Data Localization
At What Cost?

Maxwell G., ‘25
Anthony K., ‘23

April 2023

PPCY 100
Professor Christine Walker

Table of Contents

Executive Summary

The average cost of a data breach in the United States was estimated to be $9.44 million.[1]The evolving global power structure poses not just a significant national security and economic threat to the United States, but also to the privacy of its citizens. A critical reason why this is increasingly occurring has to deal with the storage and processing of U.S. data that is mainly being conducted outside of its borders because of its lower cost, which has inherent consequences that are being seen today with the rise in data breaches.

Scale, Scope, and Root Cause of the Problem

Over 83% of the organizations IBM studied had encountered at least one data breach that compromised their servers.[2] Many cyberattacks can be linked to the rising axis of powers – Russia, China, North Korea, and Iran – who have been exposing weaknesses in the way the U.S. handles its data. The lack of U.S. data privacy legislation has led to the storage and processing of sensitive data in foreign states, making it susceptible for being intercepted by foreign adversaries.

Future Implications of Maintaining the Status Quo

The United States and its citizens will continue to be at significant risk to cyberattacks unless legislation aimed at providing comprehensive data security is enacted. If the lack of legislation continues, the U.S. will lag behind its foreign adversaries economically, militarily, and technologically. Future generations will have to grapple with the increase in identity theft and decrease in privacy, their data almost being held hostage by foreign entities. The lack of a data privacy framework will ultimately incapacitate the influence of the United States as a superpower in the world unless action is taken now.

Recommended Policy

[1] "Cost of a Data Breach 2022." IBM. Accessed April 9, 2023. https://www.ibm.com/reports/data-breach.

[2] IBM, p. 4.

This white paper supports the implementation of data localization policies in the United States, requiring all sensitive data to be stored and processed within its territories.

Expected Outcomes

1. Increased national security by reducing the risk of foreign adversaries getting access to sensitive military information
2. Improved privacy protections for U.S. citizens
3. Significant reduction in data breaches

Costs

- **Infrastructure cost:** Increased cost on companies to shift their servers and jobs to the U.S.
- **Impact on Small Businesses:** may be more difficult for them to comply due to less financial capital available
- **Resistance from U.S. citizens:** may fear that these policies can infringe on their privacy.

Benefits

- **Stimulating the economy:** shifting jobs and moving infrastructure to the U.S. may lead to job creation.
- **Peace of mind:** citizens may feel peace of mind knowing that their data is not being sent to foreign entities.
- **Greater control over data:** because citizen data is within the jurisdiction of the U.S., it may be easier for law enforcement to access data for national security purposes.

Practicalities

Citizens and politicians alike may see this greater control over their data by law enforcement as an invasion of their privacy, making it unlikely that they would support data localization policies. Conversely, companies and their lobbyists may not support a policy that would require them to invest billions into bringing jobs and infrastructure back to the United States.

Key Assumptions, Risks, and Success Factors

It is assumed that U.S. citizens will be in favor of data localization. However, there is a risk that the practicalities mentioned will discourage citizens from calling on the government to enact such policies. Success factors include engaging with technology experts, corporations, and the U.S. government to responsibly implement data localization.

Policy Effectiveness Plan

The effectiveness of the proposed plan should be tracked through a variety of metrics, including through the number of data breaches occurring yearly and their average cost. A decrease in the number of reported cyber attacks will indicate a positive impact.

Introduction

The late twentieth and early twenty-first century has seen the historic rise of the internet, allowing billions of people to communicate and connect. Technology provides many benefits in the lives of Americans, but at what cost? As more Americans connect to the internet, more data is harvested by brokers and companies for their own benefit.

Addresses, phone numbers, and other personal information have time after time again been sent to data brokers, seemingly without the consumer's permission. Although this information is typically entered to benefit the user, this information is also valuable to the provider, who can sell a user's personal data to benefit their own agenda.

This has led to a rise in concerns from consumers, who are increasingly looking for methods to protect their privacy in the digital age, and ask themselves this question: “At what cost do I get to use the internet?”

This paper will delve into data localization, a promising solution that has been implemented in various regions in the world, in order to combat the rise in cyberattacks and misuse of user data. These solutions are referred specifically to the United States and American tech users. Data localization will focus primarily on sensitive data, including military, health, or government knowhow.

Although data localization appears to show potential, several trade-offs exist if either of these methods were to be enforced. Both pros and cons of these options, if they were to be implemented, will be addressed in this paper. Seemingly no solution is perfect, but these privacy concerns must be addressed before they continue to evolve. Both organizations and governments must ask themselves this question “At what cost?” when creating a compromise between user privacy and national security.

Future Implications of Maintaining the Status Quo

As mentioned earlier, a fundamental issue surrounding data privacy in the United States and the world is that technology is outpacing legislation. Conversely, there is no single data privacy law in the United States that guarantees protection to citizen data. With the rise of superpowers like China and Russia, it is more imperative now than ever to find a solution to this ever-growing issue. Failure to implement data privacy policies in the United States can lead to reduced global competitiveness, since other countries are already implementing such policies, ensuring that their sensitive military, health, and government data is secure. Therefore, maintaining the status quo means that the United States will lose its status as the world's most advanced country as it increasingly falls behind the world in implementing data privacy policies that ensure the protection of national security and user privacy.

Key Assumptions of Enforcing Data Localization in the U.S.

- Companies will comply with U.S. data localization regulations and shift servers and jobs to the U.S.
- Because jobs and servers will shift to the U.S., it is assumed that these policies will ultimately stimulate the creation of jobs and support local economies
- Because data will now be stored in the U.S., it will be easier for law enforcement to access it when needed. Therefore, law enforcement is likely to support such policies, as it can streamline investigations and improve national security.

Risks

- Enforcing localization policies has shown to increase the costs of data-hosting for one company by 30-60%[3]
- Increasing costs can consequently lead to less capital available for innovation. Less capital = less innovation
- Data localization policies will be in direct conflict with existing policies. For instance, the United States-Mexico-Canada Agreement (USMCA) has distinctly banned data localization laws in an effort to improve a free flow of data[4]

Sensitivity Analyses and Success Factors

Because businesses are sensitive about cost, it is necessary to formulate policies that ensure the least financial burden on them while still achieving the desired data localization objectives. Similarly, citizens are sensitive to any privacy changes, and any policy implemented must strike a balance between

[3] Engdahl, Sylvia. “Blogs.” Amazon. Greenhaven Press/Gale, 2008. https://aws.amazon.com/blogs/security/introducing-a-new-aws-whitepaper-does-data-localization-cause-more-problems-than-it-solves/.

[4] Yayboke, Erol, Carolina G. Ramos, and Lindsey R. Sheppard. “The Real National Security Concerns over Data Localization.” CSIS. Accessed April 9, 2023. https://www.csis.org/analysis/real-national-security-concerns-over-data-localization.

securing their data and protecting individual liberties. Citizens are a key factor in the success of any possible implementation of data localization laws.

Current Legislation to Protect Data

The United States has not released any recent legislation to control the flow of information and prevent bad actors from breaching private user data, leading to a recent rise in data breaches from foreign adversaries and hackers. There is no single data privacy law in the United States that guarantees protection to citizen data.[5]

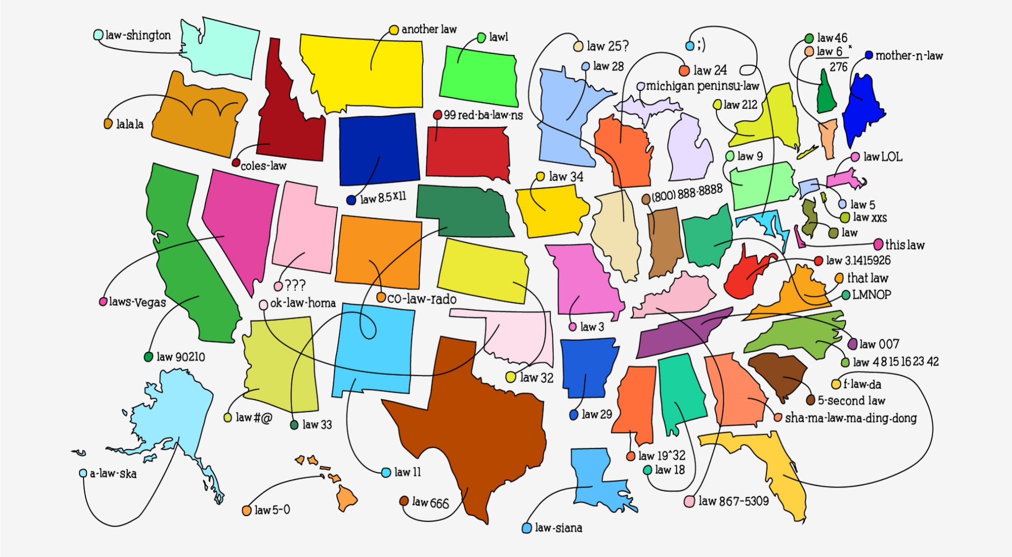
Instead, states have their own mix of laws and regulations that creates a murky, confusing mess for both the federal government and companies. States have their own laws that protect specific types of data (HIPAA, FCRA, etc).[6] These laws can help protect information regarding one's health and

[5] Klosowski , Thorin. "The State of Consumer Data Privacy Laws in the US (and Why It Matters)." The New York Times. The New York Times, September 6, 2021. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

[6] Klosowski, p. 3.

credit card information within specific organizations (health care provider or credit bureau).

However, the majority of data within the United States remains unregulated and generally can be used by anyone for any purpose. In most states companies can use, share or sell data without notifying the consumer. If sold, third-parties may continue to sell or use data without notifying the consumer.



Challenges in Keeping Up with Technology

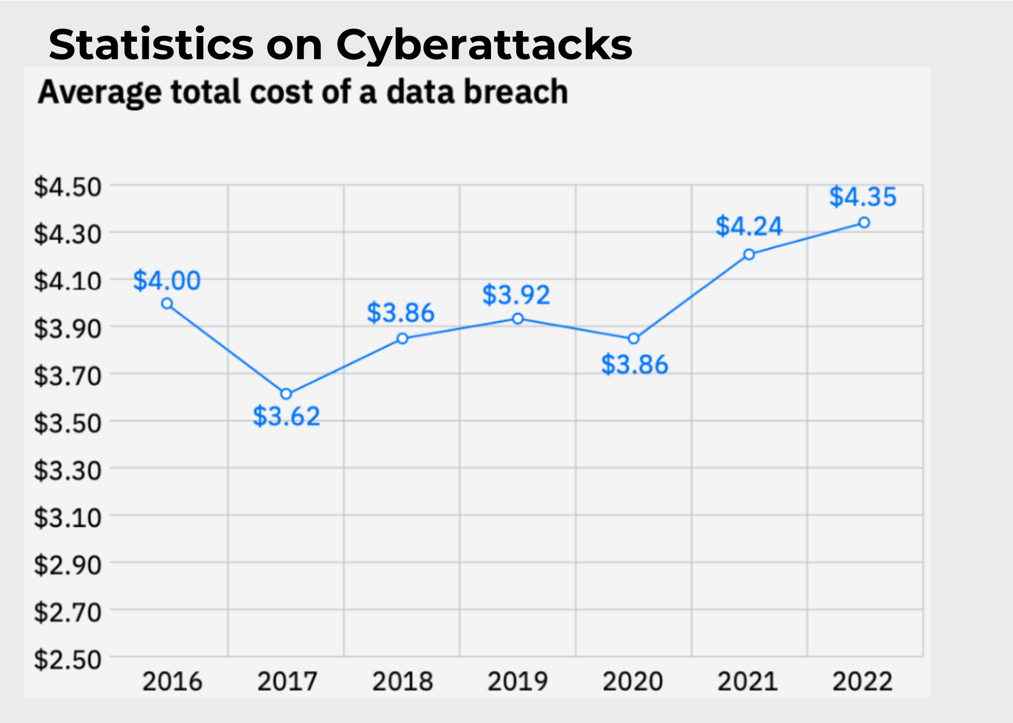
As the internet continues to expand at a rapid pace, and tons of data is produced every second, it has been challenging for legislation to keep up and find more permanent solutions. The Privacy Act of 1974 is one of the only federal laws aimed at protecting consumer data. However, this act only applies to the protection of consumer information within the government and does not protect consumer information within private companies. As a result, the current legislation from decades ago may not be sufficient to address the evolving landscape of data privacy.

The exponential rise of Artificial Intelligence (AI) has led experts in the field to call for a six-month halt to allow for the creation of ethical guidelines and regulations that can control this powerful technology and prevent its misuse.[7]The pace of technological change creates a regulatory lag that makes it difficult to create meaningful legislation. However, this regulatory lag creates an opportunity to create comprehensive data privacy policies that address the scale and scope of this issue. This issue creates the opportunity to brew the rise of jobs companies invested in reducing the lack of data privacy, while also strengthening the security of U.S. data infrastructure to ensure that foreign entities are unable to access any sensitive data.

Scale and Scope of Cyber Breaches

[7] Narayan, Jyoti, and Krystal Hu. “Elon Musk and Others Urge Ai Pause, Citing 'Risks to Society'.” Reuters. Thomson Reuters, April 5, 2023. https://www.reuters.com/technology/musk-experts-urge-pause-training-ai-systems-that-can-outperform-gpt-4-2023-03-29/.

According to a 2022 study from IBM, over 83% of the organizations they have studied had encountered at least one data breach that compromised their servers, with an average cost of one data breach in the United States being $9.44 million in 2022, and $4.35 million globally.[8] With the average cost of a data breach rising year-to-year as the amount of data sent to servers also increases, it is in the best interest of governments and companies to take preventative action against cyberattacks. The bulk of legislation aimed at preventing such anti-privacy attacks comes from the late 20th and early 21st century, an inherent issue considering that the internet has developed exponentially since.



[8] IBM, p. 5.

What Specifically is Data Localization?

Data Localization is the practice in which data is stored and processed within a certain jurisdiction. A method to ensure that data is kept within the confines of a country, ensuring that no outside force can gain unauthorized access.[9] For instance, data collected by an organization in the United States must be stored and processed in the United States – it cannot leave. For this to happen, servers that drive the processing and storing of data must be in the United States, rather than in servers located abroad. This ensures that the

[9] Devane, Heather. “Data Localization: A Complete Overview.” Immuta, October 24, 2022. https://www.immuta.com/blog/data-localization/.

data is under the jurisdiction of U.S. laws and regulations, ensuring a high level of control over the data that is processed in the region.

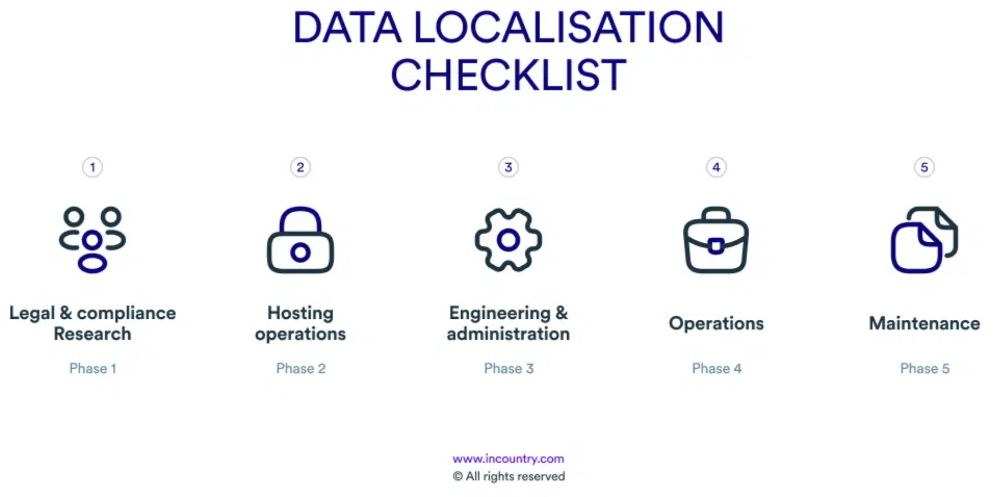
Benefits of Data Localization

- **Sensitive data secured within borders:** Servers stored within countries do not have to be analyzed by foreign forces. Servers abroad have their data analyzed routinely to follow their own laws or jurisdictions.
- **Creation of lasting server and building management and temporary construction jobs:** Servers and server buildings and infrastructure often take years to develop guaranteeing the creation of many construction jobs. Management of these facilities will help create jobs for many areas around the US.
- **Analyze all outgoing data from countries abroad:** All data will need to be analyzed to ensure all outgoing data does not contain any sensitive material.
- **Increased regulation for global corporations to secure our data:** Data security often falls onto corporations. Instituting regulation will ensure that they are required to not store sensitive data overseas.
- **Support for local governments:** Local governments will benefit from data centers being incorporated into their towns as they will create management, security, and construction jobs.

Policy Options for Implementation

How Can Data Localization be Implemented?

InCountry – a global data regulations organization designed to assist and ensure that organizations meet local data compliances – has created several standard phases that organizations and governments can take to implement data localization. It may be necessary for large multinational organizations to have multiple data centers in different parts of the world to ensure smooth and responsive services to their customers.



DATA LOCALISATION CHECKLIST

1. Legal & compliance Research – Phase 1
2. Hosting operations – Phase 2
3. Engineering & administration – Phase 3
4. Operations – Phase 4
5. Maintenance – Phase 5

www.incountry.com
© All rights reserved

- **Legal and Compliance Research:** create plans to build data centers in the countries in which data seek to be stored while researching their respective data regulation laws
- **Hosting Operations:** find hosting and backup providers for new servers and determine their cost
- **Engineering and Administration**: setting up the technical infrastructure and ensuring secure data access for administrators
- **Operations:** Create and implement cybersecurity and risk monitoring plans
- **Maintenance:** Define facility maintenance costs[10]

Trade-off: Although the amount of logistics and planning required to abide by the data regulations for one country ensures adequate security for data, it can be so time-consuming and extensive that companies would be deterred from expanding overseas. No expansion = less innovation, because they will be unable to access new markets and subsequently attract more capital that can be used to drive innovation.

What Competitors Are Doing

[10] Staff, InCountry. "Data Localization Checklist for Global Companies." InCountry, April 6, 2022. https://incountry.com/blog/data-localisation-checklist-for-global-companies/.

Seeing what China and Russia are doing – two countries at the forefront of data localization innovation – can give the United States some food for thought as to how to implement such policies.

The Personal Information Protection Law (PIPL) and the Data Security Law (DSL) that was passed in China ensures the protection of their citizens and national data while also filtering out data that could be sent overseas.[11] This data localization law also requires that the storage of sensitive data must be stored within the country's borders. However, there is some data that is stored within China that is permissible to be sent out of the country only after it has been analyzed to ensure safety. Violations of this law can come with heavy fines or even suspension of operations. Russia passed the Personal Data Law that grants similar requirements as China.[12] However, their punishments are more lenient, only focusing on fines instead of operational suspension.

Counterarguments for Data Localization

Innovation Cost, and Impact on Businesses

[11] Dorwarst, Hunter. "Demystifying Data Localization Report - FPF.org." https://fpf.org/blog/new-fpf-report-demystifying-data-localization-in-china-a-practical-guide/ Future of Privacy Forum, February 21, 2021. https://fpf.org/wp-content/uploads/2022/02/Demystifying-Data-Localization-Report.pdf.

[12] "How to Comply with the Russian Requirements on Localisation of Personal Data." Financier Worldwide. Financier Worldwide, November 2017.

Critics of Data Localization have voiced their opinions about government legislation to enact data localization laws in the United States. The concerns include:

- **Infrastructure Development:** building data centers and shifting jobs to the U.S. will require significant investment and time. It cannot happen overnight. There is both a megawatt infrastructure cost and building cost. The average reported cost of building a facility is $9.5 million per megawatt, and $1,000 per square feet.[13] Therefore, the cost of one 50,000 square foot facility with electricity infrastructure can cost $525 million, depending on location. Facebook, for example. developed a facility in Oregon costing $2 billion with 450,000 square feet of land to develop.
- **Compliance and Enforcement:** When Facebook launched its construction in Oregon, it did so because they received a tax break worth $73 million. Implementing opportunities for companies to save money from tremendous costs will entice them to abide by any regulation passed for localization. Enforcement of those laws if a company is in absolute violation of localization regulations will be difficult in a country where no such regulations exist. Even when they are in fruition, it will be difficult to enforce them effectively and

[13] Zhang, Mary. “How Much Does It Cost to Build a Data Center?” DGTL Infra, March 7, 2023.

consistently. China, however, has shown that a government is able to enforce data policies when they see fit. In 2021, they fined a company named Didi $1.2 billion for violating the CAC.[14]

5.2 – Trade-offs and Unintended Consequences

- **International Cooperation:** it is possible that U.S. data localization policies may clash with the data-sharing practices created by other nations, leading to either no data being transferred at all or a reduction in data trade.
- **Political Awareness:** lobbying efforts from companies may create obstacles to adopt data localization laws, who may argue that such policies will stifle innovation and unnecessarily increase costs for businesses.
- **Potential Misuse of Data:** under data localization laws, data is subject to the jurisdiction of the land it is in. Because data is no longer located outside its borders, it will be easier to attain it when needed. Therefore, for example, the United States has the right to gain access to a citizen's data when it deems fit. Critics argue that data localization laws can subsequently create a precedent for potential government overreach and infringe on individual liberties.

[14] Xiong, Yong, Larry Register, and Laura He. "China Fines Didi $1.2 Billion for Violating Cybersecurity and Data Laws | CNN Business." CNN. Cable News Network, July 21, 2022.

With this in mind, it might be worthwhile for the United States developing a committee similar to China's who's sole responsibility is to develop ways to heavily screen all ingoing and outgoing data to ensure that no sensitive data is at risk of being surveilled or captured by foreign adversaries. These regulatory methods could apply to companies both originating and not originating and operating within the U.S.

To encourage companies to shift their servers, the U.S. should consider Implementing subsidies or tax breaks that can offset the costs associated with implementing data localization policies. Opportunities for companies to save money from tremendous costs will entice them to abide by any regulation passed for localization. Finally, this development will secure the creation of many construction jobs as well as longer-lasting ones maintaining the data center. This could assist in financially depressed and sparsely populated towns within the U.S.

The effectiveness of the proposed plan should be tracked through a variety of metrics, including through:

- Number of data breaches occurring yearly
- Economic cost of each data breach
- Percentage of businesses in the U.S. complying with data localization regulations
- Public perceptions of possible privacy improvements through surveys sent to citizens

Conclusion

Because countries are now starting to develop methods and legislation in response to a rapidly growing technological world, data localization is still in its infancy when it comes to effective application. However, it will become increasingly important for countries to develop this legislation that forces globalized companies to abide by those same data protection laws to ensure the adequate protection of sensitive data. The age of information has made it clear that if there are companies who hold sensitive information, that information may get in the wrong hands either by accident, faulty code, malicious attacks, or simply by the regulation of where they store their servers. Thus, it is important for companies to be regulated on this crucial issue. Data is the most important article of information in the world and it must be protected by any means necessary.

Although data localization has its trade-offs, the United States and its government must recognize that they are the single most breached country since 2004.[15]More data protection laws would undoubtedly minimize this unsettling fact, but where is the line drawn between balancing personal liberties and protecting national security? The answer lies in the middle. Compromises will have to be made, but such is life in the digital age.

[15] "Data Breaches Rise Globally in Q3 of 2022." Surfshark, October 19, 2022. https://surfshark.com/blog/data-breach-statistics-2022-q3.