Sovereignty and Data Localization

Emily Wu
Sovereignty and Data Localization

Emily Wu
# Table of Contents

**Executive Summary** .................................................................................................................. 1

**Introduction** .......................................................................................................................... 3

**Data sovereignty and its importance in the emerging technology landscape** ........................................... 5
   - Spotlight: Cloud computing ........................................................................................................ 6
   - Spotlight: 5G telecommunications .......................................................................................... 7
   - Spotlight: Artificial Intelligence .............................................................................................. 8

**Data localization is used to assert data sovereignty** ................................................................. 9

**Types of Data Localization Policies** .................................................................................... 11
   - Local-only storing, transmission, and processing .................................................................. 11
   - Local copy required .................................................................................................................. 12
   - Narrower, conditional restrictions ......................................................................................... 13

**Reasons for Data Localization Policies** ............................................................................... 14
   - Technical concerns .................................................................................................................. 14
   - Value concerns ........................................................................................................................ 17

**How should policy makers respond?** .................................................................................. 19

**Conclusion** ........................................................................................................................... 22

**Bibliography** ......................................................................................................................... 23
Executive Summary

Data localization policies impose obligations on businesses to store and process data locally, rather than in servers located overseas. The adoption of data localization laws has been increasing, driven by the fear that a nation’s sovereignty will be threatened by their inability to exert full control over data stored outside their borders. This is particularly relevant to the US given its dominance in many areas of the digital ecosystem including artificial intelligence and cloud computing.

Unfortunately, data localization policies are causing more harm than good. They are ineffective at improving security, do little to simplify the regulatory landscape, and are causing economic harms to the markets where they are imposed. In order to move away from these policies, the fear of sovereignty dilution must be addressed by alternative means. This will be achieved most effectively by focusing on both technical concerns and value concerns.

To address technical concerns, the US should:

1. **Enact a federal national privacy law** to reduce the fears that foreign nations have about the power of US tech companies.

2. **Mandate privacy and security frameworks by industry** to demonstrate the importance that US industry places on privacy and security, recognizing it as fundamental to their business success.

3. **Increase investment in cybersecurity** to ensure that in a competitive market, the US has the best offering in both customer experience and security assurance.

4. **Expand multi-lateral agreements under CLOUD Act** to help alleviate the concerns that data stored by US companies will be inaccessible to foreign governments in relevant to a criminal investigation.
To address value concern:

5. **Take a collaborative approach to technology innovation with key allies**, working together to facilitate technology development in a way that is safe, effective and in line with liberal and democratic values.

6. **Develop norms and standards around data use in collaboration with allies**, particularly as they relate to privacy, security, the rule of law and human rights.¹

7. **Make public and explicit commitments to criticize neocolonialism with respect to data** to give developing countries, or those with less technological capabilities, confidence that the US does not condone data exploitation.

¹ Lawrence and Cordey, “The Case for Increased Transatlantic Cooperation on Artificial Intelligence.”
Introduction

Artificial intelligence, advanced analytics, cloud computing, the Internet of Things are examples of emerging technologies that rely on or produce data. Whether used for national security, business growth, fraud detection, or scientific discovery, the way data is collected, stored, used, and transferred can have a material impact on national security, industry growth, geopolitical relationships and civil society. Access to data that is safe, secure, and stored in a way that gives customers comfort and protection is a desire that stakeholders across this landscape share. This shared interest is motivating nations to implement data protection laws that try to balance security and domestic control with economic innovation and globalization.

A category of such laws focuses on data localization. In general, these laws require data to be stored and processed domestically, with the ultimate aim of enhancing sovereign control over citizens’ data. These laws are primarily driven by concerns about foreign government interference, so their central objective is to curb foreign governments’ access rights to data stored outside of their jurisdiction. As these new data-dependent technologies emerge, and our dependence on them in everyday life grows, fear of foreign governments accessing personal data (by request or by force) has deepened. Fear of falling behind in technology development also drives these policies, with a secondary objective being to make it more difficult for foreign companies to operate in domestic markets.

This paper will examine how data localization laws are used by governments to safeguard sovereignty and preserve their ability to oversee how citizens’ and inhabitants’ data is used. Unfortunately, rather than making data more secure, data localization laws have handicapped innovation, increased regulatory complexity, and perhaps even threatened security. Further, the US CLOUD Act has clarified that US tech companies are subject to US laws no matter where in the world they are operating, or whose data they are storing. This means, for example, a US company storing EU data on EU soil would still be subject to access requests from the US Government. This substantially reduces the efficacy of data localization laws as a mechanism to protect data stored by US companies from US law
enforcement agencies because these companies remain within the jurisdiction of US law enforcement no matter where their servers may be located.

In light of these limitations, a new data governance approach for policymakers that balances the desire for sovereignty with the need for global and cross-sectoral cooperation is proposed in this paper. The importance of national laws that demonstrate the US’ commitment to data privacy and security will be essential for maintaining and/or restoring trust and confidence that foreign nations have in doing business with the US. They will also help clarify the confusions that ultimately end up being costly for companies to overcome. As such, the focus of the paper will be primarily on the US but will draw on global experiences to illustrate concepts as needed.

There are two critical elements to the CLOUD Act:

1. The CLOUD Act clarifies that service providers are required to disclose all data in their possession, custody, or control, pursuant to lawful process, regardless of the location of the data. The Act amended the federal Stored Communications Act, to state that a criminal warrant served on a U.S.-based provider extended to all e-mails in scope regardless of where in the world the e-mails were located.

2. The CLOUD Act also makes it easier for foreign governments to request access to data stored by companies in the US. Previously, these requests were made through the Justice Department and required a warrant. Under the new legislation, foreign countries can request the data directly from the tech company, using a lower legal threshold than the probable-cause standard required for a warrant.

---

2 Review, “Microsoft Ireland”, the CLOUD Act, and International Lawmaking 2.0.”
3 “US CLOUD Act and International Privacy.”
4 Ford, “Should Foreign Countries Be Allowed to Snoop on Data on American Soil?”
Data sovereignty and its importance in the emerging technology landscape

Given the vast amounts of data that emerging technologies both use and produce, exploring the way that nation states assert control over data on behalf of their citizens and inhabitants is increasingly necessary for innovation and national security alike. Known as data sovereignty, control over data is often claimed through assertions of geopolitical power, international agreements about sovereignty recognition, and domestic policy creation.

While the US is already in a strong position to claim such sovereignty based on its position as a geopolitical leader, foreign nations—both allies and adversaries—are anxious that the US’ (and China’s) dominance in emerging technologies will be a threat to their own assertion of data sovereignty. Digital dominance is increasingly becoming synonymous with economic dominance, and such dominance comes with the power to infringe on the sovereignty of others. Further, concerns about a growing sense of ‘neocolonial’ dependence on multinational tech companies is a motivating force behind much of the proliferation of new data protection and privacy policies globally.

An example of this colonialism threat is the introduction of Facebook Free Basics. This is a limited internet service that Facebook offers for free that serves the purposes of getting new consumers online and eventually reliant on the internet. It also facilitates the collection of vast amounts of data on users, which can ultimately be used to ‘feed’ AI technology. Ellery Biddle, an advocacy director of Global Voices said “Facebook is not introducing people to open internet where you can learn, create and build things… it’s building this little web that turns the user into a mostly passive consumer of mostly western corporate content. That’s digital colonialism.”

5 Torreblanca, “Europe’s Digital Sovereignty.”
6 “It’s Digital Colonialism.”
Importantly, it is not just developing markets that fear foreign digital dominance. The EU’s introduction of the General Data Protection Regulation (GDPR) is a clear example of a highly tech capable economy seeking to assert sovereignty and regain some digital independence. In an open letter to the President of the European Commission, Heads of Government from Germany, Denmark, Finland and Estonia wrote: “the dependencies and shortcomings in European digital capacities, skills, and technologies have become more apparent. A significant amount of digital value-added and innovation takes place outside Europe. Data has become a new currency that is mainly collected and stored outside Europe. And fundamental democratic values are under severe pressure in the global digital sphere. Now is the time for Europe to be digitally sovereign.”

To better understand the fears motivating assertions of sovereignty (often in direct opposition to both US tech companies and the regulatory authorities these companies are subject to), it is useful to consider the ways in which a few key emerging technologies use, store, create or relate to data.

**Spotlight: Cloud computing**

Behind the many promises of emerging technologies there is a growing need for data storage and processing which is increasingly being offered through cloud computing. Cloud computing services are highly efficient, easily scalable, and extremely flexible. They offer services to customers ranging in size from governments to multinational companies to start-ups, with a pay-for-what-you-use model that makes the technology highly accessible.

Sovereignty has traditionally meant control within geographical borders, but services like cloud computing are often delivered most efficiently (from a cost perspective) when data is free to flow between national borders. For public sector agencies in particular, the risk that data stored offshore could be accessed by foreign governments is a front-of-mind threat to their security. In order to assert and/or reclaim sovereignty, policies that restrict the business operations of data storage and processing companies are becoming very popular.

---

7 Merkel et al., “Letter to COM President on Digital Sovereignty.”
Spotlight: 5G telecommunications

5G is the fifth generation of wireless network technology and operates largely in the cloud. It allows for the delivery of internet-based services at faster speeds, lower latency, and more capacity. The speed of internet delivery is particularly important for devices and technologies that rely on real-time data e.g., location-based services such as driverless cars.

US Internet and telecommunications companies are already heavily invested in building out their 5G networks, motivated in large part to not lose the ‘arms race’ against China. Unlike other emerging technologies where the US is the clear leader (or at least has comparable market power to China), China is dominant in the 5G market. 5G has been a critical part of China’s Digital Silk Road initiative, which is focused on provision of communications technology and systems to the developing world. Asia and Africa are expected to account for 90% of the world’s population by 2050, and if China leads in the provision of essential technology services on these continents, then China is in the best position to dominant the digital ecosystem.

This threat of dominance is the main force behind the US rejection of Huawei and ZTE, who together account for ~40% of global 5G infrastructure. US intelligence agencies say equipment made by Chinese telecom companies are a national security threat; if China controls the infrastructure, the Chinese government will have access to data that traverses that infrastructure. The US policy response has been to invest in domestically owned infrastructure, reject Chinese suppliers, and encourage allies to do the same.

---

8 “Cloud Computing and 5G.”
9 “Competing with China’s Digital Silk Road.”
10 “68% of the World Population Projected to Live in Urban Areas by 2050, Says UN | UN DESA | United Nations Department of Economic and Social Affairs.”
11 Benner, “China’s Dominance of 5G Networks Puts U.S. Economic Future at Stake, Barr Warns.”
Spotlight: Artificial Intelligence

Advanced, accurate, and socially responsive AI technology relies on high-quality, diverse and readily accessible datasets. Because AI ‘learns’ from data, the wider and more diverse that data is, the more readily applicable the AI technology can be to our diverse world. If we feed AI data on just one community or one context, that AI technology will develop bias. Because AI is already permeating many aspects of our daily lives, there is a pressing need for AI developers to have access to high quality ‘training data’ that will enable the technology to obtain the necessary level of intelligence needed for real world application.

Unfortunately, foreign nations are concerned about the relative strength of the US’ position on AI development, and a bias towards data nationalism is developing as a result. There are growing concerns that AI dominant countries will use data for only their advantage with little or no input from the nations and peoples that the data is being sourced from. For some countries, this threat is a form of modern colonialism.

---

12 Lawrence and Cordey, “The Case for Increased Transatlantic Cooperation on Artificial Intelligence.”
Data localization is used to assert data sovereignty

An increasingly common way for a nation to assert data sovereignty, particularly if the country is not in a dominant position of geopolitical power, is to pass data localization measures. Generally, governments want to claim sovereignty over their citizens’ data no matter where or by whom it is stored. In the strictest sense, forced data localization means data created within State borders must stay within those borders.13

Domestic storage aims to increase control over citizen data by bringing decision making and access rights within jurisdictional boundaries. It also serves to put foreign companies at a disadvantage relative to domestic companies. It is generally a policy introduced at the government level that all organizations operating in that country must abide. Particularly in the course of criminal investigations or regulatory activity, access to this data can be important. Further, as citizens become increasingly engaged in both technology products and their policies, political commitment to personal privacy can be persuasive at the ballot box. If data isn’t stored or processed locally, there can be much confusion and concern about which sovereign nation’s laws should apply to that data in which circumstances. Data localization seeks to simplify this.

---

13 “Data Sovereignty vs Data Residency vs Data Localization.”
The increased number of data localization policies is a reflection of the fear that nations have of losing or diluting their data sovereignty.

Figure 1: Increase in data localization measures globally (1960 - 2015)

Source: ECIPE Digital Trade Estimates database\textsuperscript{14,15}

\textsuperscript{14} DeFilippo and Coleman, “Market Opportunities and Key Initiation Foreign Trade Restrictions.”

\textsuperscript{15} Data originally sourced from ECIPE Digital Trade Estimates database
Types of Data Localization Policies

Data localization policies tend to fall into three categories:

Local-only storing, transmission, and processing

This generally means an obligation to locally manage data or as a prohibition of international data transfers. This is the strictest type of localization policy and is more likely to be descriptive of nations seeking broader control over citizen activities.

Example: Russia

Under Russia’s Federal Law No. 242-FZ, operators must ensure the recording, systematization, accumulation, storage, adjustment (update, alteration), and retrieval of personal data of citizens of the Russian Federation will be performed through database serves located in the territory of the Russian Federation. Substantial fines are imposed on organizations and individuals that fail to comply with data localization requirements.

Example: China

Article 37 of the Cybersecurity Law of People’s Republic of China (‘CSL’) requires critical information infrastructure operators (‘CIIOs’) to store personal information and important data generated from critical information infrastructure in China. These requirements are likely to be expanded by the Personal Information Protection Law, the draft of which was released in October 2020.

---

17 “Russia Increases Fines for Violation of Its Data Localization Law.”
18 “Russian Data Localization Law.”
19 “China.” the Cyberspace Administration of China (‘CAC’)
20 “China Releases Draft Personal Information Protection Law - Privacy - China.”
Local copy required

companies are required to keep a copy of data in local servers or data centers. This allows for easier access to this data for regulation and law enforcement purposes. I.e., it is generally easier for local law enforcement agencies to access data stored locally than it is for them to access data stored in another jurisdiction.

Example: India

Under India’s Personal Data Protection Bill, sensitive personal data (which includes financial information) must be stored in India, but a copy of the data can be transferred internationally if certain requirements are met.21 These include:

- The data principal provides explicit consent, the transfer is made pursuant to a contract or intra-group scheme approved by the Data Protection Authority22
- The government has deemed a country to provide adequate protection23
- The Data Protection Authority has specifically authorized the transfer24

21 Wimmer, Maldoff, and Lee, “Indian Personal Data Protection Bill 2019 vs. GDPR.”
22 Wimmer, Maldoff, and Lee.
23 Wimmer, Maldoff, and Lee.
24 Wimmer, Maldoff, and Lee.
Narrower, conditional restrictions

Transfers of data outside the country are only permitted if certain conditions are met by the transferee and/or by the recipient country.25

Example: European Union

Under the EU’s GDPR, the transfer of personal data outside the European Economic Area is permitted only where:

• The recipient is in a territory considered by the European Commission to offer an adequate level of protection for personal data26

• Safeguards are in place such as binding corporate rules approved by Data Protection Authorities27

• A legal exemption applies, such as where data subjects provide explicit consent, the transfer is necessary to fulfil a contract or there is a public interest founded in EU or member state law28

Example: Brazil

Under the General Personal Data Protection Law (LGPD) international data transfers are only permitted in certain situations, including when recipient countries ensure an adequate level of data protection, when approved legal mechanisms (such as model contract clauses) are employed or when data subjects have provided their consent.29


26 Wimmer, Maldoff, and Lee, “Indian Personal Data Protection Bill 2019 vs. GDPR.”

27 Wimmer, Maldoff, and Lee.

28 Wimmer, Maldoff, and Lee.

Sovereignty and Data Localization

Reasons for Data Localization Policies

Reasons for data localization policies can be broadly split into two categories. The first is technical concerns, which relate to known risks and generally have a known solution set. The second is values concerns which are more ambiguous, complex and harder to define; the solution set is unknown but generally requires a change in attitudes, values or norms.

Technical concerns

When policy makers explain their motives behind data localization policies, they tend to focus on the technical concerns: improved security, protections for the domestic economy, simplification for local law enforcement agencies and reducing the risk of foreign interference. While the concerns may be legitimate, data localization as a mechanism for addressing them is ineffective for the following reasons:

- **Local data storage does not improve data security**: Full control of the physical stack no longer provides the security assurance it once did. Storage in the cloud has actually improved security because information is typically distributed among multiple systems rather than stored in a single location, not to mention the significant investments that these companies make in their cybersecurity capabilities. When it comes to data security, investment in infrastructure and maintenance is more critical than the physical location of data.

- **Local data storage does not necessarily mean improvements for the domestic economy**: In theory, if companies are required to locally store and process data, they will have to invest in local servers and data centers which would generate economic activity.

---

30 AWS, “Data Residency - AWS Policy Perspectives.”
31 Cory, “The False Appeal of Data Nationalism.”
32 Cory.
and employment opportunities.\textsuperscript{33} Like economic nationalism, data nationalism can actually stifle innovation and harm growth.\textsuperscript{34} Requiring data to be stored within the borders of the country in which it is collected can hurt local economies by increasing prices and limiting availability of ICT products and services.\textsuperscript{35} A report by the Leviathan Security Group estimates that efficiency losses from data localization measures can increase the costs of data hosting by 30-60\%.\textsuperscript{36} This raises the barriers for market entry, which suppresses entrepreneurial activity and reduces the ability for an economy to compete globally.

Further, a smaller local provider may actually be at increased threat of security breach given their relatively smaller capabilities to protect against malicious actors. As an alternative to cloud storage, businesses may opt for hardware storage which is also more costly and less secure.\textsuperscript{37} For example, Mastercard spent $350M of its $1B investment in India on localization compliance.\textsuperscript{38} In some cases, the cost of compliance is too great, leading large multinational firms to exit a market which is ultimately detrimental to users. For example, PayPal suspended its Turkish operations in response to a requirement that PayPal fully localize its information systems within Turkey.\textsuperscript{39}

- **Local data storage is not the only way to ensure access for local law enforcement or regulatory supervision:** When information relevant to a legal investigation is located offshore, governments fear their capacity to access this data may be restricted by the territorial limit of their powers.\textsuperscript{40} However contractual access through multilateral and bilateral agreements is also an effective way to ensure regulators can perform their roles.\textsuperscript{41}

\begin{itemize}
  \item \textsuperscript{33} "Data Flows across Borders: Overcoming Data Localization Restrictions."
  \item \textsuperscript{34} Castro, "The False Promise of Data Nationalism."
  \item \textsuperscript{35} Wallace, "Double Consent'
  \item \textsuperscript{36} "Quantifying the Cost of Forced Localization."
  \item \textsuperscript{37} "The High Costs of Storing Data Locally in a Cloud Native Era | TechRadar."
  \item \textsuperscript{38} Prasad, "Mastercard Begins Deleting Indian Transactions Data Stored Overseas."
  \item \textsuperscript{39} DeFilippo and Coleman, "Market Opportunities and Key Initiation Foreign Trade Restrictions."
  \item \textsuperscript{40} "Data Flows across Borders: Overcoming Data Localization Restrictions."
  \item \textsuperscript{41} "Financial Data Localization: Conflicts and Consequences."\
\end{itemize}
With respect to the US, the CLOUD Act attempts to make it easier for foreign governments to request access to their own citizens’ data stored by companies in the US by authorizing “the United States to enter into executive agreements with other countries that meet certain criteria, such as respect for the rule of law, to address the conflict-of-law problem. For investigations of serious crime, CLOUD agreements can be used to remove restrictions under each country’s laws so that cloud service providers can comply with qualifying, lawful orders for electronic data issued by the other country.”42 Previously, these requests were made through the Justice Department and required a warrant. Under the new legislation, foreign countries can request the data directly from the tech company, using a lower legal threshold than the probable-cause standard required for a warrant.43

- **Local data storage does not remove the risk of foreign government access requests:** The US CLOUD Act clarifies that “cloud service providers subject to U.S. jurisdiction must disclose data that is responsive to valid U.S. legal process, regardless of where the company stores the data.”44 This means the reach of the US Government extends beyond its borders; a US company is not immune to an access request simply by virtue of locating the data in a different jurisdiction making localization laws ineffective against US law enforcement.

In addition to being ineffective at addressing the aforementioned risks, the cost of localization policies can be hugely detrimental to the global economy. Cross-border data flows added some US $2.8 trillion to world GDP in 2014, surpassing the impact of the global goods trade.45 Digitization of trade and commerce has allowed businesses to connect with customers and suppliers throughout the world, which increases access and decreases costs. Globalization was once reserved for large companies, but global data flows

---

43 Ford, “Should Foreign Countries Be Allowed to Snoop on Data on American Soil?”
have reduced the scale that is needed to go global. In a 2016 worldwide survey conducted by McKinsey, 86% of survey respondents pointed to at least one cross-border activity. 46

Value concerns

While the technical concerns outlined above are relatively easy to discharge, another set of concerns based on values, fears, and emotions exist. Value concerns are harder to articulate and harder to address, so they are often cited as the reason for data localization. Some examples of value concerns include:

- **Fear of dependence:** Emerging data-driven technologies are already defining global markets and geopolitical power. Because this technology is dominated by the US and China, nations around the world fear that their sovereignty (i.e., their ability to govern by their own rules and values) will be hamstrung by their reliance on these players. The idea of “neocolonialism” is pertinent, as nations fear that by controlling access to technology, the US /China will have the power to control other key aspects of domestic life (such as the economy and even politics).

- **Mistrust in foreign governments:** Access by foreign governments is a known technical risk that US business and government representatives spend enormous amounts of time and energy trying to address. But the issue runs deeper than technical risks, evidenced by the ineffectiveness of industry assurances about data protection and privacy. Particularly in light of the clarifications made in the US CLOUD Act (that US companies are not immune to access requests even if data is located in another jurisdiction), and with the unauthorized disclosure of classified information by Edward Snowden still fresh in the minds of decision makers, the mistrust of the US intelligence agencies runs deep. A similar fear is felt in relation to China, although government interference with private data is perhaps more of an expectation than a fear.

46 Manyika et al.
Fear of losing control: The pace of modern technological development is astounding, and for many countries, there is a deep-seated fear that without radically nationalist policies to govern the data of their citizens and handicap the growth of market competitors, they will lose control. Once their digital development is linked to the cooperation of foreign powers, they may be unable to regain independence and data sovereignty. Further, for countries like India, asserting independence against foreign colonial powers has been an integral part of the nation’s modern identity.
How should policy makers respond?

Data localization was believed to provide nations with control over data in the absence of trust. Unfortunately, data localization is an ineffective means for control. Security offerings of smaller providers is generally weaker than larger players and foreign access cannot be barred simply by storing the data locally. While localization laws may reduce the competitive advantages of big tech companies, they also increase regulatory complexity, harm innovation and stifle economic growth. There are other, more effective and less damaging ways to keep the power of big tech in check.

How to address technical risks:

1. **National privacy law:** National data privacy legislation would signal to the global community that data privacy and security is paramount to the US Government. The lack of a national privacy law raises questions about how the US prioritizes data privacy. While there are a number of sector specific privacy laws (e.g., the Gramm-Leach-Bliley Act for financial services data or the Health Insurance Portability and Accountability Act for health insurance data) and state specific privacy laws (e.g., the California Consumer Privacy Act or the Massachusetts Data Privacy Act), there is no unifying central data privacy law. For businesses and consumers, both domestically and globally, this creates confusion and complexity. Fortunately, there does appear to be bipartisan support for the introduction of a national privacy law in the US. The latest attempt to introduce such a law is the SAFE DATA Act which amalgamates elements of previous attempts to introduce federal privacy legislation. The Act would provide consumers with more control over their data as well as holding business accountable for their data practices. While this may be met with some resistance from industry, stricter regulation of the private sector could be ultimately beneficial for international business as it could reduce the fears that foreign nations have about the power of US tech companies.
2. **Privacy and Security frameworks by industry:** Continued assurances by industry to customers about privacy and security will be important. For example, AWS recently updated its policy for EU customers\(^\text{47}\) to provide assurances that in the event of an access request under the US CLOUD Act, AWS would commit to challenging the request in court. Such a commitment demonstrates the importance that the company places in privacy and security, recognizing as fundamental to their business success.

3. **Investment in cybersecurity:** the US needs to be a leader in both the provision of services the protection of data and security. Where the US will set itself apart from China will be in the provision of digital services in a way that aligns with democratic values such as sovereignty, trust, the rule of law, justice, privacy and consent. Industry and public investment in cyber security will build strength in this area and ensure that in a competitive market, the US can offer a favorable alternative.

4. **Multi-lateral agreements under CLOUD Act:** leveraging the provisions of the CLOUD Act to form bilateral agreements should be a priority for the US Commerce Department’s foreign commercial service. Having these agreements in place for all key trading and business partners will help alleviate the concerns that data stored by US companies will be inaccessible to foreign governments in relevant to a criminal investigation.

How to address value concerns:

5. **US should take a collaborative approach to technology innovation with key allies:** Given the continued rise of a multipolar world order (incl., the US, China and Russia) and the ways in which emerging technologies could amplify a country’s economic, informational and military power, there is a growing need to ensure US is working in tandem with allies rather than against them. Instead of competing with allies (including but certainly not limited to the EU and UK), we should work together to facilitate technology.

\(^{47}\) “Supplementary_Addendum_to_the_AWS_GDPR_DPA.Pdf.”
development in a way that is safe, effective and in line with liberal and democratic values.

6. **Norms and standards around data use should be developed in collaboration with allies:** A national commitment to development such norms can help reset the table on sovereignty recognition and the importance of open and secure data (which are not mutually exclusive). While there will inevitably be divergence on the exact principles that should guide development, it is likely that much common ground can be found around the importance of privacy, security, the rule of law and human rights.48

7. **The US should make public and explicit commitments to criticize neocolonialism with respect to data:** For developing countries, or those with smaller economies or less technological capabilities, a major concern is the threat of data exploitation and colonization. Left unaddressed, multinational technology companies could collect huge pools of data on citizens and use that as ‘food’ for AI development.49 Addressing this concern may reduce the perceived need for data localization laws in these less powerful countries. Foreign service agencies, in collaboration with industry, should develop a set of principles that demonstrate commitment to data sovereignty and a commitment to use data only in ways that are consistent with the values of the US and its allies. As a starting point, these principles could be incorporated as part of a “responsible use of foreign data” section in the National Data Privacy Framework mentioned above.

---

48 Lawrence and Cordey, “The Case for Increased Transatlantic Cooperation on Artificial Intelligence.”
49 Ago, “Data as ‘Food’ for AI and Why We Need Data Sovereignty SOON.”
Conclusion

Both domestically and internationally, and in all imaginable spheres of life (healthcare, education, voting, transportation, energy, to name a few), emerging technologies are changing the world as we know it. These technologies create and use vast pools of data and governments must be able to assert sovereignty over this data on behalf of their citizens. Such assurances are essential for public trust in civic institutions, but must be balanced with needs to promote innovation, economic growth and collaboration between allies.

Particularly for nations with less digital independence (highly correlated to less geopolitical power) the dilution of data sovereignty is an ever-present fear. In response to this threat, decision makers have turned to data localization policies.

Unfortunately, data localization is proving ineffective. It does little to improve technical security and is an ineffective mechanism for stimulating domestic innovation and growth. What the policies seek at their core, is safety and security from nations that have conflicting values or have historical records of interfering with the sovereignty of other nation states.

In order to overcome the fear motivating these data localization policies, the US needs to overcome its growing reputation of digital autocracy and reassert its commitment to the success and development of all allies. While there may be some hesitancy about whether such assertions would be damaging for business, the clarity and security they would provide would actually be to the benefit of large tech companies. Operating in a global economy is challenging, and the concerns that arise in contexts where regulations is lacking end up being costly. For both economic and political ends, the US should aim for data policies that demonstrate a strong commitment to personal privacy, to sovereignty, and to the equitable advancement of digital capabilities in all allied nations.
Bibliography


