intervention. Otherwise, differential and restrictive regulations can prevent technical systems from working across borders. Application Programming Interfaces (APIs) and international standards are two key tools that create common protocols and specifications that allow different services and applications to connect and work across jurisdictions.[61] For example, the International Organization for Standardization and the International Electrotechnical Commission joint committees are developing standards to facilitate technology interoperability,

including of AI, big data, and Internet of Things systems.[62] Digital economy agreements cite specific international standards to ensure interoperability between payment systems.[63] There are also initiatives such as the U.S. National Institute of Standards and Technology's Cybersecurity Framework and APEC's Cybersecurity Workstream that seek to build a risk- and standards-based approach to cybersecurity.

At the third stage, stakeholders can build network interoperability so multiple parties can connect their individual systems to a broader network to ensure seamless processing. Much like the Internet, networks need common rules and regulations to support reliability and access. For example, payment network interoperability involves bilateral agreements and connections (e.g., between a payment network and a central bank or a remittance provider) to provide processing across multiple networks for complex cross-border transactions.

At the fourth and final stage, governments build regulatory interoperability through mutual recognition agreements between countries, recognizing other countries' respective regulatory approvals or certifications as valid in their own country, and explicitly referencing specific standards and legal frameworks (such as APEC CBPR).

Pursue New Digital Economy Agreements and Mechanisms for Cooperation

The global digital economy is in dire need of new rules to protect digital trade and data flows. However, these rules are not sufficient given how fast technology and regulatory requirements change. Technology and associated business models outpace traditional trade agreements and domestic regulations related to data and digital trade. This mismatch in speed will continue.[64] Digital trade needs early and ongoing engagement to ensure regulatory interoperability, both now and in the future. It is the reverse approach in Europe—rush to regulate and restrict and then consider international implications (when reforms to address barriers to trade are hard to do). Digital trade cannot be just one and done as in traditional trade negotiations. Digital economy agreements should be living agreements.[65] Countries such as Canada, Japan, the United States, and others that support an open, innovative, and integrated global digital economy should join or emulate the digital economy agreements Australia, Chile, New Zealand, and Singapore have negotiated.[66]

Digital economy agreements combine legally binding and enforceable commitments on well-known digital trade issues (such as data localization) and soft commitments to cooperate on emerging regulatory issues (via memorandums of understanding (MOUs)). They can adjust to the changing nature of digital trade, technology, and regulation. This involves proactively bringing domestic regulatory agencies into trade discussions when they are only just starting to think about new rules for digital issues. The nonbinding nature of the cooperation enables experimentation and allows partners to address new problems quickly without getting distracted by the horse trading involved in traditional trade negotiations.

Digital economy agreements represent a flexible and accessible approach to building interoperability between digital economies at varying levels of development. In particular, the Chile-New Zealand-Singapore Digital Economy Partnership Agreement (DEPA) and its modular structure for its various issue (AI, e-identities, data flows, open data, fintech, e-invoicing, etc.) areas are open to all who can meet its ambitions.[67] Canada and Korea have expressed interest in joining. Just as APEC's early and ongoing digital economy discussions built the foundation for the ambitious digital rules in the Comprehensive and Progressive Agreement for Trans-Pacific

Partnership (CPTPP), so too can these digital economy modules provide the basis for new norms and rules.[68]

Digital economy agreements raise different challenges to traditional trade negotiations. Mainly, they require genuine buy-in from regulatory agencies to work with their trade colleagues and their foreign counterparts. MOUs and soft commitments to cooperate in trade agreements are a dime a dozen. The benefits of digital economy agreements depend on parties bringing the commitment to cooperate to life. For example, Australia and Singapore have already done a joint study to identify ways to cooperate on new digital standards. They are also developing pilot projects for shared e-identify and e-invoicing policies.[69]

The benefits of digital economy agreements are harder to quantify than are the econometric modeling of tariff cuts in traditional trade agreements. Firms benefit from the certainty of knowing they can transfer data as part of cross-border digital trade and innovation. In the long term, firms also benefit from early regulatory interoperability by avoiding barriers to digital trade related to new laws. Regulatory engagement also builds trust and confidence among regulators (and consumers) that trade commitments on data do not impede regulatory responsibilities (for privacy, etc.) and can improve oversight as it allows information sharing and joint investigations.

Support Data-Driven Health Research via Interoperability Frameworks

Countries that recognize the value in supporting data-driven health research should work together to create domestic and international frameworks to facilitate the reasonable, responsible, and ethical cross-border sharing of health and genomic data. Data-driven health services and research holds enormous societal and economic benefits. From screening chemical compounds to optimizing clinical trials to improving post-market surveillance of drugs, the increased use of data and better analytical tools such as AI hold the potential to transform drug development, leading to new treatments, improved patient outcomes, and lower costs.[70]

Yet, health and genomic data are among the most common targets of data localization.[71] Health data requires specific attention, as it often involves sensitive personal data. However, enacting overly severe restrictions on its use does nothing to help improve health outcomes. For example, multiple joint EU-U.S. health research initiatives have ended or been severely restricted due to the EU's GDPR.[72] A growing number of health firms and researchers have called for governments to step in as restrictive data privacy rules prevent cross-border health research. For example, in February 2020, leading health researchers called for an international code of conduct for genomic data following the end of their first-of-its-kind international data-driven research project that ran into significant issues when using data centers across various regions.[73]

Policymakers should create clear rules and frameworks to allow people, firms, universities, and public agencies to share health data. For example, the Global Alliance for Genomics and Health brings together hundreds of health care, university, and biopharmaceutical and technology companies to create ways to enable the responsible, voluntary, and secure sharing of genomic and health-related data.[74] The World Economic Forum's Breaking Barriers to Health Data is also working to build a pilot project that uses federated data systems to share genomic data.

Use APEC's Cross-Border Privacy Rules to Build a Global Data Privacy Framework

Australia, Canada, Japan, Singapore, the United States, and others interested in developing a high-standard framework for data protection and digital trade should use APEC's Cross Border Privacy Regime to create a global interoperable model for data governance.

Europe's push for harmonization—that every country adopt its ever-shifting and restrictive approach to data privacy—is misguided and untenable in the long term. There is no single data privacy law. Countries should ignore European privacy officials' critical view of interoperability, which threatens their strict adherence to privacy fundamentalism.[75] There is no way every country will harmonize rules on government surveillance, government access to data, and data privacy. As U.S. Deputy Assistant Secretary for Services Christopher Hoff tweeted, "A lot of awesome things about the GDPR but there have been 13 adequacy decisions in the past 26 years and one keeps getting knocked down. So interoperable frameworks ... have to be the future."[76]

APEC's CBPR is an accountability-based mechanism that facilitates privacy-respecting data flows.[77] Firms must implement a set of data privacy policies consistent with the APEC Privacy Framework, such as those on accountability, notice, choice, collection limitation, integrity of personal information, uses of personal information, and preventing harm. An APEC-approved accountability agent audits and certifies companies meet these commitments. Each CBPR member country's data privacy agency is responsible for enforcement. Despite being in place for some years, CBPR is still in its early stages, with only around 40 certified companies, such as Apple, Cisco, IBM, Tencent (their Singapore entity), and Mastercard. Thus far, Australia, Canada, Chinese Taipei, Japan, Mexico, Singapore, South Korea, and the United States have joined CBPR.

Countries that recognize the value in supporting data-driven health research should work together to create domestic and international frameworks to facilitate the reasonable, responsible, and ethical cross-border sharing of health and genomic data.

Existing CBPR members should open CBPR to non-APEC members so it can become a global (rather than regional) model for data governance. The United States has proposed this.[78] CBPR would be attractive to a diverse range of countries. Other APEC and non-APEC countries could join the system, the benefits of which would grow with each new member. The Philippines is already in the process of joining CBPR. Adding Brazil, Chile, Colombia, New Zealand, Peru, the United Kingdom, and others would make it a global framework. A global CBPR would be attractive to governments as it would focus on core principles and accountability (rather than strict legal harmonization), recognizing that there is no one-size-fits-all approach to privacy. CBPR certification would also be attractive to firms as it would mean that they would essentially be subject to one privacy regime for data transfers between all CBPR members. It would provide enormously valuable economies of scale in terms of incentivizing firms to undergo certification.

The United States and others would need to create a new CBPR outside of APEC, as China and Russia would likely oppose efforts to make reforms within APEC (even though they are not members of CBPR). CBPR would essentially become a global data privacy certification mechanism that countries could recognize as a valid legal transfer mechanism in domestic laws

(as Bermuda has done, even though it is not in APEC).[79] Ultimately, a new global CBPR also presents an opportunity for Australia, Japan, the United States, and others to bring to life a clear alternative data governance model to the EU's restrictive GDPR and China's model of digital control and protectionism.

Build a Framework for Government Access to Data

Like-minded, value-sharing democratic countries should work together to develop a "Geneva Convention for Data" to establish common principles, processes, and safeguards to government access to data. Such an agreement could also settle questions of jurisdiction, establish rules of transparency, create better cooperation for legitimate law enforcement requests, and limit unnecessary access to data by governments. Like-minded countries need to find a way to develop a common approach that balances privacy, trade, law enforcement, and national security interests, as concerns about mass government access to data underpin many data localization proposals worldwide.

The Snowden revelations about U.S. government surveillance created the first major wave of data localization proposals. Since then, concerns—real and imagined—about foreign government access to data have led to greater data localization worldwide, even if these concerns are often selectively and hypocritically applied (such as in Europe). Concerns about Chinese government access to data is motivating a second wave of restrictions.

A new global CBPR also presents an opportunity for Australia, Japan, the United States, and others to bring to life a clear alternative data governance model to the EU's restrictive GDPR and China's model of digital control and protectionism.

Government access to data, especially for national security-related surveillance, is an extraordinarily sensitive issue. Despite its sensitivity, a tightrope to progress has appeared. In 2021, the G7 put the issue on its agenda and tasked OECD to provide research and advice, including a comparative assessment of frameworks that will hopefully identify commonalities, conflicts, and gaps. This is enormously useful and will hopefully provide the basis for constructive discussions.[80]

The best chance of developing a common approach would be via a small group of democratic, rule-of-law countries—brought together due to shared values and interests and a commitment to digital innovation—to discuss pragmatic ways to balance competing equities, including privacy expectations, national security concerns, economic interests, and democratic values. The goal would be to move away from creating nation-based clouds and instead move toward value-based clouds. It would be pragmatic by creating common oversight and accountability measures to reduce costs and improve trust. Ideally, any such Geneva Convention for Data would settle questions of jurisdiction; set common terminology, safeguards, and remedies; improve accountability and transparency; provide some independent oversight; and increase cooperation and understanding between national security, data protection agencies, and the broader public.

Focus on Access, Not Location: Support Financial Regulatory Oversight and Data Flows

Australia, Japan, Singapore, the United Kingdom, and the United States should develop a financial data governance strategy to advocate that financial, banking, securities exchange, and payment regulators focus on access to data rather than where it's stored.

Financial data is among the most targeted categories for localization. Yet, in the logical end state where many countries enact localization, all will be hampered because today's global digital economy means there will inevitably be cross-jurisdictional data. Several enlightened financial regulators—usually reticent to give up any semblance of control—have worked with their trade officials and foreign counterparts on new legal frameworks and mechanisms for cooperation. The goal is to support cross-border data flows while ensuring they still have access to data for oversight purposes.[81]

Like-minded, value-sharing democratic countries should work together to develop a "Geneva Convention for Data" to establish common principles, processes, and safeguards to government access to data.

Recommendations:

- Leading countries and their regulators need to develop a global financial data strategy to create "trust" mechanisms between financial regulators to ensure financial oversight does not impede financial data flows and innovation. Financial regulators from Australia, Singapore, the United Kingdom, and the United States demonstrate how this can be done via new MOUs that provide certainty about regulatory responsibilities, improve cooperation between regulators, and give assurances to firms that financial data can move freely.[82]
- Leading countries should advocate for clear and detailed financial data governance and transfer rules in trade agreements, such as in the U.S.-Mexico-Canada Trade Agreement and the Australia Hong Kong Free Trade Agreement.[83]
- Build out the G7's role as a central forum for leading countries and institutions to manage shared concerns about financial data flows and governance. It already involves leading governments and institutions, such as the Financial Stability Board, the Bank for International Settlements, and the International Monetary Fund.
- Leading countries should pursue greater bilateral engagement to help encourage as many countries as possible (and not in the G7/G20) that the same principles and processes are relevant. Building understanding among financial regulators through engagement, workshops, and conferences will be a slow process. Still, it is essential to get them onboard with enacting the proper framework for managing financial data across jurisdictions.

Improve Mechanisms to Help Law Enforcement Make Cross-Border Requests for Data

The globalization of criminal evidence should drive reforms regarding how law enforcement can access communications and other records in other countries as part of legitimate investigations while abiding by privacy and human rights protections. Criminals should not escape the law simply because police cannot access the data they need efficiently. Unfortunately, in the

absence of updated legal mechanisms, there is the potential for a legal arms race calling for mandatory data localization requirements, which will ultimately hurt all law enforcement efforts to deal with what is a global problem. The following recommendations proceed along a sliding scale from least to most advanced, depending on the country and its situation.

Countries such as India and Indonesia should review and reform domestic legal frameworks to enable more efficient cross-border access. For example, the EU's "e-evidence" proposal streamlines cooperation between service providers and law enforcement in the bloc.[84] Central to this effort would be a working group with diverse stakeholders, including representatives from different government departments, the private sector, civil society organizations, researchers, and experts in international law to formulate reforms and model data transfer agreements.[85] There are various issues involved in improving legal cooperation and compatibility: the standard of proof, authorized authorities and the judicial or independent validation of requests, necessity and proportionality, the ability for service providers to challenge requests, the types of crimes covered, and others.[86]

Countries should pay attention and provide the necessary resources to improve existing legal processes and treaties, as existing legal processes and treaties are out of date, needlessly complex, and often delayed due to poorly resourced local agencies.[87] At the moment, MLATs remain the dominant international framework for enabling cross-border data access. The MLAT process is not working well. For example, the U.S. government can take up to 10 months to complete MLAT requests (leading to a massive backlog), while requests from the United States to Ireland take only 15 to 18 months.[88] Meanwhile, some countries take years to respond to requests, while others, such as Russia, often do not respond at all.[89]

Countries should sign on to the Budapest Convention on Cybercrime—the world's first cybercrime treaty, negotiated 20 years ago—and support ongoing efforts to improve it via a new (second) protocol. This new protocol would help law enforcement agencies secure evidence from service providers in foreign jurisdictions.[90] The proposed language of the second protocol focuses on five major provisions: language of requests, videoconferencing, emergency mutual legal assistance, direct disclosure of subscriber information, and giving effect to foreign orders for the expedited production of data.[91]

Criminals should not escape the law simply because police cannot access the data they need efficiently. Unfortunately, in the absence of updated legal mechanisms, there is the potential for a legal arms race calling for mandatory data localization requirements

At the most advanced stage, countries should consider new legal mechanisms that make the exchange of data for law enforcement purposes more efficient while still providing privacy and other safeguards. For example, the EU-U.S. Umbrella Agreement, the EU-U.S. Terrorist Finance Tracking Program Agreement, and the U.K.-U.S. CLOUD Act executive agreement represent useful models. They incorporate commonly recognized global privacy principles while accounting for local interpretation and different legal structures. And overall, they work without impeding data flows.[92]

The United States should pursue more CLOUD Act agreements, just as other countries should consider reforms to allow them to enter negotiations. The United States' first CLOUD Act

agreement with the United Kingdom established a baseline for talks with Australia and the European Union.[93] They provide a lawful mechanism for law enforcement in either the United States or the other signatory to request data directly from a service provider in the other country without going through the mutual legal assistance process.[94] CLOUD Act agreements do not give law enforcement agencies any new legal authority to acquire data. They simply help like-minded, rights-respecting countries improve the exchange of data for legitimate law enforcement investigations.[95] Furthermore, the United States has made clear that it wouldn't pursue CLOUD Act agreements with countries that do not respect the rule of law and fundamental human rights.[96]

CLOUD Act agreements are in everyone's best interest. They minimize potential conflicts of law between countries, thus providing legal certainty for both firms and law enforcement agencies. If anything, non-U.S. law enforcement agencies benefit more from CLOUD Act agreements, as many of the world's leading service providers are American. It helps firms because it is a clear, efficient framework. The CLOUD ACT is also a direct tool to counter data localization. It requires DOJ to provide a written certification that a country "demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet."[97]

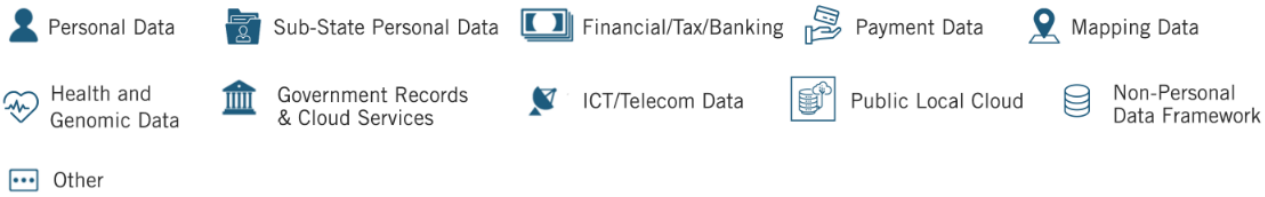
CONCLUSION

Data-driven innovation and digital trade are only going to become more central to the global economy. Governments need to update laws to address legitimate data-related concerns that arise, but this should be done in a considered way so that people, firms, and governments can maximize the enormous societal and economic benefits of data and digital technologies. Restricting the movement of data does nothing to help improve societal or economic outcomes. The recommendations show how like-minded countries can develop shared governance arrangements that can work across legal systems, create reciprocity and nondiscrimination, and build-in independent redress and oversight, all the while allowing data flows.

Meanwhile, digital protectionists and scofflaws such as China and Russia refuse to support digital free trade or join global efforts to improve law enforcement cooperation on cybercrime.[98] What is particularly crucial is that countries that support shared digital governance need to dedicate far more resources to help the many "swing states" that have not enacted localization and have not yet decided to follow the EU or China's model of restrictions and control. The success or failure of this engagement and these new agreements and legal mechanisms will go a long way toward shaping the Internet of the future and whether it remains open, integrated, and innovative or closed, fragmented, and based on state control.

APPENDIX A: LIST OF DATA LOCALIZATION MEASURES

This a comprehensive list of explicit, de facto, and proposed data localization policies around the world, organized by specific region, and in some cases, country.



AFRICA

Country	Type of Data	Data-Localization Policy
Cote-d'Ivoire		**Indirect and De Facto Localization** 2013: Cote-d'Ivoire enacted privacy laws which 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).[99]
Ghana		**Direct and Explicit Localization** 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.[100] 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 is wholly owned by the Central Bank of Ghana). However, there was significant industry concerns, so the final implementing directive has not yet been issued.
Kenya		**Indirect and De Facto Localization** 2019: Kenya's Data Protection Act excluded explicit data localization provisions from in 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. Regulations implementing these provisions are being developed. **Proposed Measures** 2021: Kenya's released draft data protection regulations (to implement the Data Protection Bill) requires 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 systems 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.[101] 2018: Kenya released a draft Data Protection Bill for comment that included a number of provisions that either directly or indirectly lead to data localization.[102] Kenya's Data Protection Bill (part VI, section 44) states: Every data controller or data processor shall ensure the storage, on a server or data center located in Kenya, of at least one serving copy of personal data to which this bill applies; The cabinet secretary shall prescribe, based on strategic interests of the state or on protection of revenue, categories of personal data as critical personal data that shall only be processed in a server or data center located in Kenya; and Cross-border processing of sensitive personal data is prohibited.[103] 2016: 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.[104]
Nigeria		**Direct and Explicit Localization** 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.[105] 2011: The Central Bank of Nigeria enacted 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.[106]

Rwanda		**Direct and Explicit Localization** 2012: Rwanda enacted a regulation that all critical information data within 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.[107] **Indirect and De Facto Localization** 2017: Rwanda's telecommunications regulator fined MTN (a telecommunications company that is a subsidiary of South Africa's MTN Group) US$8.5 million (10 percent of its annual turnover) for maintaining Rwandan customer data in Uganda and for running its IT services outside the country in breach of its license.[108]
Senegal		**Direct and Explicit Localization** 2021: Senegal announced that it will move all government data and digital platforms from foreign servers to a new national data centre in hopes of strengthening its digital sovereignty.[109]
South Africa		**Direct and Explicit Localization** 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.[110] **Indirect and De Facto Localization** 2013: South Africa's Protection of Personal Information Act (the POPI Act), which makes the transfer of personal information outside of South Africa subject to certain exceptions, which raise potential concerns about how these rules will be interpreted and enforced, as they could become de facto data localization tools, especially given its requirement for explicit consent for transfers.[111] **Proposed Measures** 2021: 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.[112]

EUROPE

Country	Type of Data	Description
Andorra		**Indirect and De Facto Localization** 2004: According to the Protection of Personal Data Law, personal data can only be transferred freely to states deemed sufficiently secure in their cyber capabilities. Personal consent must be obtained to transfer data to an insecure state.[113]
Armenia		**Indirect and De Facto Localization** 2015: According to the Law on Personal Data, personal data may only be transferred cross-border when there is personal consent, or it is necessary to finish processing previously consented to by the individual. A transfer permit is required to transfer personal data to states deemed insufficiently secure.[114]
Azerbaijan		**Indirect and De Facto Localization** 2010: According to the Law on Personal Data, cross-border personal data transfers are prohibited if the transfer creates a threat to the national security of the Azerbaijan Republic, or if the transfer is going to a country not deemed sufficiently secure. Personal data can still be transferred to an insecure country if the individual consents to it, however.[115]
Belgium		**Direct and Explicit Localization** 2005: According to Companies Code – Article 463, the company register of shareholder and register of bonds must be kept at the office, or since 2005 can be stored electronically as long as they are readily accessible at said office.[116] 1992: According to the Income Tax Code – Article 315, income tax documents must be kept at the disposal of the office where they have been kept, prepared, or sent.[117] 1992: According to VAT Code – Article 60, VAT invoices must be stored in Belgium or another EU member state.[118]
Bosnia and Herzegovina		**Indirect and De Facto Localization** 2006: According to the Law on Protection of Personal Data, personal consent, contractual necessity, or vital interest are needed to transfer personal data cross-border to a state deemed insufficiently secure. However, there is no specific list of which states Bosnia and Herzegovina views as secure, so the individual data controller is responsible for making this decision.[119]
Bulgaria		**Direct and Explicit Localization** 2012: According to the Gambling Act, when applying for a gaming license all relevant data must be stored on a server in Bulgaria. Communications equipment and the central computer must be located in the EEA or Switzerland.[120]

Cyprus		**Direct and Explicit Localization** 2007: Cyprus has failed to replace several restrictive provisions under the Directive on Data Retention, which was declared invalid by the Court of Justice of the European Union (ECJ). This directive required data operators to retain certain categories of traffic and location data (excluding the content of those communications) for a period between six months and two years and to make them available, on request, to law-enforcement authorities for the purposes of investigating, detecting, and prosecuting serious crime and terrorism.[121]
Denmark		**Direct and Explicit Localization** 2007: According to the Audit Act (section 45), financial records for government institutions must be stored domestically. This data can be stored abroad as long as a copy is made monthly and stored in Denmark.[122] 2006: According to the Bookkeeping Act (section 12), financial records must be stored either in Denmark or one of the Nordic countries.[123] **Indirect and De Facto Localization** 2011: According to the Danish Data Protection local authorities' data cannot be processed outside Denmark without a standard contractual clause. Software commonly used in offices such as Dropbox, Microsoft Office 365, and Google Apps therefore cannot be used until a standard contractual clause is agreed upon.[124]
European Union		**Indirect and De Facto Localization** 2020: The July 2020 decision by the European Court of Justice (ECJ) to invalidate the EU-U.S. Privacy Shield will have an immediate and potentially long-term impact on the thousands of organizations that relied on it to legally transfer data abroad. By making transfers of European personal data so costly and complicated, if not illegal, the European Union's General Data Protection Regulation (GDPR) is becoming a de facto data localization requirement.[125] 2019: Originally announced in 2019, France and Germany have been spearheading a project titled "GAIA-X" that would create a European cloud system in an effort to claim "digital sovereignty" and end reliance on U.S. cloud companies.[126] It is also portrayed as a "trusted cloud" for EU member states' public data.[127] 2018: According to the General Data Protection Regulation, personal data may flow freely between European Economic Area (EEA) states as well as select states deemed sufficiently secure in their data protection. In order to transfer data to any other state, there must be binding contractual agreements, the consent of the data

		subject, or the data transfer is necessary to carry out a contract for the data subject.[128] Through the US-EU Privacy Shield Framework, the United States was one of the countries allowed free data transfers with the EU. However, since a 2020 CJEU decision, Privacy Shield's adequacy decision has been invalidated[129] **Proposed Measures** 2021: Portugal (as president of the EU) proposed for a European Data Governance regulation that would restrict foreign governments' access to European industrial data, impose more obligations to transfer data held by a European public body, to ask for explicit consent if the public data relates to a person, and to create a European Data Innovation Board to "advise and assist" the European Commission when deciding to restrict "highly sensitive" industrial data flows.[130]
Finland		**Direct and Explicit Localization** 1997: According to the Accounting Act, a copy of accounting records must be stored in Finland. The data can be stored in another EU member state if immediate access is guaranteed.[131]
France		**Direct and Explicit Localization** 2016: A ministerial circular announced that data produced by public administrations cannot be stored in a non "sovereign" (i.e., foreign) cloud, as this data is to be considered archives and stored domestically.[132] **Proposed Measures** 2021: Two French tech giants have announced plans to create a trusted cloud ("Cloud de Confiance") called "Bleu." Bleu will meet the sovereignty requirements to be used by French public bodies. This is part of the wider GAIA-X project to make an EU-wide sovereign cloud.[133]
Georgia		**Indirect and De Facto Localization** 2014: According to the Law on Protection of Personal Data, cross-border transfers of personal data are only permitted to select countries deemed sufficiently secure in their data protection. Transfers to any other state must be approved by the Georgian Data Protection Authorities.[134]
Germany	 	**Direct and Explicit Localization** 2017: According to the German Telecommunications Act, telecommunications providers must store data on phone numbers, the time and place of communications (except for emails), and involved IP addresses for four to 10 weeks on servers within Germany.[135] 2013: According to the Tax Code, persons and firms that are required to keep books and records must keep them within Germany. There are some exceptions for multinational companies.[136]

		2013, According to the Act on Value Added Tax, all VAT invoices must be stored within Germany. When these invoices are stored electronically, they can be stored within another EU member state; however, the tax authority must be notified of the location of the data servers, and have the ability to access and download the data.[137] 2008: According to the German Commercial Code, accounting documents and business letters must be stored on servers within Germany.[138]
Greece		**Direct and Explicit Localization** 2011: According to Law No. 3971/2011, retained data on traffic and localization must remain within Greece.[139]
Italy		**Indirect and De Facto Localization** 1972: According to Presidential Decree no. 633, accounting data for VAT declarations can only be kept in a third country if that country has signed a convention with Italy regarding the exchange of information for direct taxation. Therefore, all EU member states qualify.[140]
Kosovo		**Indirect and De Facto Localization** 2010: According to the Law on the Protection of Personal Data, to transfer data to a country that has not been deemed sufficiently secure in its data protection, the Kosovar data protection authorities must be notified and give authorization, and these transferred will only be approved if there is individual consent, contractual necessity, or vital interest.[141]
Luxembourg		**Direct and Explicit Localization** 2012: According to the Circular CSFF 12/552, financial institutions must process data within Luxembourg, except with explicit consent or for an entity of the group to which the institution belongs.[142]
Malta		**Indirect and De Facto Localization** 2003: According to the Data Protection Act, a cross-border transfer of personal data must be notified to the Commissioner's Office.[143]
Moldova		**Indirect and De Facto Localization** 2012: According to the Law on Personal Data Protection, to transfer data to a country that has not been deemed sufficiently secure in its data protection, the Moldovan data protection authorities must be notified and give authorization, and these transferred will only be approved if there is individual consent, contractual necessity, or vital interest.[144]
Monaco		**Indirect and De Facto Localization** 1993: According to the Protection of Personal Data Act, personal data can only be transferred to states deemed insufficiently secure in their data protection with consent, vital interests, contractual necessity, or the authorization of

		the Monégasque data protection authorities on the basis of appropriate contractual clauses.[145]
Montenegro		**Indirect and De Facto Localization** 2012: According to the Personal Data Protection Law, personal data can only be transferred to states deemed insufficiently secure in their data protection with consent, contractual necessity, vital interest, or authorization from the data protection authorities.[146]
Netherlands		**Direct and Explicit Localization** 1995: According to the Public Records Act, records that have been stored in archives in certain locations in the Netherlands must be stored within the country, this applies to paper and electronic records.[147]
North Macedonia		**Indirect and De Facto Localization** 2005: According to the Law on Personal Data Protection, personal data can only be transferred to states deemed insufficiently secure in their data protection with consent, contractual necessity, vital interest, or authorization from the data protection authorities. Authorization from the data protection authorities can be obtained with a written data transfer agreement, preferably modelled off EU standard contract clauses.[148]
Poland		**Direct and Explicit Localization** 2009: According to the Polish Gambling Act, data on legal gambling activity must be archived in real time on a server in Poland.[149]
Romania		**Direct and Explicit Localization** 2015: According to Law No. 124, all data related to the provision of remote gambling services, including records and identification of the players, the stakes placed and the winnings paid out, must be stored within Romania.[150] **Indirect and De Facto Localization** 2001: According to the Data Protection Law, any cross-border transfer of personal data requires notification to the National Supervisory Authority for Personal Data Processing (NSAPDP), and requires NSAPDP approval if to a country deemed insufficiently secure in its data protection.[151]

Russia		**Direct and Explicit Localization** 2021: Russia released a draft (although it seems to already be enforced) law that included a range of conditions and restrictions on foreign firms using the Internet and telecommunication services (especially Facebook, Twitter, Google, and others) to provide services to more than 500,000 Russian users within a 24-hour period, including storing all personal data locally and that such foreigners setup a branch or representative office.[152] 2019: Russia enacted a two-year ban on the public procurement of data storage from foreign firms. Policymakers justified the ban on the need to protect Russia's "critical informational infrastructure."[153] 2018: Russia enacted another set of Yarovaya amendments that required companies to retain a broader range of communications content for six months, to store this data on Russian servers, and make them available to the authorities on demand without judicial oversight.[154] In 2019, Russia enacted additional amendments that internet service providers store data, as prescribed by the Yarovaya amendments, using only Russian-manufactured technical means.[155] 2016: Russia enacted new laws (the first of the so called "Yarovaya" Amendments) that require telecommunications and certain internet companies to retain copies of all contents of communications for six months (including text messages, voice, data, and images) in Russia for up to three years and to this data to authorities on request and without a court order.[156] 2014: Russia's Federal Law No. 242-FZ "On Amending Certain Legislative Acts of the Russian Federation Regarding Clarifying the Personal Data Processing Procedure in Information and Telecommunication Networks'' require personal data localization. After initial collection and storage, it can be transferred overseas (subject to conditions). It does not prohibit remote access to personal data stored in Russia. Any subsequent modification to the personal data should also be performed first in Russia.[157] In 2019, Russia's Federal Security Service required companies to install special equipment giving the FSB automatic access to their information systems and encryption keys to decrypt user communications without authorization through any judicial process.[158] Russian policymakers have justified these rules by citing a need to protect state security, the Russian internet, and the privacy of Russian users. 2014: According to Federal Law No. 161-FZ "On the National Payment System," international payment cards must be processed locally. International payment systems

		must transfer their processing capabilities for Russian users to the local state-owned operator.[159] 2013: Russia enacted a regulation that requires all "credit institutions" (presumably banks and other financial institutions, although it's unclear) should store all data locally.[160] It does not detail whether this is a strict localization requirement or mirroring requirement.[161] **Indirect and De Facto Localization** 2009/2016: The Bank of Russia has issued recommendations, such as Recommendations RS BR IBBS-2.22009 and Recommendations RS BR IBBS-2.9-2016, which imply that financial institutions should store certain sensitive (confidential) data (the scope of which is defined very broadly and would include personal data) in Russia. While these are not normative acts and thus not binding, they are authoritative and financial institutions follow them in practice.[162] 2012: Russia has licensing and certification requirements (relating to protection of confidential information, as well encryption licenses, and certification of the information systems used for the storing and processing the data) for credit and financial institutions and the data they manage that, in practice, can only be satisfied by Russian cloud storage providers.[163]
San Marino		**Indirect and De Facto Localization** 1995: According to The Law Regulating the Collection of Personal Data, in order to transfer personal data on any citizen or company to any third country, authorization is required from the data protection authorities, though there are no specific conditions that need to be met to obtain this authorization.[164]
Serbia		**Indirect and De Facto Localization** 2009: According to The Law on Personal Data Protection, in order to transfer personal data to a country not deemed sufficiently secure in its data protection, authorization from the Serbian data protection authorities is required.[165]
Sweden		**Direct and Explicit Localization** 1999: According to the Swedish Accounting Act, firms' annual financial reports and balance sheets must be physically stored in Sweden for seven years.[166] **Indirect and De Facto Localization** 2019: Financial services are de facto required to physically store data within Sweden as The Financial Services Authority requires physical access to data servers.[167]

Switzerland		**Indirect and De Facto Localization** 2020: Cross-border data transfers of personal data to countries deemed insufficiently secure in their data protection requires the use of standard contract clauses or binding corporate rules.[168] The list of insufficiently secure countries includes the United States after a 2020 decision that the Swiss–U.S. Privacy Shield Framework does not provide an adequate level of protection.[169]
Turkey		**Direct and Explicit Localization** 2020: Turkey's Banking Regulatory and Supervisory Authority released the Regulation on Information Systems of Banks, which reinforces that banks and financial services keep their primary (live/production data) and secondary (back-ups) information systems within the country.[170] 2020: Turkey passed legislation ("Law on Amendment of the Law on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications") that includes data localization and grants the government sweeping new powers to regulate content on social media. The law requires social network providers with more than 1 million users to: establish a representative office in Turkey; respond to individual complaints in 48 hours or comply with official take-down requests of the courts in 24 hours; and keep personal data of Turkish citizens in country.[171] 2019: Turkey released a Presidential Circular on Information and Communication Security Measures No. 2019/12, which includes data localization and other digital restrictions. Article 3 prohibits public institutions and organizations' data from being stored in cloud storage services that are not under the control of public institutions. The Circular also requires that critical information and sensitive data be stored domestically. Draft regulation is expected that will also mandate localization of data produced by banks and financial services.[172] 2018: Turkey's Capital Markets Board (CMB) enacted new rules (the Communiqué on the Management of the Information Systems (VII-128.9)) for how publicly traded firms should manage their IT systems—which included data localization—in requiring primary and secondary IT systems only be in Turkey. The regulations cover a broad range of firms and organizations, including all publicly traded companies; the Istanbul Stock Exchange; organized markets; pension funds; the Istanbul Clearing, Settlement and Custody Bank; the Central Securities Depository of Turkey; custodians; the Capital Markets Licensing Agency; capital markets institutions; the Turkish Capital Markets Association; and the Turkish Appraisers Association.[173]

		2013: Turkey enacted a law—the Law on Payments and Security Settlement Systems, Payment Services and Electronic Money Institutions—that forces Internet-based payment services, such as PayPal, to store all data in Turkey for 10 years.[174] **Indirect and De Facto Localization** In 2016: Turkey enacted the Law on the Protection of Personal Data, which requires all cross-border transfers of sensitive and non-sensitive personal information require the explicit consent of data subjects, or have to meet other legal grounds.[175] Data may only be transferred without consent to a country with sufficient protections in place. The Personal Data Protection Board determines which countries have adequate standards of protection and approves cross-border transfers to countries that lack such a standard.[176] U.S. industry reports that conditions make it hard to transfer data. Turkey has not yet announced a list of countries that meet the standard of adequate level of protection. Further, the Data Protection Board has yet to grant approval to companies that have sought the ad-hoc approval.[177] 2008: According to the Electronic Communications Act, the data subject's explicit consent is required to transfer traffic and location abroad anywhere.[178]
Ukraine		**Indirect and De Facto Localization** 2011: According to the Law on the Protection of Personal Data, cross-border personal data transfers to a country deemed insufficiently secure requires consent, contractual necessity, or vital interest.[179]
United Kingdom	 	**Indirect and De Facto Localization** 2014: According to the National Health Service information governance rules, it is not illegal to store NHS data abroad; however, it is viewed as a risk factor to do so and is therefore discouraged.[180] 2006: According to the Companies Act, if accounting records are stored outside the U.K., a copy of the accounts and returns must be stored domestically and available for inspection at all times.[181]

MIDDLE EAST AND NORTH AFRICA

Country	Type of Data	Description
Algeria		**Direct and Explicit Localization** 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.[182]
Egypt		**Indirect and de Facto Measures** 2020: Egypt enacted the Personal Data Protection Act (Law No. 151/2020), which requires licenses for cross-border data transfers.[183]
Jordan		**Proposed Measures** 2020: Jordan's draft Personal Data Protection Law prohibits the transfer of personal data outside the Kingdom to any person that does not have sufficient levels of personal data protection. Exceptions to this rule include international cooperation, intra-organizational transfers, and health data that matters for the public health of the kingdom. Further, Article 5 requires the Council of Personal Data Protection to implement an approval process and permits for transferring data as well as issue a list of countries with sufficient levels of protections.[184]
Kuwait		**Indirect and de Facto Measures** 2021: Kuwait's Data Confidentiality Protection Regulations requires firms to notify data subjects if their data is transferred abroad. The regulation requires firms to provide information on how long data will be stored overseas and where it is stored (an onerous and infeasible administrative requirement).[185] The regulations are not applicable to security agencies.
Saudi Arabia		**Direct and Explicit Localization** 2020: Saudi Arabia's National Data Management Office published the National Data Governance Interim Regulations, which requires firms to store and process personal data within Saudi Arabia "in order to ensure preservation of the digital national sovereignty over such data." Data Controllers may only process or transfer personal data outside the Kingdom after obtaining written approval from the relevant regulatory authority.[186] The legal status (whether they are mandatory regulations or voluntary guidance) remains unclear. 2018: Saudi Arabia issued its cloud computing regulatory framework, which includes data localization requirements for various categories of data.[187] As part of its classification framework, it states that no level 3 data (including data from private-sector-regulated industries (it is unclear what these are) and sensitive data from public authorities) can be transferred outside of Saudi Arabia, for whatever

		purpose and in whatever format, whether permanently or temporarily (e.g., for caching, redundancy, or similar purposes), unless expressly allowed by the government. Furthermore, the framework (section 3.3.9) states that cloud providers are not allowed to transfer, store, or process level 3 data in any public, community, or hybrid cloud unless registered with local authorities. Cloud providers must also register and disclose where their data centers are in Saudi Arabia, and the countries where they have data centers process, store, transit, or transfer data from Saudi Arabia.[188] 2018: Saudi Arabia's National Cybersecurity Authority 2018 Essential Cybersecurity Controls framework states that data hosting and storage when using cloud computing services must be located with the country.[189] The draft NCA 2020 Cloud Cybersecurity Controls framework requires operators to provide cloud computing services from within country, including all systems including storage, processing, monitoring, support, and disaster recovery centers. The requirement applies to all levels of data.[190]
United Arab Emirates		**Direct and Explicit Localization** 2019: The UAE's health data protection law (UAE Federal Law No.2 of 2019) introduced a general prohibition (article 13) on the transfer of health data outside the UAE.[191] In 2021, the UAE's Ministry of Health and Prevention issued a long awaited resolution setting out exceptions that allow health data transfers, but the general prohibition remains in place.[192] **Proposed Measures** 2021: The UAE's draft Data Privacy Law requires firms to get a permit from the local data protection authority prior to transferring sensitive personal data (article 38). Sensitive data is broadly defined, including any data that directly or indirectly relates to a person's family or ethnic origin, health or personal data, or any Data that discloses psychological, genetic and biometric data, financial or economic data, and data related to religious beliefs and political opinions.[193]

CENTRAL ASIA

Country	Type of Data	Description
Kazakhstan		**Direct and Explicit Localization** 2021: Kazakhstan adopted new rules as part of its personal data protection framework, which specified that all personal data should be stored locally.[194] 2015: Kazakhstan enacted a law (No. 418-V) on informatization that reaffirmed that organizations store electronic databases containing personal data in the country.[195] 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.[196] 2010: Kazakhstan enacted a regulation on telecommunication subscriber information, which prohibits the storage of subscriber information outside the country.[197] 2005: Kazakhstan requires all domestically registered domain names (i.e., those on the ".kz" top-level domain) operate on physical servers within the country).[198] 2004: Kazakhstan enacted a communications law that requires certain communication services to store data in the country.[199]
Uzbekistan		**Direct and Explicit Localization** 2019: Uzbekistan's revised personal data law requires explicit local personal data storage and processing.[200]

SOUTH ASIA

Country	Type of Data	Description
Bangladesh		**Indirect and de Facto Measures** 1991: Bangladesh's Bank Company Act (section 12) states that banks can't transfer business related documents outside the country without first getting the Bangladesh central bank's permission.[201] **Proposed** 2020: Bangladesh's draft Data Protection Act includes data localization and data mirroring provisions. Also, it requires firms to segregate data post-processing into sensitive, critical, and general personal data is technically

		impracticable. It also includes extremely broad and far-reaching investigative powers, including the power to obtain access to all personal data and access to any premises.[202] 2020: Bangladesh's draft National Cloud Policy includes explicit data localization for all personal and government data. Transfers of data are only allowed for backup purposes, but only if the data doesn't include any personal or sensitive data or data that is otherwise "not detrimental to the security of Bangladesh and important infrastructure" and if the transfer is to a country where Bangladesh can fully (unspecified) enforce its laws through bilateral or multilateral agreements.[203]
India		**Direct and Explicit Localization** 2021: The Reserve Bank of India released a revised regulations on electronic know your customer (eKYC) requirements which states that the technology infrastructure should be housed in the Regulated Entity own premises and the video-based customer identification process connection and interaction (to do digital due diligence and verification of a customer) shall necessarily originate from its own secured network domain.[204] 2020: The Securities and Exchange Board of India released a cybersecurity-related circular that financial institutions should "…ensure complete protection and seamless control over…critical systems…while keeping the critical data within the legal boundary of India."[205] 2018: The Reserve Bank of India enacted rules forcing all payment to be stored in India.[206] Despite not providing any evidence of having faced regulatory issues pertaining to access to data, the RBI's notional reasons for data localization were concerns over regulatory oversight and cybersecurity, as the bank cited the need for "continuous monitoring and surveillance" of payments data in order to reduce the risk of data breaches by ensuring payment services use the best global cybersecurity standards.[207] There is no bar on processing of payment transactions outside India. However, the data shall be stored only in India after the processing. In case the processing is done abroad, the data should be deleted from the systems abroad and brought back to India not later than the one business day or 24 hours from payment processing, whichever is earlier.[208] In June 2019, RBI stated that the requirement to store payments data locally also applies to banks operating in India.[209] 2017: The Ministry of Electronics and Information Technology released Guidelines for Government Departments on Contractual Terms Related to Cloud Services. The guidelines require that any government

contracts contain a localization clause mandating that all government data residing in cloud storage networks is located on servers in India.[210]

2017: The Consolidated FDI Policy Circular of 2017 mandates certain conditions for the Broadcasting Sector. Clause1.3 (ix) states that:"the Company shall not transfer the subscribers' databases to any person or place outside India unless permitted by relevant law."[211]

2017: The Insurance Regulatory and Development Authority of India mandates that all original policyholder records should be maintained in India and obtain express consent from the data subject to transfer data outside India.[212]

2013/2014: India enacted the Companies (Accounts) Rules law, which said if financial information is primarily stored abroad, its backups must be stored in India.[213]

2012: India enacted the "National Data Sharing and Accessibility Policy," which effectively means that government data must be stored in local data centers.[214]

2007: The terms of India's unified telecom license agreement required Indian telecom service providers not to transfer certain subscriber information outside India.[215]

1993: Section 4 of the Public Records Act 1993 prohibits public records from being transferred out of India except for official public purposes. Section 4 states: "No person shall take or cause to be taken out of India any public records without prior approval of the Central Government: provided that no such prior approval shall be required if any public records are taken or sent out of India for any official purpose."[216]

Indirect and de Facto Measures

2021: India's new Intermediary Guidelines and Digital Media Ethics Code includes a very short time period (72 hours) to respond to government orders to remove illegal content that would create a de facto data localization requirement for online intermediaries as it'd otherwise be hard, if not impossible, for them to comply (and thus avoid fines and other penalties).[217]

2011: Amendments to India's Information Technology Act of 2000, limited the transfer of data in cases only "if it is necessary for the performance of the lawful contract" or when the data subject consents to the transfer. However, the necessity requirement is not adequately explained, effectively limiting transfer of data only when consent is given.[218]

Proposed

2021: India's Department of Science and Technology released the Draft National Geospatial Policy includes data localization and measures that discriminate against foreign firms and products.[219]

2020: Report by the Committee of Experts on Non-Personal Data Governance Framework includes a range of data localization measures for non-personal data.[220]

2019: The Securities and Exchange Board of India considered forcing foreign financial institutions (like banks) who operate brokerage and custodian services to store all data locally.[221]

2019: India's Draft Personal Data Protection Bill proposed mandating the storage of 'one serving copy' of all personal data within India. The bill would also impose onerous conditions on the cross-border transfer of "sensitive" personal information, including "explicit consent" by the data principal. "Critical" personal information—an undefined category—could not be transferred out of India under any circumstances. This Bill also proposes to empower the central government to classify any personal data as 'critical personal data' to be processed exclusively in India.[222] The draft bill is still being debates and amended.

2018/2019/2021: Various drafts of India's National E-commerce Policy explicitly call for forced data localization as a privacy, cybersecurity, and regulatory measure.[223]

2018: the Central Government released a draft set of rules to regulate online pharmacies in India. This was in the form of amendments to the Drugs and Cosmetics Rules, 1945. The proposed rule mandates that: "The e-pharmacy portal shall be established in India through which they are conducting the business of e-pharmacy and shall keep the data generated localized: Provided, that in no case the data generated or mirrored through e-pharmacy portal shall be sent or stored, by any means, outside the India."[224] As at writing, the final version had not been released.

2015: India released a National Telecom Machine-to-Machine (M2M) road map that requires all relevant gateways and application servers that serve Indian customers be located domestically. The Roadmap has not yet been implemented.[225] It was an overarching policy strategy, so did not have any mandated localization measures.

2014: The Indian National Security Council proposed a policy that would institutionalize data localization by requiring all email providers to set up local servers for their

		India operations, and mandating that all data related to communication between two users in India should remain within the country.
Pakistan		**Proposed** 2020: Pakistan's draft Personal Data Protection Bill includes a range of data localization and processing requirements (including for "critical personal data" (which is not clearly defined)). It requires Pakistan's Personal Data Protection Authority to introduce a broad data localization framework to force firms to store copies (mirroring) of personal data in Pakistan, even where that data may otherwise be allowed to be transferred out of the country.[226]
Sri Lanka		**Proposed** 2019: Sri Lanka's draft Data Protection Bill only allows cross-border transfers of data to countries designated by a government minister (it does not provide details about the approval process, nor assessment criteria). Furthermore, the draft bill does not acknowledge a range of other common legal mechanisms that firms use to transfers data, such as through standard contractual clauses, certifications, and binding corporate rules, as well as bilateral, reginal, and multilateral mutual recognition frameworks.[227] Personal data processed by a 'public authority' as a data controller is to be processed only in Sri Lanka, unless the data protection agency classifies such categories of personal data that are permitted to be processed outside Sri Lanka.[228]

SOUTHEAST AND NORTHEAST ASIA

Country	Type of Data	Description
Indonesia		**Explicit Data Localization** 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.[229] 2016: Indonesian 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.[230]

Indirect and De Facto Localization

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 be cover a broad range of digital activity. It requires all ESAs to register (whether foreign or domestic) with KOMINFO. Those that 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 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 holder of "Strategic Electronic Data" are: energy, transportation, financial, healthcare, ICT, food, defense, and any other sectors stipulated by the Government.[231]

2020: Indonesia's General Regulation Number 80 of 2019 (GR 80) stipulates that personal data cannot be transferred offshore, unless the receiving nation is deemed by the Ministry of Trade as having the same level of personal data standards and protection as Indonesia. However, this stipulation in GR 80 may not be immediately enforced, as the regulation has a 2-year transition period.[232]

Proposed Measures

2020: Indonesia's Ministry of Communications and Information Technology draft Ministerial Regulation No. 5/2020 (which deals with sensitive online content and electronic system operators and therefore relates to the above) contains a range of problematic provisions that lead to de facto localization. It only allows for 24 hours to respond to requests to take down illegal content, and for content deemed urgent, only 4 hours. It also included providing mandatory access to data for government and law enforcement agencies. It also allows them to obtain traffic and subscriber data, without a clear requirement to provide

		legal reasoning. These would potentially apply to a broad range of services, such as startups, e-commerce players, social media, and game developers.[233]
Malaysia		**Indirect and De Facto Localization** 2020: For several years Malaysia's central bank enacted a law maintained a moratorium on outsourcing hindering financial institutions' ability to utilize their global digital platforms. Bank Negara Malaysia also has data localization elements in its Risk Management in Technology framework, but has indicated that it intends to remove them. It has amended its recent Outsourcing Guidelines to remove original data localization requirement.[234]
South Korea		**Explicit Data Localization** 2019: Korea's Cloud Security Assurance Program (CSAP, which governs cloud services for public sector agencies) requires the physical location of the cloud system and data shall only be within Korea and that cloud services for public institutions shall be physically separated from the cloud service area for private institutions.[235] 2016: Korea's Regulation on Supervision of Electronic Financial Transactions was amended to allow the use of cloud services by financial firms; however, the Financial Services Commission specifically requires that such data be maintained on servers located in Korea.[236] **Indirect and De Facto Localization** 2014: South Korea's Act on the Establishment, Management, Etc. of Spatial Data Korea and associated (discriminatory) licensing regime prevents firms from transferring location-based data outside the country.[237] 2011: Korea's Personal Information Protection Act requires companies to obtain consent from "data subjects" (i.e., the individuals associated with particular data sets) prior to exporting that data. The act also requires "data subjects" to be informed of who receives their data, the recipient's purpose for having that information, the period that information will be retained, and the specific personal information to be provided. This is clearly a substantial burden on companies trying to send data across borders.[238]
Vietnam		**Explicit Data Localization** 2020: Vietnam: Decree 72 on the management, provision and use of Internet services and online information: Among other things, the new Decree proposes to regulate foreign social media platforms, app store platforms, in-app transaction payments, and all other businesses that need to use user ID verification technologies. introduce new obligations to both local telecoms and foreign platforms who have caching servers in Vietnam, making them liable for objectionable contents on the foreign platforms. An internal government report associated with this decree

		denotes how the country has become overly dependent on foreign platforms and how government control/national digital sovereignty has been weakened by these foreign companies.[239] **Proposed Measures** 2019: Vietnam: Draft of Law on Cybersecurity (effective since January 1, 2019) includes extensive local data storage requirements. The implementation decree is under consideration with the Office of the Government and the Ministry of Industry and Trade.[240]

SOUTH AND CENTRAL AMERICA

Country	Type of Data	Description
Brazil		**Explicit Data Localization** 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.[241] **Proposed Measures** 2020: Policymakers introduced Bill 4723/2020 to Brazil's parliament to amend Brazil's Data Protection Law requiring all personal data to be stored within the country. The bill also would forbid the use of cloud computing for any data processing when data is stored outside the country.[242]
Chile		**Explicit Data Localization** 2020: Chile's financial regulatory authorities released updated regulations (Chapter 20-7 of Recopilación Actualizada de Normas Bancos, the Updated Compilation of Banking Standards) requiring "significant" or "strategic" outsourcing data be held in Chile. The same requirement is outlined in Circular No. 2, which is addressed to non-banking payment card issuers and operators. In effect, these regulations can apply to any confidential records. In the case of the international transfer of such data, transfer may occur but duplicate copies of such records must be held in Chile.[243]
Peru		**Proposed Measures** 2021: Peru's draft National Strategy for AI, they encourage all projects financed with public resources to incorporate

		the use of local data centers and/or cloud platforms whose infrastructure is installed in Peru.[244] 2020: The Digital Government Secretariat of Peru released draft regulations for a Digital Trust Framework, which gives preferential treatment to domestic data storage and domestic service providers.[vi] U.S. firms reports that the draft proposal includes: (1) the creation of a whitelist of permitted countries for cross-border transfer of data (even though the Peruvian Data Protection Law does not include such restrictions); and the creation of a national data center intended to host the information provided by the public sector entities.[245]
Venezuela		**Explicit Data Localization** Venezuela has passed regulations requiring that IT infrastructure for payment processing be located domestically.[246]

CHINA

Country	Type of Data	Description
China		**Direct and Explicit Localization** Overview: China's Cybersecurity Law (CSL), draft Personal Information Protection Law, and Data Security Law are central to China's evolving data governance framework, and each include extensive explicit and de facto data localization measures. However, even with these three major pieces of legislation in place, the patchwork of requirements related to data localization and cross-border data transfers are liekly here to stay.[247] Typical of Chinese policymaking, Chinese laws like the CSL often only offer high-level requirements, so sectors wait on subsequent draft laws, regulations, standards, and implementing regulations be released and discussed to see how it'll ultimately affect how they do business. Another factor that is unique to China is that it has many regulations that are recommended best practices or standards that in practice are mandatory requirement. These measures exist in sectors such as banking,[248] insurance,[249] credit investigation,[250] post and courier services,[251] population health and genetic information,[252] online taxi booking businesses,[253] location services[254] and civil aviation.[255] Many of these overlap with listed policies, but some are separate so a thorough analysis of localization needs to consider both tools.[256] Some sector regulators/regulations allow data transfers to overseas entities or individuals in limited circumstances, and often on a case-by-case basis, but such requirements are uneven

and the process to obtain regulators' consent is often opaque. Some of China's earliest data localization requirements have been superseded by new laws and regulations, but are included to show the trend towards more and broader localization in China.

2020: PBOC Technical Specification for Protection of Personal Financial Information, personal financial information (PFI) must not be transferred or shared, except where essential for the processing and settlement of financial transactions. PFI collected or generated in China must be stored and processed in China.[257] This applies to all banks, financial institutions, and insurance firms. PFI is widely defined and includes personal and non-personal information which is collected, processed, generated and secured through the provision of financial products or services within China.[258] Firms may only transfer personal data cross-border in select, restrictive circumstances.[259] The specification is a "recommended" national standard within China's vast and complicated standards system, where these standards are in fact mandatory as authorities will use it as a benchmark for compliance assessments during audits and enforcement.

2020: TC180 & PBOC Personal Financial Information Technical Specification, Classifies PFI into three levels. All PFI collected and produced in China must be stored, processed, and analyzed in China. Can do intra-company transfers.[260]

2020: The PBOC's "Interim Measures for Administration of the Credit Rating Industry" came into effect. It reiterates existing localization requirements in requiring credit rating agencies to process and store all information they collect in China.[261]

2019: The PBOC and CBIRC issued "Administrative Measures for Bank Card Clearing Institutions" for bank card clearing agencies which included forced data localization and data processing (articles 3 and 20).[262]

2019: NPC PRC Securities Law (Article 117), no business or individual may send abroad documents and materials related to securities business activities without the approval of the State Council's oversight bodies.[263]

2019: CBIRC Banking Financial Institutions Anti-Money Laundering and Counter Terrorist Financing Management Measures (Article 28), banking and financial institutions are not allowed to send abroad customer identification information and transaction information obtained when performing anti-money laundering and anti-terrorist financing obligations, except when permitted by laws and administrative regulations.[264]

2019: According to the Regulations of the People's Republic of China on the Administration of Human Genetic Resources, the Chinese government reserves the right to manage the genetic data of its citizens. Article 7 stipulates that foreign organizations may not collect or preserve Chinese genetic data domestically or abroad.[265]

2019: The People's Bank of China's (PBOC) Implementing Measures of Financial Consumer Rights Protection (Article 34), the storage, processing and analysis of consumer financial information collected in China shall be carried out in China. (Exceptions for intra-company transfers, required for int'l transactions, authorized by consumer).[266]

2018: According to the Measures for the Administration of Scientific Data (the "Measures"), any scientific data supported by Chinese government funding must be stored domestically. Notably, this also applies to scientific data collected by foreign firms who are then "encouraged by the stick" to store their data in China or face harsh regulation enforcement.[267]

2017: China's Cybersecurity Law requires operators of "critical information infrastructure" (CII) to store personal information and "important data" within the PRC. In order to transfer this data abroad, a security assessment must be undertaken by the appropriate authorities. It is still unclear what a "critical information infrastructure" operator is, or what constitutes "important data," and the scope of both terms may expand (or shrink) as respective agencies enact implementing regulations. Some examples of CII that have been provided include public communication and information services, energy, communications, water conservation, finance, public services and e-government affairs.[268]

2016: NASG (the regulatory body in charge of issuing licenses for mapping and surveying) defined that the autonomous mapping feature used in automated vehicles is a form of electronic navigation map, and that all data collection, editing, processing and production of autonomous driving maps must be done by a NASG licensed firm. Of the 14 entities licensed by NASG, all are domestic Chinese firms.[269]

2016: According to the Interim Regulations for the Management of Network Appoint Taxi Services Operations, there is a licensing system for online taxi companies that requires them to host user data on servers located in China.[270]

2016: According to China's Map Management Regulations, online maps must acquire an official certificate and set up their servers within China.[271]

2016: China's Administrative Measures for the Online Payment Business of Non-Banking Payment Institutions requires relevant firms to have their data and IT systems in China and that all data processing must be done locally.[272]
2016: China's Provisions on Administration of Online Publishing Services requires firms to keep servers and storage equipment in China.[273]

2014: According to the Administrative Measures for Population Health Information, population health data can only be stored and processed within China.[274]

2013: According to Article 24 of the Regulation on the Administration of Credit Investigation Industry, organizing, preserving and processing of consumer or commercial data by credit reporting agencies must take place within China.[275] This older law was left purposely vague so foreign credit firms (but not local firms) could still transfer data, but new (2021) credit investigation regulations (below) include explicit localization requirements that affect all firms.

2011: According to the Notice to Urge Banking Financial Institutions to Protect Personal Financial Information, personal data collected by commercial banks can only be stored, handled, and analyzed in China.[276]

2006: China's Measures for the administration of Electronic Banking Businesses (then known as e-banking) required Chinese-invested banking institutions to keep IT systems and data in China.[277]

2000: According to China's Telecommunications Regulations, all data collected inside China must be stored on Chinese servers.[278]

1989: According to the Law of the People's Republic of China on Guarding State Secrets, it is prohibited to transfer cross-border any data containing state secrets. There is no detailed definition of what constitutes a state secret.[279]

De Facto Data Localization
2021: CAC releases draft revision of Cybersecurity Review Measures, which explicitly require review before foreign listing of firms holding over 1m users' data.[280]

2020: China's Data Security Law (coming into force September 1, 2021) creates new liabilities for entities engaging in activities that might harm the "national

security, public interest, or lawful interests of citizens or organizations" in China. The draft states that China will establish a security review mechanism, data processors must obtain licenses, and cooperate with national security agencies while going through data review processes.[281]

Proposed Data Localization

2021: China's draft Credit Business Management Measures requires firms to store data in China (article 35). In cases where firms need to provide credit information to foreign counterparts and other foreign organizations for the purpose of cross-border trade and finance, it must assess the request and file any such requests with the PBOC.[282]

2021: CAC released "Draft Provisions on the Management of Automobile Data Security" personal information and "important data" be stored in China, and where it is necessary to provide such information and data abroad, the Operator shall conduct a cross-border data transmission security assessment organized by the CAC. The measure defines "important data" broadly, including surveying and mapping data, operational data on vehicle charging grids, statistics on the types and flows of vehicles on the road, audio and video data outside a vehicle, "other data deemed to affect national security and public interest."[283]

2019: China's draft Critical Information Infrastructure Regulations expanded the scope of what constitutes CII in the Cybersecurity Law. Under this draft, CII protection would also apply to government agencies and entities in the energy, finance, transportation, water conservation, healthcare, education, social insurance, environmental protection and public utilities sector; information networks, such as telecommunication networks, broadcast television networks and the internet, and entities providing cloud computing, big data and other large-scale public information network services; research and manufacturing entities in sectors such as science and technology for defense, large equipment manufacturing, chemicals industry and food and drug sectors; and press entities such as broadcasting and television stations, news agencies and other key entities.[284]

2019: China's Cyberspace Administration of China released the draft "Measures of Security Assessment of the Cross-border Transfer of Personal Information," which would require strict and comprehensive security assessments for the cross-border transfer of personal information from any "network operator."[285] The draft details several elements of China's (2017) Cybersecurity Law. These measures would likely cover most, if not all, cloud providers and larger organizations and firms requiring large data transfers (e.g., over 500,000 records). In the draft's current form, critical information infrastructure

		operators, national authorities, and data controllers processing above an undefined threshold may only transfer personal data abroad after an approved security assessment. It is unclear how this draft affects previously issued mandates in the Cybersecurity Law.[286] 2020: China's draft Personal Information Protection Law (PIPL) would require personal information process by a state organ be stored within China and may only be transferred abroad when there is a business or contractual necessity and may only happen after an application is filed and a risk assessment is conducted.[287] PIPL will undergo its 3rd draft review in August and is likely to be implemented shortly after. 2019: China's draft Administrative Measures on Data Security stipulate that in order to publish, share, trade or send important data to overseas, a network operator must independently assess its own security risks and report to (unspecified) relevant industry regulators for approval.[288]

OCEANIA

Country	Type of Data	Description
Australia		**Direct and Explicit Localization** 2012: Australia's Personally Controlled Electronic Health Records Act requires that personal health records be stored only in Australia.[289]
New Zealand		**Direct and Explicit Localization** 2010: New Zealand's Inland Revenue Act requires businesses to store business records in local data centers.[290]

NORTH AMERICA

Country	Type of Data	Description
Canada		**Direct and Explicit Localization** 2003: Two Canadian provinces, British Columbia and Nova Scotia, have implemented laws mandating that personal data held by public bodies such as schools, hospitals, and public agencies must be stored and accessed only in Canada, unless certain conditions are fulfilled. The tender for the project to consolidate the federal government's ICT services, including email, for 63 different agencies requires the contracting company to store the data in Canada (citing national security reasons).[291] **Indirect and De Facto Localization** 2006: Quebec requires public bodies ensure that "equivalent" data protection must be demonstrated before personal data can be transferred cross-border. No list of equivalent states has been released.[292] **Proposed/Considered Data Localization** 2019: The Office of the Privacy Commissioner (OPC) proposed revising its policy position on transborder data flows under the Personal Information Protection and Electronic Documents Act (PIPEDA), to assert that a company that is disclosing personal information across a border, including for processing, must obtain consent. OPC ultimately withdrew its proposal, however, it did so with the caveat that it would maintain the status quo only "until the law is changed."[293]
Mexico		**Indirect and De Facto Localization** 2010: According to the Federal Law for the Protection of Personal Data in the Possession of Private Parties, consent is required for cross-border transfers of personal data except when the transfer is intra-group, or it is required by a contract.[294] **Proposed Measures** 2020: Mexico's central bank (Banxico) and the National Banking and Securities Commission (CNBV) issued draft fintech regulations (Provisions Applicable to Electronic Payment Fund Institutions) that would force firms to only choose cloud providers based in Mexico. Article 50 would impose a local data storage requirement. Article 49 would establish a regulatory approval model with a high degree of discretion and lack of transparency for determining what cloud computing services payments and financial firms could use.[295]

United States



Direct and Explicit Localization
2011: Specific federal U.S. government agencies (mainly defense and intelligence related) require the use of a specific U.S.-based cloud service (GovCloud) and stipulate local data storage in ICT contracts. Previously, government agencies with data subject to compliance regulations were unable to process and store data in the cloud that the federal government mandated be accessible only by U.S. persons.[296] GovCloud is used by U.S. government agencies for sensitive workloads that need to meet specific regulatory and compliance requirements, such as those set by the International Traffic in Arms Regulations (ITAR), the Federal Risk and Management Program (FedRAMP) High, Department of Defense Security Requirements Guide (DoD SRG) Impact Levels 4 and 5, and Criminal Justice Information Services (CJIS). AWS GovCloud regions are only in the United States and are logically and physically administered exclusively by AWS personnel that are U.S. citizens only.[297] They are physically separated from all other AWS cloud regions. This localization requirement is contractual, rather than based in legislation. For example, FedRAMP control specific contract clauses guide refers to U.S. National Institute of Standards and Technology standard SP 800-53 and outlines how U.S. government agencies "with specific data location requirements must include contractual requirements identifying where data-at-rest (primary and replicated storage) shall be stored."[298]

Sub-National Requirements
2009: The City of Los Angeles requires Google to store its data within the United States.[299]

Proposed/Considered Data Localization
2021: A draft bill presented by Senator Ron Ryden (D-Ore.) calls for the Secretary of Commerce to lead an investigation determining categories of sensitive data that could harm U.S. national security if exported to certain countries, and draft a list of countries whose data security would allow Americans to safely export data. Bulk exports of data to countries not on this white-list would require a license.[300]

2016: In 2016, the United States considered exempting financial data from provision in the Trans-Pacific Partnership trade agreement that would have prohibited data localization. But thankfully, these agencies saw the errors of this approach. U.S. trade policy now included extensive details that specific the importance of access to data.

U.S. State-Level Regulations
2011: A New York senator proposed a law that would prohibit the transfer of personal information outside the

	United States without the prior written consent of the consumer.[301] 2004: Proposed in Ohio, Bill no. 459 would prohibit transferring personal data overseas without written consent as part of any state procurement projects.[302] 2004: Similar to the Ohio bill, Missouri proposed House Bill no. 1497 which would also require consent to transfer telecommunications data.[303]

APPENDIX B: MODEL METHODOLOGY

Selecting a Data Restrictiveness Index

ITIF used OECD's Indicators of PMR data to compute an index of data restrictiveness because it has the broadest range of recorded years out of any viable index on data governance in a publicly available database. A longer range of time in a country's recorded DRI is more useful than data only available for recent years. Also, the distribution of a PMR-based DRI shows greater variation in the distribution of countries' measurements than indices computed with other applicable databases. This normal distribution makes any quantitative exercise more feasible since statistical trends are best identified with wide variations in data. With data inputs taken from the PMR database to form a DRI, modeling has panel data available for countries from 1998 to 2018. When extending regression findings, it is worth noting that OECD's configuration of available PMR sub-indicators changes between 2013 and 2018. DRI proxies between years are computed using equations 1 and 2 listed below. Unweighted averages of select PMR sub-indicators are taken to further isolate data-relevant restrictions on trade while excluding additional confounding factors included in the overall tabulation of OECD's PMR index.

(1) [2003, 2008, 2013]

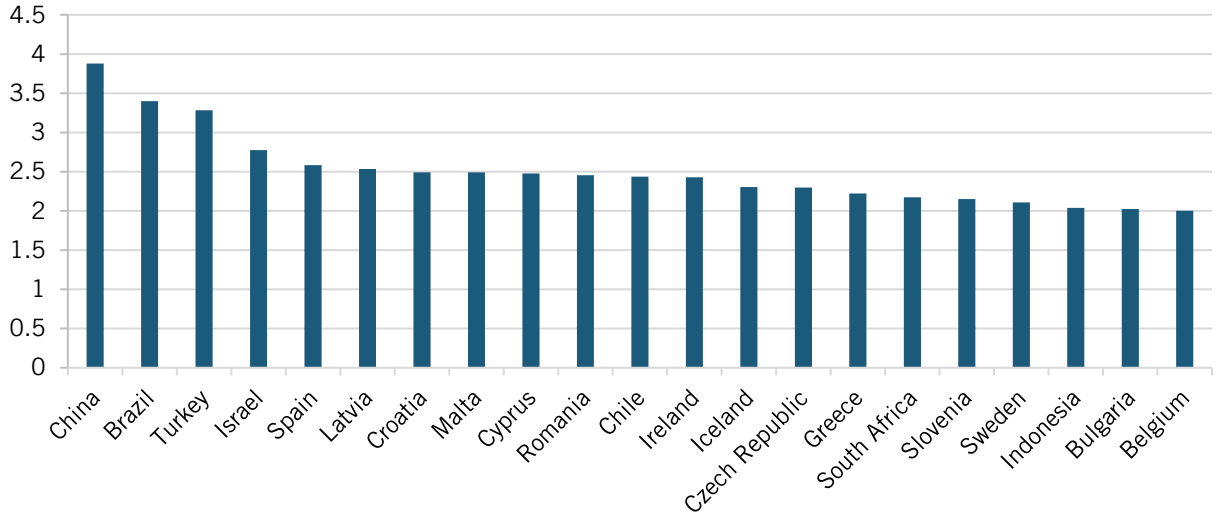
$$DRI_{xt} = \frac{(Administrative\ Barriers\ to\ Startups_{xt} + AdminReg\ Opacity_{xt})}{2}$$

(2) [2018]

$$DRI_{xt} = \frac{(Assess.Competition + Interaction.IG + Reg.Complexity + Barriers.Services + Barriers.Network)}{5}$$

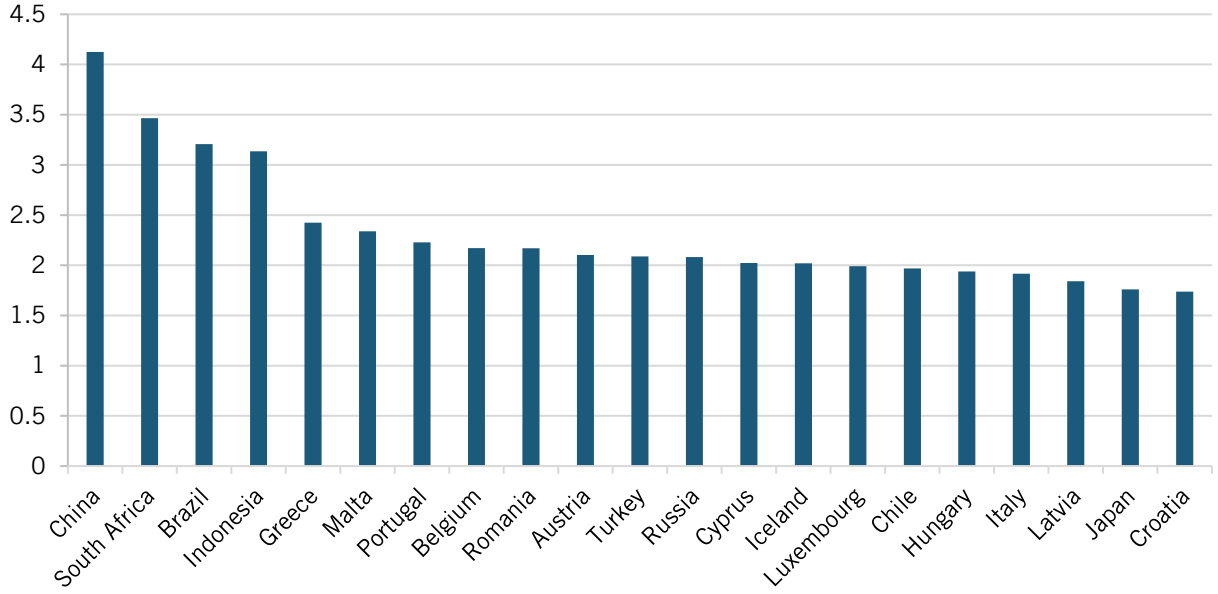
Given that measurements within the OECD's PMR Indicators database are recorded on a scale of 0–6 (0 being most open for trade, and 6 being most restrictive to trade flows), DRI is also computed on the same scale, wherein a higher measurement of DRI indicates greater restrictions on data flows within a country. Figures 1 and 2 and three show the rankings of most data-restrictive countries based on DRI scores for years 2013 and 2018.

Figure 1: 2013 DRI among most restrictive countries



Source: OECD Indicators of PMR Database and Authors' own calculations.

Figure 2: 2018 DRI among most-restrictive countries



Source: OECD Indicators of PMR Database and Authors' own calculations.

PMR sub-indicators selected for pre-2018 data are determined by best practice exhibited by CIGI & Chatham house modeling of data restrictiveness via PMR. 2018 PMR sub-indicators are selected for computing a DRI proxy due to observed correlation patterns listed below in table 1.

Table 1: Correlation table for continuity of DRI

	Correlations Between Years Within the Same Year		Correlations Between PMR and DRI Proxy Within the Same Year	
	2008 to 2013	**2013 to 2018**	**Year**	**Correlation**
PMR Index	0.968	0.854	**2008**	0.810
DRI Proxy	0.596	0.503	**2013**	0.664
			2018	0.845

Source: OECD Indicators of PMR Database and Authors' own calculations.

Best-practice methodology using PMR to proxy data restrictiveness among countries gives a correlation of 0.596 from 2008 to 2013. This comes with a correlation in OECD's overall PMR Index of 0.968 between the same years observed. Correlation between the 2013 and 2018 overall PMR index falls to 0.854, which indicates that the correlation of DRI proxy data from 2013 to 2018 should also fall by some similar amount. A correlation of DRI between 2013 and 2018 of 0.509 shows that correlation has only fallen slightly due to a drop in correlation in the original PMR index, likely due to the simple fact that greater policy changes made by countries around regulations were enacted between 2013 and 2018 than from 2008 to 2013. Therefore,

calculation of DRI using 2018 PMR data should be understood as comparable with pre-2018 PMR data.

OECD also provides additional data related to services regulation via the Services Trade Restrictiveness Index (STRI), which contains the sub-index Digital Services Trade Restrictiveness Index (DSTRI), and its component measurement Infrastructure and Connectivity. This data is newer than the PMR database yet only exists from 2014 to 2020. DSTRI intends to capture a truer representation of digital services regulations. However, the current publicly available version of the STRI database possesses a far smaller time range than PMR and a highly skewed distribution of index measurements, with little variation between countries and across years—all making econometric application less feasible. DRL using PMR sub-indicator inputs gives the most normal distribution of the three noted approaches and greatest time range, better lending itself to regression modeling than other approaches. DSTRI will likely eventually be the best publicly available index for approximating a country's data restrictiveness as OECD adds greater detail and extends the period of available years. However, as it currently exists, PMR retains more utility to observing trends over time in data restrictiveness against economic performance and for a broader swathe of countries.

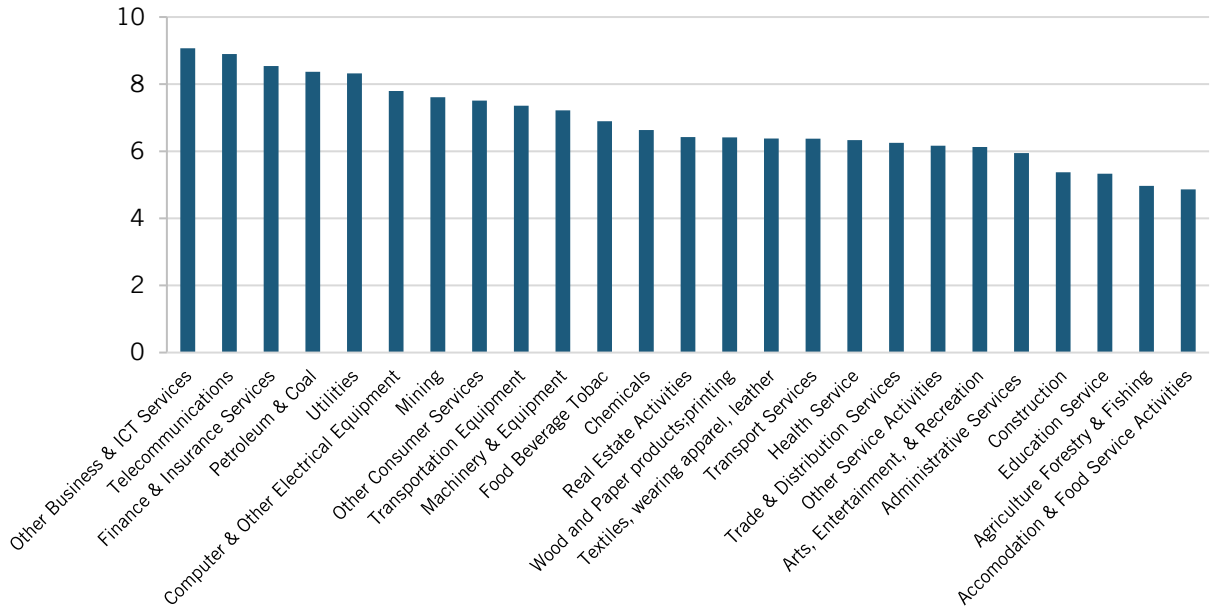
Selecting a Data-Intensity Modifier

ITIF's model assumes that data restrictions have greater effects on economic industries that are more reliant on data and data-related tools and services. To best weigh national DRI measurements as industry-specific measurements, a DIM is calculated to help correct for bias in the proxy DRI by weighting each downstream industry's linkage with national data restrictiveness for every industry within the KLEMS categorization. Furthermore, this model selects the United States as a reference country in a given baseline year for computing industry-specific measurements of DIM to be applied to countries in the sample, thus controlling for issues of endogeneity because data-intensity in the United States cannot influence data-intensity in other countries over time. However, this exogenous approach for estimating DIM assumes that countries within the sample have equal technologies as the United States. U.S. Census ICT 2013 Survey data on noncapitalized software expenditure and BLS data of employment by industry in the same year are gathered to compute the ratios of data-related service expenditure per worker in each industry. ITIF's methodology for calculating DIM is based on best practice as demonstrated by ECIPE. Labor is recorded in number of workers employed and noncapitalized software expenditure is recorded in millions of U.S. Dollars. DIM is taken as a natural log to align with previous literature on factor intensity.

(3)

$$DIM_y = \ln\left(\frac{Noncapitalized\ software\ expenditure\ _y}{Labor_y}\right)$$

Figure 4: Data intensity by KLEMS industry (as log of noncapitalized software expenditure per worker)



Source: US BLS 2013 Employment by Industry, US Census ICT survey 2013, and Authors' own calculations.

Comparing Distributions of DRL under Different Approaches

Computing both a proxy DRI and DIM by industry lets us create a composite index that links country-level data restrictiveness to downstream industry-specific measurements of vulnerability to data restrictions. The product of a country's DRI with an industry's DIM gives the DRL of each industry within sample countries. Distributions of DRL over panel data ranging from 1998 to 2018 are listed ahead (Figures 5, 6, and 74) for different proxy tools used to derive DRI, and in turn, DRL. DRL computed using DRI informed by PMR sub-indicators yields the greatest variation in data, most normal distribution, and widest max time range to observe change over time in countries' data restrictiveness levels. These factors, as discussed earlier in Appendix B, are why the final methodology and regression models analyzed use DRL data informed by PMR sub-indicators than DSTRI-related data.

(4)

$$DRL_{xty} = DRI_{xt} * DIM_{y}$$

Figure 5: Histogram of DRL from PMR sub-indicators

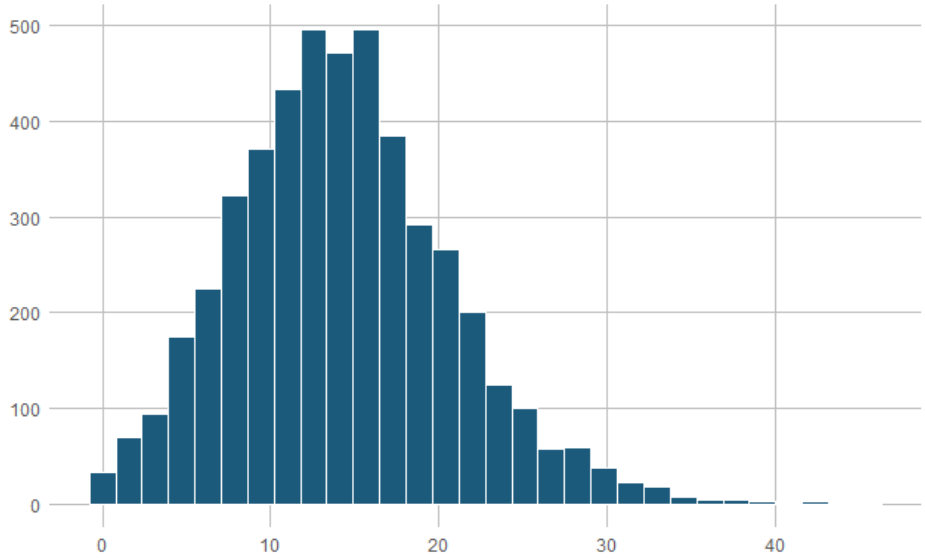


Figure 6: Histogram of DRL using DSTRI: overall

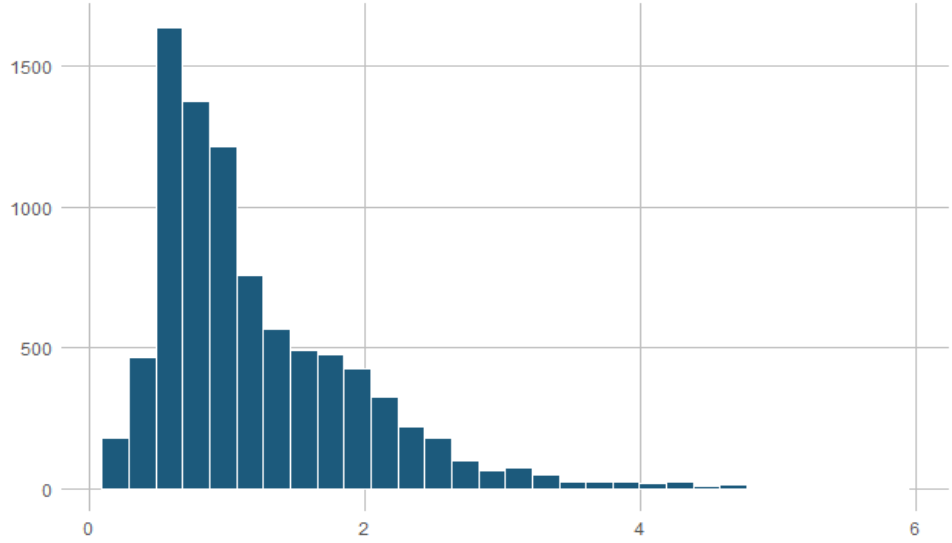
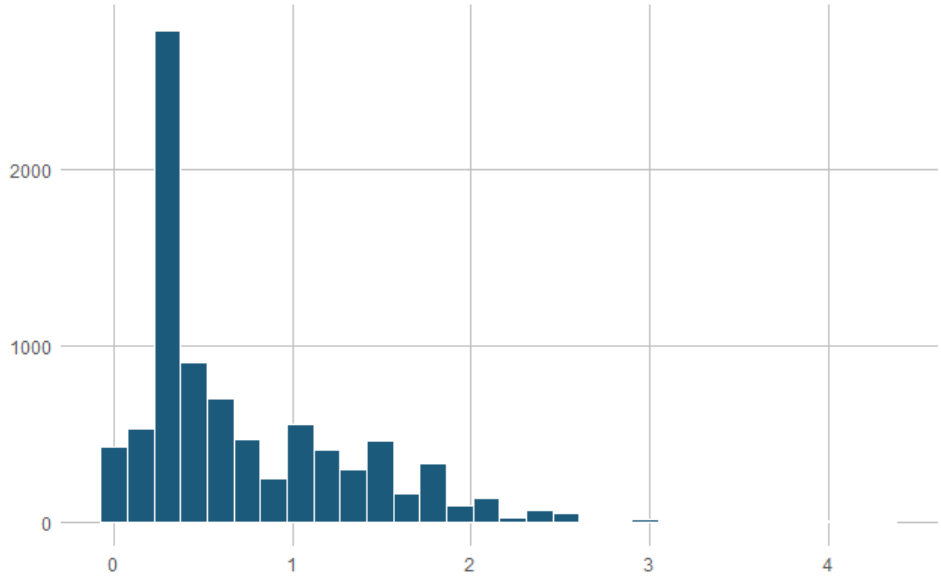


Figure 7: Histogram of DRL using DSTRI: classification 1- Infrastructure & Connectivity



Selecting Industry-Level Indicators of Economic Performance

This model seeks to examine economic performance among countries at the industry level. The EU-KLEMS Database has a wide range of economic indicators available among a set of over 28 OECD member nations within the EU plus other developed partners outside Europe for every industry within the KLEMS categorization. EU-KLEMS details economic data for observing both intermediate and final trade flows via the volume of gross output (GOV) per industry. We select this variable along with a measurement of price indexes based on value added (PVA) in gross output, which aggregates prices to consumers for each industry per country. Lastly, we select a third variable of TFP, which provides a measurement of productivity marked by efficient usage of labor and capital aggregated to industry-level measurements for each sample country. The 2019 version of EU-KLEMS provides these industry-level measurements among countries throughout a panel of data ranging from 1995 to 2017, allowing for a robust time series to observe sufficient changes in both national policies and economic performance, and supporting a time lag in data.

Regression Models

The purpose of this regression modeling is to measure the causal relationship between the index of DRL for the previous year with the log of volume of gross output (GOV), log of TFP, and log of value-added price-indexes (PVA). ϕ is the intercept (β_0 estimate). This model runs log-linear regressions in order to estimate the expected changes in percentage of GOV, TFP, and PVA associated with a change in the DRI. θ is the estimated regression coefficient of DRL, δ_{xt} represents fixed effects by country-year, and γ_{yt} represents fixed effects by sector-year. ε_{xyt} is the residual. The fixed effects are controls placed for unobserved variations between countries and industries not able to be recorded in the model. A time lag is added to all regression modeling wherein dependent data in year T is regressed against DRL data in year T - 1 given that changes in economic performance induced by restrictions on data transfers that would be expected to occur over time (economic performance would not change as immediately as a new policy is enacted).

(5) [Regression Model for GOV]

$$\ln(GOV_{xty}) = \phi + \theta * DRL_{x\,y\,t-1} + \delta_{xt} + \gamma_{yt} + \varepsilon_{xyt}$$

(6) [Regression Model for Total Factor Productivity]

$$\ln(TFP_{xty}) = \phi + \theta * DRL_{x\,y\,t-1} + \delta_{xt} + \gamma_{yt} + \varepsilon_{xyt}$$

(7) [Regression Model for Prices (PVA as price index based on value added)]

$$\ln(PVA_{xty}) = \phi + \theta * DRL_{x\,y\,t-1} + \delta_{xt} + \gamma_{yt} + \varepsilon_{xyt}$$

Table 2: Regression results

Dependent Variable	Coefficient Estimates of Data Restrictiveness Linkage	Pr(>|t|)	Standard Error	Number of Observations	R-Squared
ln(TFP)	-0.02918 ***	0.000937	0.0088	1691	0.1165
ln(PVA)	0.01448*	0.063356	0.0078	2351	0.2271
ln(GOV)	-0.07306***	0.00005	0.018	1990	0.9496

Note: Robust standard errors in parentheses, *** p<0.001, ** p<0.05, * p<0.1
Source: Authors.

Extending Regression Models to Identified Countries Outside Sample

Regression results on the statistical relationship between an industry's DRL and its economic indicators for productivity, prices, and trade volumes can be applied to make estimates as to the national economic impacts borne by countries implementing new data restrictions over time. While regression panel data spans 1998 to 2013, the most recent year in the OECD PMR database, 2018, has data available to compute DRI measurements to quantify changes in data restrictions between 2013 and 2018. While OECD's methodology in compiling PMR sub-indicators changed in 2018, 2018 PMR data can still be compared with previous years, allowing for new DRI proxies in 2018 to still be comparable with pre-2018 DRI. In order to do this accurately, the methodology of DRI calculations must change for 2018. This change in calculation methodology is provided in equation 2. Five PMR sub-indicators are selected to form an unweighted average that matches correlation trends between previous years in DRI and between DRI and overall PMR within years. These lowest-level sub-indicators are all the components of the two medium-level indicators Simplification and Evaluation of Regulations, and Barriers in Service and Network Sectors. Calculating 2018 DRI measurements of countries using this data produces correlation results observable in Table 1, supporting this selection. Table 3 shows estimated costs of increased DRI to a set of four countries of interest available to OECD's PMR database in both 2013 and 2018, as percentage changes over the six-year span of 2013 to 2018.

Table 3: Economic costs of case studies due to changes in DRI

Country	2013 DRI	2013 DRI Ranking	2018 DRI	2018 DRI Ranking	DRI Difference	Total Cumulative Change in Gross Output Volume (2013–2018)	Total Percent Change in Productivity (2013–2018)	Total Percent Change in Prices (2013–2018)
China	3.88	1st	4.13	1st	0.25	-1.7%	-0.7%	0.4%
Indonesia	2.03	19th	3.14	4th	1.11	-7.8%	-3.2%	1.6%
Russia	1.38	39th	2.08	12th	0.70	-4.9%	-2.0%	1.0%
South Africa	2.17	16th	3.47	2nd	1.30	-9.1%	-3.7%	1.9%

Note: DRI rankings are based out of 46 countries maintained in both 2013 and 2018 within the OECD "Indicators of PMR" database. As a result, this ranking excludes notable countries such as India and Argentina.
Source: Authors.

Acknowledgments

This report was made possible in part by generous support from the IT Industry Council. The authors thank Javier Lopez Gonzalez (senior trade policy analyst, OECD) and Erik van der Marel (senior economist, ECIPE) for their advice, encouragement, and good humor. The authors also wish to thank Rob Atkinson, Stephen Ezell, Daniel Castro, and Malachy McLaughlin and the many government officials, private sector representatives, trade associations, academics, and others who helped build the list of data localization measures and to understand the changing nature and impact of data localization around the world. Any errors or omissions are the authors' responsibility alone.

About the Authors

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

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

About ITIF

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

For more information, visit us at www.itif.org.

ENDNOTES

1. Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (ITIF, May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost
2. For example: Avi Goldfarb and Daniel Trefler, "AI and International Trade" (National Bureau of Economic Research, working paper No. 24254, 2018), https://www.nber.org/papers/w24254; Jack Triplett and Barry Bosworth, "Productivity Measurement Issues in Services Industries: Baumol's Disease Has Been Cured," *Economic Policy Review, 2003,* 9(3): 23–33, https://ssrn.com/abstract=789545.
3. Organization for Economic Cooperation and Development (OECD), *Digital Trade and Market Openness* (Paris: OECD Trade Policy Papers, No. 217, 2018), https://doi.org/10.1787/1bd89c9a-en.
4. "OECD Privacy Guidelines," https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm.
5. Alan McQuinn and Daniel Castro, "A Grand Bargain on Data Privacy Legislation for America" (ITIF, January 14, 2019), https://itif.org/publications/2019/01/14/grand-bargain-data-privacy-legislation-america.
6. Hosuk Lee-Makiyama, "Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows" (World Economic Forum, May, 2020), http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf.
7. "Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union," European Commission website, 2019, https://digital-strategy.ec.europa.eu/en/library/guidance-regulation-framework-free-flow-non-personal-data-european-union.
8. Nigel Cory, Ellysse Dick, and Daniel Castro, "The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade" (ITIF, December 17, 2020), https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade.
9. Anirudh Burman and Upasana Sharma, "How Would Data Localization Benefit India?" (Carnegie India, April 14, 2021), https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291.
10. Daniel Castro, "The False Promise of Data Nationalism" (ITIF, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.
11. The hack on the U.S. Office of Management and Budget occurred, at least in part, in an on-premises environment as a result of compromised user credentials. While the AWS report does not specify that it was referring to the OPM hack, it is more than likely the example it refers to. It's fairly clear from the agency OIG reports that OPM was running a number of their own data centers and that they were behind on security. Min Hyun, "Addressing Data Residency with AWS," AWS Blog post, February, 2018, https://aws.amazon.com/blogs/security/addressing-data-residency-with-aws/; The Majority Staff Report, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation" (Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress, September 7, 2016), https://republicans-oversight.house.gov/report/opm-data-breach-government-jeopardized-national-security-generation/.
12. The Security and Exchange Board of India, "Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions," November 3, 2020, https://www.sebi.gov.in/legal/circulars/nov-2020/advisory-for-financial-sector-organizations-regarding-software-as-a-service-saas-based-solutions_48081.html.
13. Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law" (ITIF, March 2016), http://www2.itif.org/2016-unlocking-encryption.pdf.

14. https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where.

15. "India Releases Revised Non-Personal Data Framework," Hunton Andrews Kurth blog post on the National Law Review, January 15, 2021, https://www.natlawreview.com/article/india-releases-revised-non-personal-data-framework; Ministry of Electronics and Information Technology, *Report by the Committee of Experts on Non-Personal Data Governance Framework* (Government of India, December 16, 2020), https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf.

16. Jeet Singh, "Digital Industrialisation in Developing Countries—A Review of the Business and Policy Landscape" (IT for Change, report written for the Commonwealth Secretariat, 2018), https://unctad.org/system/files/non-official-document/dtl_eWeek2018c06-ITforChange_en.pdf.

17. For example, a July 2020 publication by the European Parliament's think tank states that, in the EU context, "digital sovereignty" refers to: "Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)," Tambiama Madiega, "Digital sovereignty for Europe" (European Parliamentary Research Service Ideas Paper, July 2020), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

18. European Commission president Ursula von der Leyen clearly stated regarding the EU's protectionist's objectives, "We must have mastery and ownership of key technologies in Europe," naming quantum computing, AI, blockchain and critical chip technologies as examples. "Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme," November 27, 2019, https://ec.europa.eu/commission/presscorner/detail/es/speech_19_6408.

19. German Chancellor Angela Merkel saying that the EU should claim digital sovereignty by developing its own platforms to manage data in order to reduce its reliance on U.S. providers is simply a call for protectionist-based import substitution in the digital era. Guy Chazan, "Angela Merkel urges EU to seize control of data from US tech titans," *Financial Times,* November 12, 2019, https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca; French President Emmanuel Macron is blunt: "The battle we're fighting is one of sovereignty." Charlene Barshefsky, "EU digital protectionism risks damaging ties with the US," *Financial Times,* August 2, 2020, https://www.ft.com/content/9edea4f5-5f34-4e17-89cd-f9b9ba698103.

20. Javier Espinoza and Guy Chazan, "Germany calls on EU to tighten grip on Big Tech," *Financial Times,* November 11, 2019, https://www.ft.com/content/2d538f22-048d-11ea-a984-fbbacad9e7dd.

21. Eline Chivot, "EU Data Strategy Has Worthwhile Goal, But Misses the Mark," Center for Data Innovation blog post, August 13, 2020, https://datainnovation.org/2020/08/eu-data-strategy-has-worthwhile-goal-but-misses-the-mark/.

22. Nigel Cory, "Response to the public consultation for the European Commission's white paper on a European approach to artificial intelligence" (ITIF, June 12, 2020), http://www2.itif.org/2020-eu-approach-ai.pdf?_ga=2.86726097.873378596.1596032106-254668983.1577993982.

23. United Nations Committee on Trade and Development (UNCTAD), "Global efforts needed to spread digital economy benefits, UN report says," press release, September 4, 2019, https://unctad.org/en/pages/PressRelease.aspx?OriginalVersionID=522; Anri van der Spuy, "Colonising ourselves? An introduction to data colonialism," London School of Economics blog post, March 19, 2020, https://blogs.lse.ac.uk/medialse/2020/03/19/colonising-ourselves-an-introduction-to-data-colonialism/; Jacqueline Hicks, "'Digital colonialism': Why countries like India want to take control of data from Big Tech," *The Print,* September 29, 2019,

https://theprint.in/tech/digital-colonialism-why-countries-like-india-want-to-take-control-of-data-from-big-tech/298217/.

24. Trisha Ray, "The quest for cyber sovereignty is dark and full of terrors," Observer Research Foundation blog post, May 25, 2020, https://www.orfonline.org/expert-speak/the-quest-for-cyber-sovereignty-is-dark-and-full-of-terrors-66676/.

25. Michael West, "Digital colonialism is threatening the Global South," *Al Jazeera,* March 13, 2019, https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south/; Michael Kwet, "Digital Colonialism: US Empire and the New Imperialism in the Global South," Race & Class Volume 60, No. 4 (April 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232297; Renata Avila Pinto, "Digital Sovereignty or Digital Colonialism?" International Journal on Human Rights, SUR 27 (2018), https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/.

26. "India's data must be controlled by Indians: Mukesh Ambani," *Mint,* January 20, 2019, https://www.livemint.com/Companies/QMZDxbCufK3O2dJE4xccyI/Indias-data-must-be-controlled-by-Indians-not-by-global-co.html; "Mukesh Ambani Takes on Amazon, Walmart in e-commerce gamble," *Mint,* July 17, 2020, https://www.livemint.com/companies/news/mukesh-ambani-takes-on-amazon-walmart-in-e-commerce-gamble-11594964172991.html.

27. 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/.

28. 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/.

29. 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.

30. 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.

31. 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.

32. Thomas Treutler and Giang Thi Huong Tran, "Update on the Implementation of Vietnam's New Cybersecurity Law and Status of Implementing Decrees," *Lexology,* December 18, 2019, https://www.lexology.com/library/detail.aspx?g=8833627c-e189-4d60-a472-6ee742cc38fd.

33. The Decree took effect on April 15, 2018. It updated Decree 72/2013/ND-CP (dated July 15, 2013). Yee Chung Seck and Thanh Son Dang, "Decree No. 27/2018/ND-CP amending and supplementing Decree No. 72/2013/ND-CP on Internet Services and Online Information," *Lexology,* April 23, 2018, https://www.lexology.com/library/detail.aspx?g=bec72ba6-167d-468e-938c-391199d8579c.

34. For example, the director general of the Department of Cybersecurity and High-Tech Crime Prevention and Control under Vietnam's Ministry of Public Security is responsible for deciding on

the required deletion, sending written requests for deletion to the relevant entities and auditing such entities' compliance with the LOC. "Updates to Draft Decree Detailing Certain Articles of Law on Cybersecurity," Baker McKenzie blog post, October 8, 2019, https://www.bakermckenzie.com/en/insight/publications/2019/10/updates-draft-decree-law-on-cybersecurity.

35. "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/.

36. Jane Kelsey, "DEPA lacks added value," East Asia Forum blog post, April 10, 2020, https://www.eastasiaforum.org/2020/04/10/depa-lacks-added-value/.

37. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians," July 27, 2018, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

38. Ibid; Amber Sinha, Elonnai Hickok, Udbhav Tiwari, and Arindrajit Basu, "Cross Border Data-Sharing and India: A Study in Processes, Content and Capacity," (Centre for Internet & Society, February 2016), https://cis-india.org/internet-governance/files/mlat-report.

39. "Centre not co-operating in complaint against websites: Court," *Zeenews,* December 5, 2012, zeenews.india.com/news/delhi/centre-not-co-operating-in-complaint-against-websites-court_814836.html.

40. "European Commission Impact assessment: electronic evidence in criminal matters," Commission Staff Working Document, April 17, 2018, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0118:FIN:EN:PDF.

41. As with the U.S. Electronic Communications Privacy Act, but this doesn't prohibit firms from voluntarily providing other non-content data.

42. Nigel Cory and Robert D. Atkinson, "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements" (ITIF, April 25, 2016), https://itif.org/publications/2016/04/25/financial-data-does-not-need-or-deserve-special-treatment-trade-agreements; Nigel Cory, "The TPP's Financial Data Carve Out—USTR Closes a Loophole for Digital Protectionists," Innovation Files blog post, July 7, 2016, https://itif.org/publications/2016/07/07/tpp%E2%80%99s-financial-data-carve-out%E2%80%94ustr-closes-loophole-digital-protectionists.

43. For details on cases in India and Turkey, see: Nigel Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018" (ITIF, January 28, 2019), https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018.

44. "Visa, MasterCard stop supporting bank cards in Crimea," *Reuters,* December 26, 2014, https://www.reuters.com/article/us-russia-crisis-visa-crimea/visa-mastercard-stop-supporting-bank-cards-in-crimea-idUSKBN0K40TN20141226; "Visa and Mastercard May Soon Exit Russia Under Draft Law — Reports," *The Moscow Times,* July 12, 2019, https://www.themoscowtimes.com/2019/07/12/visa-and-mastercard-may-soon-exit-russia-under-draft-law-reports-a66383.

45. "How Russia's MIR Marries State Goals With Payments Disruption," APEXX blog post, April 22, 2020, https://apexx.global/blog/how-russias-mir-marries-state-goals-with-payments-disruption.

46. "Consultation Paper Processing of Payments in South Africa," South African Reserve Bank, November 2018, https://financedocbox.com/Insurance/114473644-National-payment-system-department-consultation-paper-processing-of-payments-in-south-africa.html.

47. Nigel Cory, "Bring USMCA to Life: The United States Should Ensure Mexico Abides by Commitments to Allow the Free Flow of Data," Innovation Files blog post, June 17, 2021, https://itif.org/publications/2021/06/17/bring-usmca-life-united-states-should-ensure-mexico-abides-commitments-allow.

48. Martina F. Ferracane and Erik van der Marel, "Do Data Policy Restrictions Inhibit Trade in Services?"

    (ECIPE), https://ecipe.org/publications/do-data-policy-restrictions-inhibit-trade-in-services/; Martina F. Ferracane and Erik van der Marel, "Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?" (ECIPE), https://ecipe.org/publications/do-data-policy-restrictions-impact-the-productivity-performance-of-firms-and-industries/; "The 2018 edition of the OECD PMR indicators and database: Methodological improvements and policy insights" (OECD, March 23, 2020), https://www.oecd-ilibrary.org/docserver/2cfb622f-en.pdf?expires=1625672355&id=id&accname=guest&checksum=88D357DDE0C3CF200B54FB61F8A5FC11; "Trade and cross-border data flows" (OECD, December 21, 2018), https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)19/FINAL&docLanguage=En.

49. Ibid.

50. "Tracing the Economic Impact of Regulation on the Free Flow of Data and Data Localization" (Global Commission on Internet Governance, May 2019), https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf;

51. Martina F. Ferracane and Erik van der Marel, "Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?" (ECIPE, October, 2018) https://ecipe.org/publications/do-data-policy-restrictions-inhibit-trade-in-services/;

    This approach, however, assumes all modeled countries as having equal technologies since DIM is exogenously calculated. A time lag is included to match the data restrictiveness linkages of each year with industry performance for the following year, given that economic impacts are not immediately observable upon the moment of regulatory change.

53. Lee-Makiyama, Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows.

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

55. Nigel Cory, "Surveying the Damage: Why We Must Accurately Measure Cross-Border Data Flows and Digital Trade Barriers" (ITIF, January 27, 2020), https://itif.org/publications/2020/01/27/surveying-damage-why-we-must-accurately-measure-cross-border-data-flows-and.

56. Modified definition from: Urs Gasser, "Interoperability in the Digital Ecosystem," Berkman Klein Center for Internet and Society Research Publication No. 2015-13, July 6, 2015, http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552584.

57. Gasser, "Interoperability in the Digital Ecosystem."

58. Ibid.
59. Lee-Makiyama, Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows.
60. For example: Mike Gallaher, Chad Harper, and Barbara Kotschwar, "Let's talk about how we talk about interoperability," Visa Economic Empowerment Institution, May, 2021, https://usa.visa.com/dam/VCOM/global/ms/documents/veei-lets-talk-about-interoperability.pdf.
61. An early example of global standards and payment services is when industry and international standards bodies developed ISO 8583 to create a common message format for card payment networks.
62. For example: ISO/IEC 20547, ISO/IEC 21823, ISO/IEC CD 23053, and ISO/IEC AWI 38507. Also see: "Standards by ISO/IEC JTC 1/SC 42:Artificial intelligence," https://www.iso.org/committee/6794475/x/catalogue/p/0/u/1/w/0/d/0.
63. Singapore-Australia Digital Economy Agreement, Article 11.1.
64. Stephanie Honey, "Chapter 8: Asia-Pacific digital trade policy innovation" (in the e-book: Addressing Impediments to Digital Trade, April 27, 2021), https://voxeu.org/content/addressing-impediments-digital-trade.
65. Ibid.
66. "SINGAPORE, CHILE AND NEW ZEALAND SIGN DIGITAL ECONOMY PARTNERSHIP AGREEMENT ELECTRONICALLY," press release, June, 2020, https://www.mti.gov.sg/-/media/MTI/Newsroom/Press-Releases/2020/06/Joint-Press-Release--Electronic-Signing-of-Digital-Economy-Partnership-Agreement-12-June-Updated-URL.pdf; "What are Digital Economy Agreements (DEAs)?" Singapore's Ministry of Trade and Industry, https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements; "Australia-Singapore Digital Economy Agreement: fact sheet," https://www.dfat.gov.au/trade/services-and-digital-trade/australia-singapore-digital-economy-agreement-fact-sheet; Susan Aaronson, "The One Trade Agreement Biden Should Sign Up For Now," *Barron's,* March 8, 2021, https://www.barrons.com/articles/the-one-trade-agreement-biden-should-sign-up-for-now-51614607309.
67. "Digital Economy Partnership Agreement modules," https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-modules/#bookmark2.
68. Ibid.
69. "Australia-Singapore Digital Economy Agreement: fact sheet," https://www.dfat.gov.au/trade/services-and-digital-trade/australia-singapore-digital-economy-agreement-fact-sheet.
70. Joshua New, "The Promise of Data-Driven Drug Development" (Center for Data Innovation, September 18, 2019), https://datainnovation.org/2019/09/the-promise-of-data-driven-drug-development/.
71. Nigel Cory, "Viruses Cross Borders. To Fight Them, Countries Must Let Medical Data Flow, Too," Innovation Files blog post, May 7, 2020, https://itif.org/publications/2020/05/07/viruses-cross-borders-fight-them-countries-must-let-medical-data-flow-too.
72. See the health sector section in: Nigel Cory and Ellysse Dick, "How to Build Back Better the Transatlantic Data Relationship" (ITIF, March 25, 2021), https://itif.org/publications/2021/03/25/how-build-back-better-transatlantic-data-relationship.
73. Mark Phillips et al., "Genomics: data sharing needs an international code of conduct," *Nature,* February 5, 2020, https://www.nature.com/articles/d41586-020-00082-9.

74. "Breaking Barriers to Health Data Project," World Economic Forum, https://www.weforum.org/projects/breaking-barriers-to-health-data-project; "Global Alliance for Genomics and Health," https://www.ga4gh.org/about-us/.

75. Ralf Suer tweet: "Interoperable frameworks is just a fancy way of saying please allow the free flow of data, whatever the safeguards in the country of destination. Particularly appealing to countries that lack (comprehensive) privacy laws," March 10, 2021, https://twitter.com/RalfSauer3/status/1369716231134121985.

76. Vincent Maancourt tweet: "U.S.'s Christopher Hoff: "A lot of awesome things about the GDPR but there have been 13 adequacy decisions in the past 26 years and one keeps getting knocked down. So interoperable frameworks ... have to be the future." March 10, 2021, https://twitter.com/vmanancourt/status/1369677987617124366.

77. Centre for Information Policy Leadership (CIPL), "APEC CBPR & PRP: Questions and Answers" (CIPL, March, 2020), https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl_cbpr_and_prp_q_a_final__19_march_2020_.pdf.

78. Ryohei Yasoshima, "US moves to shut China out of shaping APEC data protections," *Asian Nikkei Review,* August 21, 2020, https://asia.nikkei.com/Politics/International-relations/US-China-tensions/US-moves-to-shut-China-out-of-shaping-APEC-data-protections.

79. "PrivCom recognises APEC CBPR System as a certification mechanism for overseas data transfers," Privacy Commissioner of Bermuda, March 2, 2021, https://www.privacy.bm/post/privcom-recognises-apec-cbpr-system-as-a-certification-mechanism-for-overseas-data-transfers.

80. "G7 Digital and Technology Track - Annex 2: Roadmap for Cooperation on Data Free Flow with Trust," https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986160/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf; "Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy," OECD, https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm.

81. The U.S.'s initial decision (later reversed) to exclude financial data from the Trans Pacific Partnership Agreement's anti-localization provisions is indicative.

82. "United States – Singapore Joint Statement on Financial Services Data Connectivity," speech, February 5, 2020, https://home.treasury.gov/news/press-releases/sm899; "COOPERATION ARRANGEMENT ON FINANCIAL TECHNOLOGY INNOVATION," MOU between the U.S. Commodity Futures Trading Commission and the Monetary Authority of Singapore, September 13, 2018, https://www.cftc.gov/sites/default/files/2018-09/cftc-mas-cooparrgt091318_16.pdf; "Singapore and UK to Enhance Cooperation in Data Connectivity, Talent Development, Green Finance and Cybersecurity," media release, June 13, 2019, https://www.mas.gov.sg/news/media-releases/2019/singapore-and-uk-to-enhance-cooperation.

83. Nigel Cory and Stephen Ezell, "Comments to the U.S. International Trade Commission Regarding the United States-Mexico-Canada Agreement" (ITIF, December 17, 2018), https://itif.org/publications/2018/12/17/comments-us-international-trade-commission-regarding-united-states-mexico; "Circular to Licensed Corporations - Use of external electronic data storage," Hong Kong Securities and Futures Commission, October 31, 2019, https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC59.

84. "European Commission: e-evidence," https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime/e-evidence_en; Vanessa Franssen, "The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?" European Law Blog, October 12, 2018,

https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/.

85. Smriti Parsheera and Prateek Jha, "Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?" (Carnegie India, November, 2020), https://carnegieendowment.org/files/ParsheeraJha_DataAccess.pdf.

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

87. For a detailed analysis: Alan McQuinn and Daniel Castro, "How Law Enforcement Should Access Data Across Borders" (ITIF, July 24, 2017), https://itif.org/publications/2017/07/24/how-law-enforcement-should-access-data-across-borders; Microsoft Corporation v. United States, No. 14-2985 (2d Cir. 2017), "Government's Memorandum of Law in Opposition to Microsoft's Motion," (Preet Bharara, Attorney for the United States, April 20, 2014), *Just Security*, accessed June 29, 2017, https://www.justsecurity.org/wp-content/uploads/2014/05/Governments-Memorandum-of-Law-in-Opposition-to-Motion-to-Vacate-doc-97....pdf; "FY 2017 Budget Request – National Security" (U.S. Department of Justice, 2016), accessed June 29, 2017, https://www.justice.gov/jmd/file/822376/download.

88. Richard Clarke et al., "Liberty and Security in a Changing World" (White House, December 18, 2013), accessed June 29, 2017, 227, https://obamawhitehouse.archives.gov/blog/2013/12/18/liberty-and-security-changing-world; *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights*, 115th Cong. (May 24, 2017) (testimony of Brad Wiegmann, Deputy Assistant Attorney General of the U.S. Department of Justice), accessed July 12, 2017, https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf.

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

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

91. Jennifer Daskal and Debrae Kennedy-Mayo, "Budapest Convention: What is it and How is it Being Updated?" Lawfare blog post, July 2, 2020, https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

92. Caitlin Fennessy, "A Multilateral Surveillance Accord: Setting the Table," Lawfare blog post, April 23, 2021, https://www.lawfareblog.com/multilateral-surveillance-accord-setting-table.

93. "Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime," October 3, 2019, https://www.crossborderdataforum.org/wp-content/uploads/2019/10/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf; Jennifer Daskal and Peter Swire, "The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards," Lawfare blog post, October 8, 2019, https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards; U.S. Department of Justice, "The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards," press release, October 7, 2019, https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us; Peter Swire, "EU and U.S. Negotiations on Cross-Border Data, Within and Outside of the Cloud Act Framework," Cross Border Data Forum, April 13, 2019, https://www.crossborderdataforum.org/eu-and-u-s-negotiations-on-cross-border-data-within-and-outside-of-the-cloud-act-framework/; European Commission, "Security Union: Commission receives

mandate to start negotiating international rules for obtaining electronic evidence," press release, June 6, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2891.

94. Peter Swire and Jennifer Daskal, "Frequently Asked Questions about the U.S. CLOUD Act," Cross Border Data Forum, April 16, 2019, https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act/.

95. U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World:The Purpose and Impact of the CLOUD Act* (Washington, D.C: white paper, April, 2019), https://www.justice.gov/opa/press-release/file/1153446/download.

96. Derek Johnson, "The CLOUD Act, one year on," *FCW,* April 8, 2019, https://fcw.com/articles/2019/04/08/cloud-act-turns-one.aspx.

97. Catherine M.A. Carroll, Ari Holtzblatt, and Alexandra Stewart, "Congress Enacts Law Clarifying Reach of Warrants for Overseas Data," Wilmer Hale blog post, March 26, 2018, https://www.wilmerhale.com/en/insights/client-alerts/congress-enacts-law-clarifying-reach-of-warrants-for-overseas-data.

98. "DRAFT UNITED NATIONS CONVENTION ON COOPERATION IN COMBATING INFORMATION CRIMES," Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland," February 20, 2018, https://www.rusemb.org.uk/fnapr/6394; Allison Peters, "Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime," *Foreign Policy,* September 16, 2019, https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/; Joyce Hakmeh and Allison Peters, "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet," Council on Foreign Relations blog post, January 13, 2020, https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet; Marsha Borak, "China to punish data exports to overseas courts as Beijing beefs up defence against US long arm," *South China Morning Post,* April 28, 2021, https://www.scmp.com/tech/policy/article/3131453/china-punish-data-exports-overseas-courts-beijing-beefs-defence-against.

99. "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.

100. "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.

101. Ibid.

102. Kenya's Ministry of Information, Communication, and Technology, *Request for comments on the Proposed Privacy and Data Protection Policy and Bill*, (2018, accessed January 11, 2019), http://www.ict.go.ke/request-for-comments-on-the-proposed-privacy-and-data-protection-policy-and-bill-2018/.

103. Sensitive data is defined as data revealing a person's race, health status, ethnic social origin, political opinion, belief, personal preferences, location, genetic data, biometrics, sex life or sexual orientation, and personal financial expenditures.

104. "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.

105. 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

106. Jumoke Lambo, "Data Localization Laws: Nigeria," Practical Law, https://www.uubo.org/media/1795/data-localization-laws-nigeria-w-022-1015.pdf.

107. 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.

108. "Rwanda Utilities Regulatory Authority fines MTN US$ 8,5M," *CNBC Africa,* May 17, 2017, https://www.cnbcafrica.com/news/2017/05/17/rwanda-utilities-regulatory-authority-fines-mtn-us-85m-non-compliance/.

109. 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/.

110. "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.

111. "Protection of Personal Information Act," South African Institute of Chartered Accountants website, January 14, 2019, https://www.saica.co.za/Technical/LegalandGovernance/Legislation/ProtectionofPersonalInformationAct/tabid/3335/language/en-ZA/Default.aspx. Mona Farid Badran and Rizwan Tufail, "Economic Impact of Data Localization in 5 selected African Countries: an empirical study," *Digital Policy, Regulation and Governance* 20.4 (2018): 337-357.https://pic.strathmore.edu/wp-content/uploads/2019/03/PIC_RANITP_Economic_Impact_of_Data_Localization_in_5_selected_African_Countries.pdf.

112. "Electronic Communications Act, 2005," https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf.

113. Ibid.

114. Ibid.

115. Ibid.

116. Ibid.

117. ECIPE, Digital Trade Estimates Project, (Belgium, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=BE&chapter=829&subchapter=830.

118. Ibid.

119. Ibid.

120. ECIPE, Digital Trade Estimates Project, (Bulgaria, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=BG&chapter=829&subchapter=830.

121. ECIPE, Digital Trade Estimates Project, (Cyprus, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=CY&chapter=829.

122. Ibid.

123. ECIPE, Digital Trade Estimates Project, (Denmark, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=DK&chapter=829&subchapter=830.

124. ECIPE, Digital Trade Estimates Project, (Denmark, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=DK&chapter=829&subchapter=830

125. Nigel Cory, "How 'Schrems II' Has Accelerated Europe's Slide Toward a De Facto Data Localization Regime," Innovation Files blog post, July 8, 2021, https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europes-slide-toward-de-facto-data.

126. CCIA, "CCIA Comments Regarding Foreign Trade Barriers to U.S. Exports for 2021," (Washington, DC: CCIA Net, October 29, 2020), 32-33, https://www.ccianet.org/wp-content/uploads/2020/10/USTR-2020-0034-CCIA-Comments-on-2021-National-Trade-Estimates-Report.pdf; GAIA-X, "Press Release on Franco-German common work on a secure and trustworthy data infrastructure," news release, October 29, 2019, https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Press-Releases/20191029-press-release-on-franco-german-common-work-on-a-secure-and-trustworthy-data-infrastructure.html.

127. Ibid.

128. ECIPE, Digital Trade Estimates Project, (Denmark, Restrictions on Cross-Border Data Flows; Accessed June 2021), ; https://gdpr-info.eu/art-5-gdpr/https://ecipe.org/dte/database/?country=EU&chapter=829&subchapter=830 ; General Data Protection Regulation (2016), https://gdpr-info.eu/art-5-gdpr/.

129. United States Trade Representative (USTR), *2021 National Trade Estimate Report on foreign Trade Barriers*, (Washington, DC: USTR, 2021), 222, https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf.

130. Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)," (February 22, 2021), https://data.consilium.europa.eu/doc/document/ST-6297-2021-INIT/en/pdf

131. ECIPE, Digital Trade Estimates Project, (Finland, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=FI&chapter=829&subchapter=830.

132. ECIPE, Digital Trade Estimates Project, (France, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=FR&chapter=829&subchapter=830.

133. Capgemini, "Capgemini and Orange announce plan to create 'Bleu', a company to provide a 'Cloud de Confiance' in France," press release, May 27, 2021, https://www.globenewswire.com/en/news-release/2021/05/27/2237023/0/en/Press-Release-Capgemini-and-Orange-announce-plan-to-create-Bleu-a-company-to-provide-a-Cloud-de-Confiance-in-France.html.

134. Cynthia Rich, "A Look at New Trends in 2017: Privacy Laws in Europe and Eurasia (non-EEA)," (Bloomberg Law, July 17, 2017), https://media2.mofo.com/documents/170717-privacy-laws-europe-eurasia.pdf

135. Ibid.

136. Ibid.

137. Ibid.

138. ECIPE, Digital Trade Estimates Project, (Germany, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=DE&chapter=829&subchapter=830.

139. ECIPE, Digital Trade Estimates Project, (Greece, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=GR&chapter=829&subchapter=830.

140. ECIPE, Digital Trade Estimates Project, (Italy, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=IT&chapter=829&subchapter=830.

141. Cynthia Rich, "A Look at New Trends in 2017: Privacy Laws in Europe and Eurasia (non-EEA)," *Bloomberg Law*, July 17, 2017, https://media2.mofo.com/documents/170717-privacy-laws-europe-eurasia.pdf.

142. ECIPE, Digital Trade Estimates Project, (Luxembourg, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=LU&chapter=829&subchapter=830.

143. ECIPE, Digital Trade Estimates Project, (Malta, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=MT&chapter=829.

144. Cynthia Rich, "A Look at New Trends in 2017: Privacy Laws in Europe and Eurasia (non-EEA)," *Bloomberg Law*, July 17, 2017, https://media2.mofo.com/documents/170717-privacy-laws-europe-eurasia.pdf.

145. Ibid.

146. Ibid.

147. ECIPE, Digital Trade Estimates Project, (Netherlands, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=NL&chapter=829&subchapter=830.

148. Ibid.

149. ECIPE, Digital Trade Estimates Project, (Poland, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=PL&chapter=829&subchapter=830.

150. ECIPE, Digital Trade Estimates Project, (Romania, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=RO&chapter=829&subchapter=830.

151. ECIPE, Digital Trade Estimates Project, (Romania, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=RO&chapter=829&subchapter=830.

152. Russian Duma Bill No. 1176731-7, https://sozd.duma.gov.ru/bill/1176731-7; "RUSSIA: BUSINESS ACTIVITY ON THE INTERNET NETWORK CURRIED OUT BY FOREIGN OPERATORS," May 27, 2021, https://www.pavia-ansaldo.it/en/russia-business-activity-on-the-internet-network-curried-out-by-foreign-operators/.

153. Garant, "Decree of the Government of the Russian Federation of December 21, 2019 No. 1746," news release, December 21, 2019, https://www.garant.ru/products/ipo/prime/doc/73232186/; Human Rights Watch, "Russia: Growing Internet Isolation, Control, Censorship," (Human Rights Watch, June 18, 2020), https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship; Alexander Bychkov, "Russia Prohibits Public Procurement of Foreign Data Storage Systems," (Baker McKenzie, January 10, 2020), https://www.bakermckenzie.com/en/insight/publications/2020/01/russia-prohibits-public-procurement-foreign-data.

154. Tass, "Yarovaya law obliges operators and Internet companies to store user correspondence," news release, July 1, 2018, https://tass.com/politics/1011585.

155. Garant, "Decree of the Government of the Russian Federation of May 28, 2019 No. 673," news release, May 28, 2019, http://base.garant.ru/72255540/.

156. "Russia's Assault on Freedom of Expression," (Human Rights Watch, 2017), https://www.hrw.org/sites/default/files/report_pdf/russiafoe0717_web_2.pdf#page=32; The amendments are a set of two federal laws: Federal Law No 374-FZ from July 6, 2016 "On Amendments to the Federal Law 'On Combating Terrorism' and Separate Legislative Acts Concerning Countering Terrorism and Ensuring Public Safety," http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=201078&fld=134&dst=1000000001,0&rnd=0.4015094842406974#0 (accessed February 19, 2017); and Federal Law No 375-FZ from July 6, 2016 "On Amendments to the Criminal Code and the Criminal Procedure Code of the Russian Federation Introducing Additional Counter-Terrorism and Public Safety Measures," http://www.consultant.ru/document/cons_doc_LAW_201087.

157. "The 'localisation' of Russian citizens' personal data," (KPMG, Accessed June 2021), https://home.kpmg/be/en/home/insights/2018/09/the-localisation-of-russian-citizens-personal-data.html.

158. Tass, "Yarovaya law obliges operators and Internet companies to store user correspondence," news release, July 1, 2018, https://tass.com/politics/1011585; The Bell, "FSB demanded from Internet services online access to data and correspondence of users," news release, February 11, 2020, https://thebell.io/fsb-potrebovala-ot-internet-servisov-onlajn-dostup-k-dannym-i-perepiske-polzovatelej

159. Ibid; 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.

160. The Bank of Russia Regulations on the Procedure of Creation, Maintenance and Database Storageon Electronic Media No. 397-P dated February 21, 2013 (as amended on September 14, 2016).

161. Vladimir Kanashevsky, "Use of Public Cloud Services by Russian Financial Services Institutions," *Pierstone* (November 15, 2017), https://pierstone.com/use-of-public-cloud-services-by-russian-financial-services-institutions/

162. Vladimir Kanashevsky, "Use of Public Cloud Services by Russian Financial Services Institutions," Pierstone (November 15, 2017), https://pierstone.com/use-of-public-cloud-services-by-russian-financial-services-institutions/.

163. Ibid. Such encryption requirements are the measures required by Government Decree No 1119 and FSB guidelines.

164. Cynthia Rich, "A Look at New Trends in 2017: Privacy Laws in Europe and Eurasia (non-EEA)," *Bloomberg Law*, July 17, 2017, https://media2.mofo.com/documents/170717-privacy-laws-europe-eurasia.pdf.

165. Ibid.

166. ECIPE, Digital Trade Estimates Project, (Sweden, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=SE&chapter=829&subchapter=830.

167. ECIPE, Digital Trade Estimates Project, (Sweden, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=SE&chapter=829&subchapter=830; Jennie Nilson and Edvard Henriksson, "The Swedish Data Protection Authority Publishes its Supervisory Plan for 2019–2020," *Global Compliance News*, June, 2019, https://www.globalcompliancenews.com/2019/06/27/swedish-data-protection-authority-publishes-supervisory-plan-for2019-2020-20190506/.

168. 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.

169. Ibid.

170. New Regulation on Bank IT Systems and Electronic Banking Services, Lexology, March 18, 2020, https://www.lexology.com/library/detail.aspx?g=820f9766-219b-4196-9554-bfc715fd1676.

171. "Facebook to defy new Turkish social media law," *Financial Times,* October 5, https://www.ft.com/content/91c0a408-6c15-45c3-80e3-d6b2cf913070.

172. New Presidential Decree on Information and Communication Security Measures, Lexology, July 25, 2019, https://www.lexology.com/library/detail.aspx?g=8e18f85a-286f-4d29-b017-b17541c3c66b; CCIA, "Comments Regarding Foreign Trade Barriers to U.S. Exports for 2021," (Washington, DC: CCIA Net, October 29, 2020), https://www.ccianet.org/wp-content/uploads/2020/10/USTR-2020-0034-CCIA-Comments-on-2021-National-Trade-Estimates-Report.pdf.

173. Serra Hiziroglu and Ayça Sarıkamış, "Communiqués recently published by capital markets board on information systems management and independent audit of information systems," Lexology, February 7, 2018, https://www.lexology.com/library/detail.aspx?g=c6601e1b-6d4b-40c6-81ed-834fc60cea3c.

174. Nezihe Boran Demir, "Management of Information System," Erdem and Erdem website, March 2018, accessed January 11, 2018, http://www.erdem-erdem.av.tr/publications/newsletter/management-of-information-systems/.

175. Yusuf Mansur Özer, "GDPR matchup: Turkey's Data Protection Law," August 10, 2017, https://iapp.org/news/a/gdpr-matchup-turkeys-data-protection-law/.

176. "Law on the Protection of Personal Data," https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aea97a33-089b-4e7d-85cb-694adb57bed3.pdf.

177. CCIA, "CCIA Comments Regarding Foreign Trade Barriers to U.S. Exports for 2021," (Washington, DC: CCIA Net, October 29, 2020), 66-67, https://www.ccianet.org/wp-content/uploads/2020/10/USTR-2020-0034-CCIA-Comments-on-2021-National-Trade-Estimates-Report.pdf.

178. ECIPE, Digital Trade Estimates Project, (Turkey, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=TR&chapter=829&subchapter=830

179. Cynthia Rich, "A Look at New Trends in 2017: Privacy Laws in Europe and Eurasia (non-EEA)," *Bloomberg Law*, July 17, 2017, https://media2.mofo.com/documents/170717-privacy-laws-europe-eurasia.pdf.

180. Ibid.

181. ECIPE, Digital Trade Estimates Project, (United Kingdom, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=GB&chapter=829&subchapter=830.

182. 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.

183. 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

184. Jordon Draft Personal Data Protection Law of 2020, (2020); Zain Shaheen, "Jordan: The Protection of Personal Data," (Data Guidance: March, 2020), https://www.dataguidance.com/opinion/jordan-protection-personal-data.

185. Data Confidentiality Protection Regulations, (2021); Data Guidance, "Kuwait: CITRA issues Data Privacy Protection Regulation for service providers," news release, April 15, 2021, https://www.dataguidance.com/news/kuwait-citra-issues-data-privacy-protection-regulation.

186. National Data Management Office (NDMO), "National Data Governance Interim Regulations," (NDMO, June 1, 2020), https://sdaia.gov.sa/ndmo/Files/PoliciesEn.pdf.

187. Saudi Arabia's Communications and Information Technology Commission, Cloud Computing Regulatory Framework (Riyadh, 2018), http://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf.

188. Nigel Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018," (ITIF, January 2019), https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018.

189. "National Cybersecurity Authority, Essential Cybersecurity Controls," https://itig-iraq.iq/wp-content/uploads/2019/08/Essential-Cybersecurity-Controls-2018.pdf.

190. See Saudi Arabia's draft Cloud Cybersecurity Controls, LEXOLOGY (Apr. 29, 2020), https://www.lexology.com/library/detail.aspx?g=7e35491b-6ab0-40c6-8d10-26351fb2bc37.

191. "New regulation on the use of ICT in healthcare in the UAE," Simmons and Simmons law firm, July 7, 2020, https://www.simmons-simmons.com/en/publications/ckcbolcc9l9s90a791x94jrz0/new-regulation-on-the-use-of-ict-in-healthcare-in-the-uae; "Federal Law No. 2," February 6, 2019, https://tahseen.ae/media/2702/uae-ict-health-law-english.pdf.

192. Kellie Blyth, "UAE: Health Data Law – Permitted Transfers of Health Data," Baker McKenzie law firm, July 7, 2021, https://me-insights.bakermckenzie.com/2021/07/07/uae-health-data-law-permitted-transfers-of-health-data/.

193. United Arab Emirates Draft Data Privacy Law, (2021).

194. 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/.

195. "Law of the Republic of Kazakhstan dated 24 November 2015 No. 418-V," https://adilet.zan.kz/eng/docs/Z1500000418.

196. 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.

197. "Resolution of the Government of the Republic of Kazakhstan dated March 30, 2010 No. 246," https://adilet.zan.kz/rus/docs/P100000246_.

198. 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 / Nқ," https://adilet.zan.kz/rus/docs/V1800016654.

199. "The Law of the Republic of Kazakhstan dated 5 July 2004 No. 567," a https://adilet.zan.kz/eng/docs/Z040000567_.

200. 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/.

201. Bangladesh Bank Company Act, (1991), https://www.findevgateway.org/paper/1991/01/bank-company-act-bangladesh-1991.

202. Asia Internet Coalition (AIC) policy tracker; Industry Submission by AIC on the draft Personal Data Protection Act, (2020), https://mcusercontent.com/3db897db1506081dc74dd704d/files/d7abfc5b-3035-4fea-9ae8-6095e92c7c5f/_DRAFT_Personal_Data_Protection_Act_2020.pdf.

203. Global Data Alliance, "Comments to the People's Republic of Bangladesh on The Draft Cloud Computing Policy," May 2021, https://www.globaldataalliance.org/downloads/05122021gdabdcloudpol.pdf.

204. Reserve Bank of India (RBI), *Amendment to the Master Direction (MD) on KYC*, (RBI, May 10, 2021), https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT354BE2BCC23B344982BD5793737940EFF3.PDF;

205. Securities and Exchange Board of India (SEBI), *Circular No.: SEBI/HO/MIRSD2/DOR/CIR/P/2020/221*, (SEBI, November 3, 2020), https://www.sebi.gov.in/legal/circulars/nov-2020/advisory-for-financial-sector-organizations-regarding-software-as-a-service-saas-based-solutions_48081.html

206. Reserve Bank of India (RBI), *Storage of Payment System Data*, (RBI, April 6, 2018), https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11244; Reserve Bank of India (RBI), *Statement on Developmental and Regulatory Policies,* (RBI, April 5, 2018), https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=43574; Reserve Bank of India (RBI), *First Bi-monthly Monetary Policy Statement, 2018-19,* (RBI, April 10, 2018), https://rbi.org.in/scripts/BS_ViewBulletin.aspx?Id=17479; Reserve Bank of India (RBI), *Storage of Payment System Data*, (RBI, April 6, 2018), https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130.

207. Nigel Cory, "Comments on India's Draft National E-Commerce Policy," (ITIF, 2019), https://itif.org/publications/2019/03/08/comments-indias-draft-national-e-commerce-policy.

208. Reserve Bank of India (RBI), *Storage of Payment System Data*, (RBI, April 6, 2018), https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130.

209. 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.

210. Paragraph 2.1(d)(i) of the Guidelines provides that: *"the location of the data (text, audio, video, or image files, and software (including machine images), that are provided to the cloud service provider for processing, storage or hosting by the cloud service provider services in connection with the Department's account and any computational results that a Department or any end user derives from the foregoing through their use of the cloud service provider's services) shall be as per the terms and conditions of the empanelment of the cloud service provider."* Issued by the Ministry of Electronics and Information Technology on March 31, 2017. See: https://meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf.

211. Department of Industrial Policy and Promotion, Ministry of Commerce and Industry, Government of India, Consolidated FDI Policy, 2017, http://dipp.nic.in/sites/default/files/CFPC_2017_FINAL_RELEASED_28.8.17.pdf#107.

212. Regulation 18(ii) provides that: *"In cases where Insurer outsources to the service providers outside India, the Insurers shall ensure that the terms of the agreement are in compliance with respective local regulations governing the outsourcing service provider and laws of the country concerned and such laws and regulations do not impede the regulatory access and oversight by the Authority. All original policyholder records continue to be maintained in India."* https://taxguru.in/corporate-law/insurance-regulatory-development-authority-india-outsourcing-activities-indian-insurers-regulations-2017.html

213. Rule 3(5) of the Companies (Accounts) Rules, 2014 mandates that: *"the back-up of the books of account and other books and papers of the company maintained in electronic mode, including at a place outside India, if any, shall be kept in servers physically located in India on a periodic basis."* Stephen Mathias and Naqeeb Ahmed Kazia, "Collection, Storage and Transfer of Data in India," Lexology, February 8, 2017, http://www.lexology.com/library/detail.aspx?g=00e56cb6-b0ea-46b7-ab1b-1d52de3646d0; "India Companies (Accounts) Rules 2014" (to be published in the Gazette of India, Government of India Ministry of Corporate Affairs, New Dehli, March 2014), http://perry4law.org/clii/wp-content/uploads/2014/03/Companies-Accounts-Rules-2014.pdf.

214. India Department of Science and Technology, National Data Sharing and Accessibility Policy," 2012, https://dst.gov.in/national-data-sharing-and-accessibility-policy-0.

215. Amendments in Unified Access Service License Agreement, issued by the Ministry of Communications and IT, Government of India. As per Clause 1G(iv): *"The Licensee shall not transfer the following to any person/place outside India: a. any accounting information relating to the subscriber (except for international roaming/billing) (Note: it does not restrict a statutorily required disclosure of financial nature); and b. user information (except about foreign subscribers using Indian Operator's network while roaming and IPLC subscribers)."* https://www.mondaq.com/india/data-protection/928916/what39s-driving-data-localisation-in-india-

216. The Public Records Act 1993.

217. "Ministry of Electronics and Information Technology Notification," *The Gazette of India*, February 25, 2021, https://egazette.nic.in/WriteReadData/2021/225464.pdf; Daniel Castro, "India's Intermediary Liability Law Out of Step With Global Norms," (ITIF, May 11, 2021), https://itif.org/publications/2021/05/11/indias-intermediary-liability-law-out-step-global-norms

218. The Information Technology Act, (2000), https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=#:~:text=%5B9th%20June%2C%202000%5D%20An,communication%20and%20storage%20of%20information%2C.

219. Ministry of Science and Technology, *Draft National Geospatial Policy*, (New Delhi: Ministry of Science and Technology, February 2021), https://dst.gov.in/draft-national-geospatial-policy-2021-public-consultation

220. Ministry of Electronics and Information Technology, *Report by the Committee of Experts on Non-Personal Data Governance Framework*, (2020), https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf; Asia Internet Coalition Policy Mapping Tracker.

221. Money Control, "SEBI may ask foreign brokers to store data locally: Report," (Money Control, January 14, 2019), https://www.moneycontrol.com/news/business/markets/sebi-may-ask-foreign-brokers-to-store-data-locally-report-3386101.html

222. Section 3(29) of the Draft Bill defines 'personal data' to mean data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information. Also see Section 40 of the Draft Bill. USTR, "2021 National Trade Estimate Report on Foreign Trade Barriers" (Washington, D.C: USTR, 2021), https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf.

223. Nigel Cory, "Comments on India's Draft National E-Commerce Policy," (ITIF, 2019), https://itif.org/publications/2019/03/08/comments-indias-draft-national-e-commerce-policy.

224. Ministry Of Health and Family Welfare (Department of Health and Family Welfare), Notification: Amendment to the Drugs and Cosmetics Rules (1945), 28 August 2018, http://www.cdsco.nic.in/writereaddata/2018_08_28_Draft%20GSR%20817(E)_Sale%20of%20Drugs%20by%20E-Pharmacy.pdf.

225. United States Trade Representative (USTR), *The 2017 National Trade Estimate report*, (Washington, DC: USTR, 2021), https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf.

226. 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.

227. Asia Internet Coalition, Industry Submission by AIC on Sri Lanka's Personal Data Protection Bill 2019; https://iapp.org/news/a/final-draft-of-personal-data-protection-bill-introduced-in-sri-lanka/.

228. Vijayant Singh, "Comparing The Sri Lankan Personal Data Protection Bill, 2019 And The GDPR," (Mondaq, June 2020), https://www.mondaq.com/india/data-protection/956530/comparing-the-sri-lankan-personal-data-protection-bill-2019-and-the-gdpr#_ftn16

229. Asia Internet Coalition, translation of Kominfo Circular 3/2021 on the Use of Cloud for the Public Sector.

230. 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.

231. 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.

232. Cahyani Endahayu et al., "Indonesia Now Has Specific E-commerce Regulation," Baker McKenzie, December 18, 2019, https://www.bakermckenzie.com/en/insight/publications/2019/12/indonesia-specific-e-commerce-regulation.

233. Submission on Indonesia's Ministerial Regulation No. 5/2020 ("MR 5"), (2020), https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020.

234. The Coalition of Services Industries (CSI), "Comments for the National Trade Estimate Report on Foreign Trade Barriers," 2019, https://secureservercdn.net/198.71.233.106/v8v.669.myftpupload.com/wp-content/uploads/2020/02/2019-NTE-Submission.pdf; United States Trade Representative (USTR), *2021 National Trade Estimate Report on foreign Trade Barriers*, (Washington, DC: USTR, 2021), 345, https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf.

235. "BSA/The Software Alliance: Comments on Korea's Cloud Security Assurance Program," August 8, 2019, https://www.bsa.org/files/policy-filings/en08082019bsarevisedcloudsecurityassuranceprogram.pdf.

236. E.g., under RSEFT Article 14-2-8 (Usage process of cloud computing service), finance companies and electronic finance service providers shall use domestically located information process systems and apply Article 11-12 to process personal credit information or identification information.

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

238. Alex Wall, "GDPR matchup: South Korea's Personal Information Protection Act," IAPP, January 8, 2018, https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/.

239. Asia Internet Coalition (AIC) policy tracker.

240. Yee Chung Seck, "Updates to Draft Decree Detailing Certain Articles of Law on Cybersecurity," Baker McKenzie, October 2019, https://www.bakermckenzie.com/en/insight/publications/2019/10/updates-draft-decree-law-on-cybersecurity.

241. See: GSI/PR Supplementary Norms no. 4 and 19; MP/STI Ordinance no. 20/2016; and Ordinance No. 9, 2018."

242. Projeto de Lei No. 13.709 de 2020, (2020), https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=FBFEDDCD86E43AC204C6E5AA41823F12.proposicoesWebExterno2?codteor=1932528&filename=Tramitacao-PL+4723/2020.

243. Comisón para el Mercado Financiero, "RECOPILACION ACTUALIZADA DE NORMAS Capítulo 20-7," (Santiago: Comisón para el Mercado Financiero, 2014, https://www.cmfchile.cl/portal/principal/613/articles-28982_doc_pdf.pdf; CCIA, "Comments regarding Foreign Trade Barriers to U.S. Exports for 2021 Reporting," (Washington, DC: CCIA Net, October 29, 2020), https://www.ccianet.org/wp-content/uploads/2020/10/USTR-2020-0034-CCIA-Comments-on-2021-National-Trade-Estimates-Report.pdf.

244. Presidency of the Council of Ministers, "First Draft of National Estrategy for AI," (Presidency of the Council of Ministers, 2021)

245. CCIA, "Comments regarding Foreign Trade Barriers to U.S. Exports for 2021 Reporting," (Washington, DC: CCIA Net, October 29, 2020), https://www.ccianet.org/wp-content/uploads/2020/10/USTR-2020-0034-CCIA-Comments-on-2021-National-Trade-Estimates-Report.pdf

246. Business Roundtable, "Promoting Economic Growth Through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements" (Business Roundtable, June 2012), 5, http://businessroundtable.org/uploads/studies-reports/downloads/Global_IT_Policy_Paper_final.pdf.

247. Yan Luo, Zhijinh Yu, and Vicky Liu, "The future of data localization and cross-border transfer in China: a unified framework or a patchwork of requirements?," IAPP, June 22, 2021, https://iapp.org/news/a/the-future-of-data-localization-and-cross-border-transfer-in-china-a-unified-framework-or-a-patchwork-of-requirements/.

248. Notice by the People's Bank of China Regarding the Effective Protection of Personal Financial Information by Banking Institutions, (2011), http://www.lawinfochina.com/display.aspx?lib=law&id=8837&CGid=; Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010.

249. Insurance Law of the People's Republic of China, (revision 2015), http://www.cmac.org.cn/wp-content/uploads/2018/08/Insurance-Law-of-the-People%E2%80%99s-Republic-of-ChinaRevision-2015.pdf; Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook

2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010.

250. Regulation on the Administration of Credit Investigation Industry, (2013), http://www.lawinfochina.com/display.aspx?lib=law&id=12585&CGid=&EncodingName=big5; Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010.

251. Measures for the Administration of the Real-Name Receipt and Delivery of Mails and Express Mails, (2018), http://lawinfochina.com/display.aspx?id=a81d94ee8e5f1daabdfb&lib=law; Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010.

252. Administrative Measures for Population Health Information, (2014), https://uk.practicallaw.thomsonreuters.com/4-616-3729?transitionType=Default&contextData=(sc.Default)&firstPage=true; Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010.

253. Interim Measures for the Administration of Online Taxi Booking Business Operations and Services, (2016), http://lawinfochina.com/display.aspx?id=22963&lib=law; Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010.

254. Regulation on Map Management, (2015), http://www.lawinfochina.com/display.aspx?id=21392&lib=law&EncodingName=big5; Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010.

255. Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010

256. Ibid.

257. Yan Luo and Zhijing Yu, "China Releases Personal Financial Information Protection Technical Specification," Covington, March 2, 2020, https://www.insideprivacy.com/international/china/china-releases-personal-financial-information-protection-technical-specification/ ; Tears of Loneliness, "The Central Bank officially released the 'Technical Specifications for Personal Financial Information Protection,'" (2020), https://xw.qq.com/cmsid/20200221A0OCHF00?f=newdc; Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010.

258. Scott Thiel, Carolyn Bigg, Venus Cheung, and Fangfang Song, "Stricter Data Localisation And Security Rules For Financial And Insurance Data In China Navigating China: The digital journey," Mondaq, December 22, 2020, https://www.mondaq.com/china/security/1018664/stricter-data-localisation-and-security-rules-for-financial-and-insurance-data-in-china.

259. Ibid; Conventus Law, "PBOC Publishes New Data Protection Guidelines For Financial Institutions," (Conventus Law: March, 2020), https://www.conventuslaw.com/report/china-pboc-publishes-new-data-protection/.

260. Tears of Loneliness, "The Central Bank officially released the 'Technical Specifications for Personal Financial Information Protection,'" (2020), https://xw.qq.com/cmsid/20200221A0OCHF00?f=newdc.

261. "Interim Measures for the Administration of the Credit Rating Industry," 2019, http://en.pkulaw.cn/display.aspx?cgid=e435babe476ae89dbdfb&lib=law.

262. "US-China Business Council Comments on the Administrative Measures for Bank Card Clearing Institutions (Revised Draft for Comments)," January 28, 2020, https://www.uschina.org/sites/default/files/uscbc_comments_on_administrative_measures_on_bank_card_clearing_institutions_revised_draft_for_comments_-_en.pdf; "Decision of the State Council on Implementing Access Administration of Bank Card Clearing Institutions," May 19, 2020, http://english.beijing.gov.cn/investinginbeijing/WhyBeijing/lawpolicy/policies/202005/t20200519_1901976.html.

263. Securities Law of the People's Republic of China, (2019), http://www.xinhuanet.com/legal/2019-12/29/c_1125399656.htm.

264. Order of the China Banking and Insurance Regulatory Commission, (2019), http://www.gov.cn/gongbao/content/2019/content_5446227.htm.

265. Regulations of the People's Republic of China on the Administration of Human Genetic Resources, (2019), http://www.gov.cn/zhengce/content/2019-06/10/content_5398829.htm.

266. Central Bank of the People's Republic of China, "Announcement on Open Market Operations No.131" (2021), http://www.pbc.gov.cn/tiaofasi/144941/144979/3941920/3950322/index.html.

267. Nigel Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018," (ITIF, January, 2019), https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018.

268. Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010; ECIPE, Digital Trade Estimates Project, (China, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=CN&chapter=829&subchapter=830.

269. Mark Schaub, et al., "China: Mapping the Future - Current Challenges and Forecast trends in respect of Mapping for Autonomous Vehicles," King & Wood Mallesons, January 2018, https://www.kwm.com/en/cn/knowledge/insights/china-mapping-the-future-20180119; @nigelcory on Twitter, accessed June, 2021, https://twitter.com/nigelcory/status/1144659827626520576; Mark Schaub, Xue Han, and Atticus Zhao, "Autonomous vehicles: Legal issues on Survey, Data Collection and Transfer," (King & Wood Mallesons: June, 2019), https://www.chinalawinsight.com/2019/06/articles/high-technology/autonomous-vehicles-legal-issues-on-survey-data-collection-and-transfer/.

270 Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010; ECIPE, Digital Trade Estimates Project, (China, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=CN&chapter=829&subchapter=830.

271. Ibid.

272. Timothy Stratford and Yan Luo, "3 Ways Cybersecurity Law In China Is About To Change," *Law360,* May 2, 2016, https://www.cov.com/-/media/files/corporate/publications/2016/05/3_ways_cybersecurity_law_in_china_is_about_to_change.pdf.

273. Ibid.

274. ECIPE, Digital Trade Estimates Project, (China, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=CN&chapter=829&subchapter=830.

275. Regulation on Credit Reporting Industry, (2013), http://www.pbccrc.org.cn/crc/jgyhfw/201309/1ca0f775b50744cabaf83538288d77a9/files/e8a8bf080ed64f48914a652da1d8fdc3.pdf.

276. Ibid.

277. Timothy Stratford and Yan Luo, "3 Ways Cybersecurity Law In China Is About To Change," *Law360,* May 2, 2016, https://www.cov.com/-/media/files/corporate/publications/2016/05/3_ways_cybersecurity_law_in_china_is_about_to_change.pdf.

278. Ibid.

279. Ibid; Mark Schaub, Atticus Zhao, and Xia Shengying, "China: Mapping the Future - Current Challenges and Forecast trends in respect of Mapping for Autonomous Vehicles," King and Wood Mallesons, January 19, 2018, https://www.kwm.com/en/cn/knowledge/insights/china-mapping-the-future-20180119.

280. [translated] "Notice of the State Internet Information Office on the Public Consultation on the "Cyber Security Review Measures (Revised Draft for Solicitation of Comments)," Cyberspace Administration of China, July 10, 2021, http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm.

281. CCIA, "Comments regarding Foreign Trade Barriers to U.S. Exports for 2021 Reporting," (Washington, DC: CCIA Net, October 29, 2020), 28, https://www.ccianet.org/wp-content/uploads/2020/10/USTR-2020-0034-CCIA-Comments-on-2021-National-Trade-Estimates-Report.pdf; United States Trade Representative (USTR), 2021 National Trade Estimate Report on foreign Trade Barriers (Washington, DC: USTR, 2021), 128, https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf.

282. (translated) "Credit Business Management Measures (Draft for Comments)," accessed July 10, 2021, http://www.moj.gov.cn/news/content/2021-01/11/zlk_3264282.html.

283. "China Issued Draft Provisions on the Management of Automobile Data Security," JD Supra, June 14, 2021, https://www.jdsupra.com/legalnews/china-issued-draft-provisions-on-the-6616687/.

284. Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010

285. Katharin Tai, Lorand Laskai, Rogier Creemers, Mingli Shi, Kevin Neville, and Paul Triolo, "Translation: China's New Draft 'Data Security Management Measures,'" Digichina blog post, May 31, 2021, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/.

286. CCIA, "Comments regarding Foreign Trade Barriers to U.S. Exports for 2021 Reporting," (Washington, DC: CCIA Net, October 29, 2020), 27, https://www.ccianet.org/wp-content/uploads/2020/10/USTR-2020-0034-CCIA-Comments-on-2021-National-Trade-Estimates-Report.pdf; Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010; DLA Piper, "Data Protection Laws of the World," (DLA Piper: January, 2021), https://www.dlapiperdataprotection.com/index.html?t=transfer&c=CN&c2=.

287. Samuel Yang, "China: Data Localization," (Global Data Review Insight Handbook 2021), https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation#footnote-010

288. Ibid.

289. Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost," (ITIF: May, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-

and-what-do-they-cost; Anthony Borgese, "Australia: Data Protection Laws and Regulations," (ICLG: 2021), https://iclg.com/practice-areas/data-protection-laws-and-regulations/australia

290. Ibid; ECIPE, Digital Trade Estimates Project, (New Zealand, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=NZ&chapter=829&subchapter=830

291. Ibid; ECIPE, Digital Trade Estimates Project, (Canada, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=CA&chapter=829&subchapter=830

292. ECIPE, Digital Trade Estimates Project, (Canada, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=CA&chapter=829&subchapter=830.

293. Office of the Privacy Commissioner of Canada, Commissioner concludes consultation on transfers for processing (September 2019), available at https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190923/.

294. ECIPE, Digital Trade Estimates Project, (Mexico, Restrictions on Cross-Border Data Flows; Accessed June 2021), https://ecipe.org/dte/database/?country=MX&chapter=829&subchapter=830.

295. Diario Oficial de la Federación, "PROVISIONS applicable to electronic payment fund institutions," (2021), https://dof.gob.mx/nota_detalle.php?codigo=5610487&fecha=28/01/2021

296. "Announcing AWS GovCloud (US)," AWS website, https://aws.amazon.com/about-aws/whats-new/2011/08/16/announcing-aws-govcloud-us/.

297. "What Is AWS GovCloud (US)?" AWS website, https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/whatis.html; "AWS GovCloud (US)," AWS website, https://aws.amazon.com/govcloud-us/?whats-new-ess.sort-by=item.additionalFields.postDateTime&whats-new-ess.sort-order=desc.

298. "FedRAMP Control Specific Contractual Clauses, Version 3.0," https://www.fedramp.gov/assets/resources/documents/Agency_Control_Specific_Contract_Clauses.pdf; "Security and Privacy Controls for Information Systems and Organizations," NIST website, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

299. "City of Los Angeles: Supplemental Report – Information Technology Agency Request to Enter into a Contract with Computer Science Corporation for the Replacement of the City's Email System," Office of the City Clerk, City of Los Angeles website, http://clkrep.lacity.org/onlinedocs/2009/09-1714_rpt_cao_10-7-09.pdf.

300. Ron Wyden Campaign Website, "Wyden Releases Draft Legislation to Protect Americans' Personal Data From Hostile Foreign Governments," April 15, 2021, https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-protect-americans-personal-data-from-hostile-foreign-governments.

301. "Senate Bill S3713 of 2011," New York State Senate website, accessed April 26, 2017, https://www.nysenate.gov/legislation/bills/2011/S3713.

302. "Table Tracking State and Federal Global Sourcing Legislation," National Foundation for American Policy website, accessed April 26, 2017, http://www.nfap.com/researchactivities/globalsourcing/appendix.aspx.

303. "House Bill No. 1497," Missouri House of Representatives website, accessed April 26, 2017, http://www.house.mo.gov/billtracking/bills041/billpdf/intro/HB1497I.PDF.