CSIS BRIEFS

The Real National Security Concerns over Data Localization

By Lindsey R. Sheppard, Erol Yayboke, and Carolina G. Ramos

JULY 2021

THE ISSUE

- As the internet has grown to be an integral part of society, so too have the needs of citizens, companies, and governments to consider how and where data is stored and who has access to it.
- Whether for data sovereignty, national security and intelligence gathering, commercial, or privacy reasons, governments are increasingly seeking to maintain "digital sovereignty" and control through protectionist data localization mandates.
- National security justifications for these mandates are often thinly veiled attempts at asserting greater control of the domestic digital domain; meanwhile, data localization has had negative impacts on human rights, privacy, and economic interests.
- This brief focuses on the real national security implications—which have received relatively little attention—of policies that mandate certain data be stored or processed within specific geographic boundaries.

Data localization mandates affect a variety of national security interests, including the ability of security actors to share information, promote cybersecurity, and fight the tools of digital authoritarianism. These mandates are also routinely implemented under shaky "national security" pretenses. Even established democracies have struggled to balance the allure of the so-called **digital sovereignty** afforded by data localization with the economic and national security arguments against such policies. While much has been made of **the economic impact—especially the threat to businesses**—if data cannot flow freely across borders, there has not been in-depth dialogue on the real national security implications of global data-flow restrictions. Further, while the localization of data has been discussed at length throughout the past five years, U.S. policymakers have yet to reach a formal consensus on domestic data localization mandates or assemble responses to policies enacted by allies and adversaries alike.

As the number of nations that restrict or prohibit data flows **grows**, the United States faces increased pressure from allies and the business community to articulate its long-standing stance against data localization more clearly and to formulate related, sound policy that takes into consideration the shifting global landscape. To fully assess the national security implications of localizing data, the CSIS study team convened a virtual workshop in May 2021 with senior leaders, scholars, and practitioners. As emphasized at the workshop discussion, there is a need for in-depth and nuanced conversations on specific U.S. national security-related implications of data localization.

Established democracies have struggled to balance the allure of the so-called digital sovereignty afforded by data localization with the economic and national security arguments against such policies.

There is no "one size fits all" outcome for the future of data localization policy. This brief frames the issue as it currently manifests, presents substantive national security concerns, and offers recommendations on a way forward for the United States and its like-minded friends and allies. Distinct policies addressing each localization-related concern will require deeper insight into data localization's potential to impact multiple facets of national security. Above all, policymakers must be wary of fragmenting the internet, especially if the result is increased vulnerability to manipulation and coercion.

THE SHIFT TOWARD DATA LOCALIZATION

The most common and widely accepted definition of "data localization" is policies or mandates requiring certain data related to citizens or residents of a country—whether personal, health, business, or financial—to be physically stored on infrastructure within that country's borders. Additionally, policies may establish **different categories of data**, as in the distinction between "personal data," "sensitive personal data," and "critical personal data," and apply different levels of restrictions or permissions to each.

In practice, data localization mandates come in a variety of forms and manifestations. However, most approaches can be generally classified as:

- hard localization,
- mirroring or soft localization,
- hybrid localization, or
- de facto localization.

Further, one or more of the above approaches may be applied to different categories of data within a country's overall data governance framework.

Under hard localization mandates, data may only be processed and stored within the issuing country's borders. In other words, data may not be transferred outside the jurisdiction. Hard localization affects major data flows and digital platforms. International data transfers necessary for delivery of even mundane services **like email** may require transfer, storage, and processing that may be inconsistent with hard localization mandates. For example, China's 2017 **Cybersecurity Law** and 2020 draft **Personal Information Protection Law** require that various forms of data, including personal data, be stored in China and undergo a government "security review" before transfer.

Mirroring or soft localization mandates allow data to be transferred outside the jurisdiction for processing and storage, but a copy of the data must be retained within the issuing nation's borders. An example of this form of localization is found within **India's draft Personal Data Protection Bill** (see **chapter 8** of bill text) and **Pakistan's draft Personal Data Protection Bill** (see **section 15** of bill text). Soft localization requires providers to retain a copy of the data within the country. However, the India and Pakistan bills add additional requirements to the mirroring approach, allowing for the transfer of broadly defined "sensitive personal data" outside of the issuing country, subject to certain preconditions.

Hybrid localization mandates are a form of hard localization that adopts the permissiveness of soft localization. While data can only be stored in the jurisdiction where it is created, it can temporarily be processed outside of the jurisdiction to facilitate related transactions. Through a **2018 directive** issued by the Reserve Bank of India, India has implemented hybrid localization requirements related to payments data. Within this "Storage of Payment System

Data" mandate, there are no restrictions on processing payments outside the country, but once the processing is complete, the data must be stored only in India. If stored (even temporarily) outside of the jurisdiction, it must be deleted within 24 hours or one business day. However, the data can be accessed when needed for all activities related to processing.

De facto data localization results when a nation or governing body has no express data localization requirements but does enact laws or mandates that permit data to be transferred outside of the jurisdiction only if certain conditions are met. These can include threat of fines, bureaucratic roadblocks, or other excessive requirements that make regular cross-border data transfers risky, costly, or even impossible in practice. For example, **many concerns** have been raised that de facto localization will be the outcome of the European Union's General Data Protection Regulation (GDPR), in accordance with the ruling by the **Court of Justice** of the European Union in the Schrems II case—even though the GDPR does not have explicit data localization clauses.

THE VARYING MODELS OF DATA LOCALIZATION

Data localization mandates vary greatly from country to country, depending on the intent of the governing body adopting them. They are increasingly incorporated into digital governance frameworks by autocratic and democratic governments alike. Democratic governments have argued both for and against such policies as policymakers seek to balance the business, human rights, and data privacy concerns of stakeholder communities. More authoritarian governments (and some democracies) officially cite security priorities such as counterterrorism and curtailing foreign influence as reasons to tighten control of their national digital infrastructure, ultimately enabling increased surveillance and censorship of their populations. The result is a global data governance landscape that restricts the free flow of data across some borders but not others, sets uneven data handling and storage requirements based on origin, and contributes to increased internet fragmentation.

The following sections present the major actors and influencers of data localization policy.

THE UNITED STATES AND EUROPEAN UNION

The United States currently enacts policies and signals its stance on data localization through international governance bodies and bilateral and multilateral trade agreements. The **United States-Mexico-Canada Agreement**, which entered into force in July 2020 and replaced the North American Free Trade Agreement, **prohibits data localization and formalizes the free flow of data** between the member nations. As presented in a 2021 CSIS **study** focusing on the Asia-Pacific region, the multiple trade agreements between democratic nations in the region prohibit both data localization requirements and cross-border data flow restrictions.

The result is a global data governance landscape that restricts the free flow of data across some borders but not others, sets uneven data handling and storage requirements based on origin, and contributes to increased internet fragmentation.

However, the transatlantic data flows between the United States and European Union, at least with respect to personal data, remain in question since the **Schrems II case**. In July 2020, the Court of Justice of the European Union invalidated the European Commission's adequacy decision regarding the United States—striking down the U.S. Privacy Shield, a framework for U.S.-EU data transfer, based on concerns that U.S. surveillance authorities do not provide adequate privacy protections for EU internet users. Since this ruling, negotiations to replace the Privacy Shield with a new data transfer agreement have been ongoing. While some scholars **argue** that data localization would not sufficiently address the underlying privacy and security concerns at the heart of the case, the Schrems II judgment may pave the way

for a hard localization outcome by suspending personal data transfers if the United States and European Union fail to resolve the dispute—which would also result in the suspension of personal data transfers to third-party countries that do not have adequate privacy and personal data protections with respect to EU data regulations.

THE BRICS EMERGING MARKETS

All five emerging markets informally referred to as BRICS (Brazil, Russia, India, China, and South Africa) have implemented or are in the process of implementing data localization mandates.

Brazil's data privacy and protection legislation, the General Personal Data Protection Law (Lei Geral de Proteção de Dados Pessoais, or LGPD), entered into force in February 2020. Like the European Union's GDPR, the **LGPD** enumerates the rights of individuals regarding their data and outlines how certain types of data may be used by companies and other third parties. After considering a **data localization provision** in its so-called "fake news" bill, Brazil also introduced a data localization amendment to the LGPD that, if enacted, would mandate that Brazilians' personal data be **"physically stored and maintained"** within Brazilian borders.

While Russia has been aggressively asserting control over its internet architecture—cracking down on **social media companies** that do business in Russia without a physical presence and voicing increasing concerns with data flows out of the country—its approaches to data localization have primarily focused on implementing **data mirroring policies**. Data may be transferred and processed outside Russia but must be physically stored in databases within the nation's borders. The **mandates apply to Russia-based entities** and to foreign companies that have Russian website domain names, use the Russian language on their website, or conduct business in Russia and deliver goods for payment in rubles.

India implements various data localization approaches through the current draft Personal Data Protection Bill and previous regulation on payments data. The Personal Data Privacy Bill requires soft localization for sensitive personal data, allowing for the transfer of some personal data should GDPR-like conditions be met; hard localization for "critical personal data," which may only be processed in India and may not be transferred out of the country; and hybrid localization for payments data. Notably, the draft bill provides **exemptions for government data collection** that undermines the spirit of the law to codify citizens' right to privacy.

Often contrasted with the European Union—whose approach to data privacy through the GDPR is called the "**Brussels Effect**"—China offers a different model of data governance and regulation known as the "**Beijing Effect.**" Chinese law requires that various forms of data, including **"personal information and important data,"** be stored in China and undergo a government security review before transfer out of the country, if deemed necessary. These data localization mandates, along with other Chinese regulations regarding internet content and access, have **severely restricted most foreign technology companies—with several notable exceptions**—to the point that many are unable or unwilling to continue operations within China. In the absence of foreign competition, domestic companies such as TikTok, DiDi, and WeChat have flourished while complying with China's hard localization requirements.

Finally, South Africa has taken steps to implement a GDPR-like data governance framework as well as separate legislation with explicit data localization requirements. Though South Africa's **Protection of Personal Information Act** (POPIA) does not contain explicit data localization mandates, it does introduce increased preconditions for cross-border data transfers. In addition to POPIA, South Africa introduced the **National Data and Cloud Policy**, which includes requirements to store and process data considered "critical information infrastructure" within the country's borders and to mirror data generated from South African natural resources.

INTERNATIONAL BODIES

Various formal governance bodies and informal groups of like-minded nations are working to reduce barriers to data flows, pushing back against the trend toward localization. The argument against data localization mandates is often referred to as "data free flow with trust," as coined by the Group of 20 (G20) **Osaka Leaders' Declaration** in 2019. The communique acknowledges that the "cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development, while raising challenges related to privacy, data protection, intellectual property rights, and security." Though G20 leaders supported this concept, the declaration did not have much initial success in establishing global data flow standards and norms.

The issue of maintaining an internet free of restrictive data localization mandates was addressed in a **digital and**

tech ministerial meeting in April ahead of the June 2021 Group of Seven (G7) Leaders' Summit. The **declaration** signed at this meeting puts forward new proposals intended to help guide continued development of "an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people." It calls for developing digital technical standards to which online services and protocols can refer and highlights the G7's intent to seize the benefits of "data free flow with trust" through continued surveillance of the effects of data localization, promotion of regulatory cooperation, and including more priority areas within current data-sharing approaches.

Within the World Trade Organization (WTO), members have engaged in conversations on the importance of standards setting and rule negotiations regarding data localization, as well as on how it affects international business and trade. In May 2021 e-commerce **negotiations**, WTO members emphasized the need to establish clear guidelines on data localization mandates and to create provisions that promote digital inclusion and facilitate trade. At previous **plenary** meetings, members have continually highlighted that supporting and enabling free flow of **data** across borders are integral to continued digital innovation and international cooperation.

Finally, the Organization for Economic Cooperation and Development (OECD) has focused on refining interdisciplinary, international standards on **data governance** and reducing barriers to data flows. A two-year horizontal project planned for 2021–22 seeks to advance a multifaceted approach to **build trust and minimize barriers to data flows**. The OECD project is centered around four categories it sees as integral to constructing global consensus on data governance: access, control, and data sharing; cross-border data flows; data's impact on business models, market dynamics, and market structure; and the measurement and classification of data.

HOW DATA LOCALIZATION CONCERNS NATIONAL SECURITY

Data localization puts at risk the global interconnectedness that has been the foundation of post–World War II **peace and alliances** and **has been associated** with a related overall decline in internet freedom. It has been used to target minority communities, activists, and journalists, often under the false pretense of protecting them. The **resilience** of democratic actors to authoritarian targeting is crucial; without it, countries that are increasing controls on their citizens, expanding their reach abroad, and exporting the tools and tactics of **digital authoritarianism** today could become the U.S. **national security** concerns of tomorrow.

The real national security concerns over data localization are often overshadowed by both manipulative interpretations of "national security" in support of more localization (as discussed below) and by economic and commercial arguments against it. These latter arguments abound, especially from those who believe that a free, open, secure, and reliable internet is a critical component of global trade and prosperity. Though many of the individuals and organizations making such arguments are in the United States, the pre-Brexit UK government **warned** in 2017 that such "Balkanization of the internet risks stifling the competition, innovation and trade which produce better services for consumers, and can weaken data security." Regarding the information and communications technology (ICT) sector, evidence suggests that data localization increases prices and "**[limits the] availability** of ICT products and services while creating few data center jobs." Despite **economic protectionist** arguments that cross-border data flows could make local internet-based businesses less competitive, there is **limited evidence** to suggest that data localization drives local economic development, online or off. Efforts to erect barriers might provide short-term commercial benefits to newly advantaged domestic firms, though potentially at the expense of innovation and the broader, long-lasting global economic growth spurred by the advent of the internet.

Despite these economic arguments against, the dominant global trend is toward more localization of data, leaving private-sector tech firms with **difficult choices**. Some multinational corporations **have chosen** to leave certain markets rather than comply with restrictive data localization mandates, **while others** have chosen to remain and adapt. Driving this trend are, in large part, governments making decisions based on their own interpretations of "national security."

THE NATIONAL SECURITY CASE FOR LOCALIZING DATA

There is a case to be made that the free flow of data to hostile or authoritarian regimes threatens the national security of their geopolitical adversaries. For example,

South Korea does not want data on its citizens and corporations to be accessible by North Korea. **India** and the **United States** have valid concerns about Chinese-owned companies—and, by extension, the Chinese Communist Party (CCP)—having access to their citizens' data. Further, there are legitimate reasons why law enforcement agencies, for example, would desire both access to data and to restrict the ability of malign actors to share data across international borders. While a **communiqué** by G20 finance ministers ahead of the aforementioned Osaka Leaders' Declaration mentions the benefits and challenges of data flows, the challenges are not clearly defined, and the language clearly attempts to give G20 member countries—which **represent** more than 80 percent of the world's GDP and 60 percent of its population—leeway to impose data localization requirements as they see fit.

For G20 member countries such as China, India, Indonesia, Russia, and Turkey, the lack of an agreed-upon definition of data localization-related national security concerns provides an opportunity to argue for stronger data localization mandates. Some of these justifications lack evidence; others strain credulity. The government must control data, the argument goes, to protect its citizens' privacy from external actors, despite there being no guarantee that data localization protects personal privacy any more than current cross-border flows do. In fact, data localization may undermine privacy by placing user data firmly within reach of governments or because of the deleterious effects data localization requirements have on cybersecurity. Beyond privacy, the most common excuse used to promote data localization is a nebulous and broadly defined version of "national security," even though control over data flows **has enabled** governments to assert control over citizens more than it has addressed legitimate cybersecurity and other traditional national security concerns. In other words, control over data flows is often not actually about national security; it is about control.

The lack of an agreed-upon definition of data localization-related national security concerns provides an opportunity to argue for stronger data localization mandates.

THE NATIONAL SECURITY CASE AGAINST LOCALIZING DATA

Data localization—and the resulting fracturing of the internet—does have national security implications. These can be placed into three broad categories, which collectively constitute arguments against localizing data: (1) authoritarian threats to democracy, (2) limits on security actors' collaboration and capabilities, and (3) cybersecurity threats.

1. **Data localization can be used as a tool of digital authoritarianism to limit democracy and human rights**. A recent **CSIS policy brief** defined digital authoritarianism as "the use of the internet and related digital technologies by leaders with authoritarian tendencies to decrease trust in public institutions, increase social and political control, and/or undermine civil liberties." The brief also points out that "human rights and civil liberties are at risk, including freedom of movement, the right to speak freely and express political dissent, and the right to personal privacy, online and off. Digital authoritarianism co-opts and corrupts the foundational principles of democratic and open societies; its goal is not just to break them down, but to redefine and reshape them in their authoritarian image."

Data localization territorializes data so that domestic governments can assert jurisdiction over it and, by extension, service providers. This is intended to facilitate these governments' ability to carry out a "**crackdown** on free expression, privacy, and a range of human rights," especially in jurisdictions with authoritarian governments or weak democracies. Often, these data localization mandates are put forth under the guise of "protecting" individuals' privacy or security, but the result is often the exact opposite. When citizen data—from Google Maps searches to Instagram likes to TikTok posts—is forced to be stored on local servers, governments have greater opportunities to use these data to gain greater control over the population. From Bangladesh to China to Russia and beyond, this manipulation enhances and strengthens the modern digital surveillance and censorship state.

It might make intuitive sense for a country to want to control "critical," "highly sensitive," or (as the Chinese government calls it) "important" data lest it fall into the hands of nefarious overseas actors. However, when the definitions of these terms are broadened and made more subjective over time, this increasing control has potentially negative effects on civil society, democracy, and human rights.

2. **Data localization can limit collaboration between**

military, law enforcement, intelligence, and other security actors by creating obstacles to accessing information across borders. It effectively provides a safe haven for actors who execute **gray zone** tactics, including information operations via social media and illicit financial activities, on platforms subject to localization requirements—limiting the ability of targeted countries to combat and investigate them and, if applicable, prosecute the perpetrators of related crimes.

Cross-border law enforcement cooperation is often governed through the mutual legal assistance treaty (MLAT) system, though many MLATs "**were drafted** prior to the Internet's widespread global adoption and therefore few of the treaties address core questions of data and jurisdiction" and "frequently do not specify what constitutes 'protected data.'" In practice, this means that even as requests for data through the MLAT system increase (one 2015 **estimate** by the U.S. Department of Justice indicated a 60 percent increase in "requests for assistance from foreign authorities" over the previous decade), the system cannot handle sharing the data necessary for today's law enforcement needs. If U.S. friends and allies adopt stricter data localization requirements, it could further complicate an already convoluted and outdated MLAT system, increasing barriers to law enforcement in the growing number of cases involving data that flowed across international borders. This would weaken current information-sharing channels and businesses' reporting obligations, thereby impacting intelligence-gathering methods and criminal investigations. These methods are deployed daily, whether in response to a natural disaster or a cyberattack on a critical supply chain.

Additionally, Americans abroad, including U.S. government officials, depend on secure telecommunications that become more complicated as data localization requirements harden. The accuracy and credibility of data funneled through local systems are necessarily questioned, especially in countries with adversarial relationships with the United States. It can also further culturally isolate nations from one another, making diplomacy and peacebuilding efforts more difficult. Most specifically, if certain forms of data localization (such as hard or hybrid) are widely adopted, they could impede research into terrorist organizations' funding structures, compromise informants, and weaken traditional U.S. intelligence-gathering networks.

3. **Data localization mandates introduce risk and complexity to companies' cybersecurity operations by increasing the number and locations of data centers that must be staffed and maintained**. While policymakers and businesses continue to define the division of roles and responsibilities between the public and private sectors to secure companies' data and infrastructure in cyberspace, the consensus is that cybersecurity writ large is a **national security issue** that will have increasingly dire consequences the longer it goes unaddressed.

Instead of allowing companies to store data in a few data centers globally, each nation that requires storage in-country ultimately requires applicable entities to have a physical server footprint in that country in order to comply. This organizational footprint includes physical facilities, hardware and software infrastructure, and employees. **Analysis** from the financial sector suggests that data localization could "increase IT [information technology] and data complexity; undermine the risk management, cyber security and anti–money laundering practices of financial institutions; as well as reducing access to financial services and markets in some countries." In addition to the increased costs associated with running facilities, entities must have **reliable infrastructure** to support their operations, which may not be guaranteed, depending on the location. The increased footprint creates new avenues of attack—both through hardware and software entryways into data systems and the number of workers who are vulnerable to phishing or other targeted methods of exploit.

Data localization mandates may also dictate how data and internet traffic are routed within a company and between companies and governments. This requires each data center to maintain up-to-date processes and procedures on how information is transferred, creating specialized and prescriptive mechanisms for the variety of country-to-country data transfers they must be able to facilitate. Companies are thus required to balance data loads across increasingly remote locations while complying with a complex web of inconsistent local regulations. The result is more complex technical systems, which often are less secure.

LOOKING AHEAD, BIG QUESTIONS REMAIN

This policy brief presents the state of data localization and makes national security arguments the authors feel should be included in more frequent, related debates. While the final section recommends a way forward, this

policy brief does not provide clean solutions, in part because of the following big, unanswered questions.

Will people trust the internet? In a future defined by continued debate over the use of personal data and uneven global implementation of data localization mandates, people will want to know whether they can safely use online products and, if so, how to do so. Democratic societies will want to know how data localization mandates will impact core values of privacy and freedom of expression, particularly when their citizens are traveling abroad. National security actors in these countries will need to adapt to new operational realities and authoritarians' increasingly sophisticated digital surveillance tools. If not, over time, internet users everywhere may increasingly question whether their online presence and personal data are secured by trustworthy actors.

Will the United States get in the game? To date, the United States government has largely watched from afar as the European Union, CCP, and other government actors present competing models of data governance to developing countries as they fight for influence there. It lacks federal-level privacy and data governance policies or a formal strategy to guide policy development and implementation. Even though many of the companies most affected by these competing governance models are headquartered in the United States, no GDPR-like federal privacy or data governance law exists, and few people, organizations, or government entities are actively working on these issues. The resulting lack of a coherent approach to counter the proliferation of data localization requirements gives rise to significant commercial and national security-related challenges. Developing and aligning behind such a unified approach will be easier said than done: U.S. credibility as a messenger for a free, open, secure, and reliable internet is not what it was in the 1990s, having been damaged by, for example, the Trump administration's now-abandoned efforts to ban **TikTok and WeChat** in 2020.

How will the United States and its friends and allies address a key paradox? The national security cases for and against data localization present a paradox that intertwines data privacy, rule of law, commitment to a level economic playing field, and geopolitical competition. Fears of a company sharing user data with a geopolitical rival seem to justify data localization efforts, as does reciprocity for stringent mandates imposed on U.S.-based companies operating in places like China. Nonetheless, attempts to prohibit companies (such as TikTok) based in those rival countries from controlling user data provide **useful fodder** for other governments to pursue stronger data localization policies.

Where and how will the Brussels-Beijing competition play out, especially with the United States on the sidelines? If the United States does not cooperate with like-minded friends and allies to produce a coherent strategy, the European Union and China will continue to compete for influence in non-aligned parts of the world. Whether via the **Beijing** or **Brussels** effects, the prevailing approaches to transnational data governance rely heavily on narrow privacy arguments that lack a clear, holistic understanding of the impact a more fractured internet will have on freedom, commerce, and national security. A more fragmented internet will create **separate silos** wherein open and secure communication becomes more challenging. Both policymakers and experts are increasingly concerned that the vague U.S. stance on data flow restrictions will heighten privacy fears and contribute to continued adoption of these mandates in other nations.

Will a firm U.S. stance against localization matter? Though this policy brief makes a case for the United States to develop a stance based in part on the real national security concerns presented by data localization mandates, such a stance might not be enough to persuade other democracies—let alone authoritarian-leaning countries—not to implement data localization restrictions. Authoritarian and democratic countries alike are moving forward with policies that will further fragment the internet. The United States alone is unlikely to affect data localization; however, it can make a positive difference if it reconciles and coordinates efforts with like-minded friends and allies. If the United States wants to protect its national security and economic interests, this is the way forward.

The United States alone is unlikely to affect data localization; however, it can make a positive difference if it reconciles and coordinates efforts with like-minded friends and allies.

THE WAY FORWARD

To date, the United States has largely been absent from global debates around data governance, which increasingly includes various data localization mandates. Relatedly, there has been little to no debate in the United States about the real national security challenges of data localization and what a viable, alternative model of data governance could look like. This is where a cohesive digital strategy that forms the foundation for a principles-based and consistent approach with like-minded friends and allies will be important.

Such an approach should:

(1) Start at home with the development of a strong, principles-based U.S. position on data localization. More specifically, the United States should:

- Commission full studies on the various national security implications of data localization and how the relevant parts of the U.S. government should approach them. This policy brief presents a possible foundation for such studies but does not adequately address implications at the department and agency level.
- Aggregate and summarize the various commissioned studies into concise principles that present internet fragmentation as a phenomenon with direct impacts on U.S. national security.
- Determine and document instances where it might be appropriate to control or limit cross-border data flows—especially on issues of real national security—and how to navigate the accompanying commercial concerns. When data localization is deemed to be in the national interest, relevant mandates should be specific and avoid broad generalizations that can become slippery slopes. Absent such a "**specific and compelling reason**," the U.S. government and like-minded friends and allies should avoid mandates that limit cross-border data flows.
- Consider domestic privacy or data-governance legislation that includes data localization principles and proposes updates to the MLAT system used for law enforcement purposes. Write bills to leverage existing legislation and facilitate cooperation with like-minded friends and allies and encourage emulation in the developing world. Work closely with representatives from civil society, industry, and national security groups to develop language that adequately addresses national security interests while limiting the impact of data localization mandates on democracy, human rights, and economic growth.
- Incorporate lessons from this policy brief and other data-localization–related studies into any future U.S. government **democracy** and **digital** strategies, which should showcase a deep understanding of how data localization—and the tools of **digital authoritarianism** writ large—are being used by authoritarians to **limit democratic freedoms**. Strategies should specifically include ways to guard against and counter misleading national security excuses for data localization mandates and account for potential first- and second-order impacts on the cyber offense-defense balance.

(2) Promote a shared model and consistent approach to data localization with like-minded friends and allies.

- Promote the findings of the aforementioned studies, relevant legislation texts, and associated strategies across the multilateral system, including but not limited to the WTO, the OECD, and the G7 and G20 processes. Plug into, learn from, build on, and (where appropriate) lead existing bilateral, regional, and multilateral efforts, which are the primary venues through which data localization issues are being addressed. As highlighted in a recent **policy brief** by the CSIS Economics Program, relevant efforts include the Asia-Pacific Economic Cooperation forum's **Cross-Border Privacy Rules**, the **U.S.-Japan Digital Trade Agreement**, the **Australia-Singapore Digital Economy Agreement**, and the **Digital Economy Partnership Agreement** launched by Singapore, New Zealand, and Chile.
- Focus U.S. bilateral assistance and multilateral efforts on **increasing data literacy** across the developing world, which is often overlooked in the current debates over data governance even though this is where geopolitical rivals are competing in real time for influence and access to markets.
- Develop a strong, principles-based, and sufficiently detailed narrative across these agreements and within the multilateral system around the real national security implications of data localization mandates. Present principles as counters and affirmative alternatives to digital authoritarianism. Leave little room for interpretation and misappropriation of the term "national security" in the context of data localization.
- Reaffirm and regularly reference the June 2021 Carbis Bay **G7 summit communiqué,** which committed "to preserve an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom,

innovation and trust which empowers people" and specifically expressed "opposition to measures which may undermine these democratic values, such as government-imposed internet shutdowns and network restrictions." Highlight that India and South Africa, two countries mentioned several times in this policy brief, participated in the June 2021 G7 meetings and signed an "**Open Societies Statement,**" which called out "online harms and cyber attacks" and criticized "politically motivated internet shutdowns." Use the agreed-upon language in this statement as an opening to push for reform in those two and other countries with increasingly rigid data localization mandates. ■

Lindsey R. Sheppard *is a fellow with the International Security Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***Erol Yayboke*** *is a senior fellow with the CSIS International Security Program and director of the Project on Fragility and Mobility.* ***Carolina G. Ramos*** *is a research associate with the CSIS International Security Program.*

CSIS receives support from Facebook for its work on data localization and national security.