AWS Innovating Securely

Does data localization cause more problems than it solves?

Abstract

Data localization policies often intend to secure data, encourage economic competitiveness, and protect national values. However, new research by Emily Wu published by Harvard University's Belfer Center (Wu, 2021) indicates that localization policies are often counterproductive to these goals. Wu's research suggests methods that are more effective in achieving the intended outcomes, without the unintended consequences of data localization, such as stifling innovation, harming economic competitiveness, and failing to improve cybersecurity. These methods include continued investment in cybersecurity by government and industry and support for industry-led initiatives to develop shared standards and protocols.

Data localization rules are described by Wu as requiring "data to be stored and processed domestically, with the ultimate aim of enhancing sovereign control over citizens' data."

Contents

Introduction

Government data localization policies tend to stem from a similar set of drivers, which transcend political or economic differences. The reasons behind these policies generally involve the political, economic, security, and/or societal implications of transferring, processing, and storing data outside a country's physical boundaries.

However, 2021 research from Emily Wu at Harvard University's Belfer Center, entitled "Sovereignty and Data Localization," shows that data localization policies risk doing more harm than good. Contrary to their intent, localization policies stifle innovation and may harm economic growth without strengthening cybersecurity, national sovereignty, or personal privacy.

AWS Key Points on Data Localization

1) The security capabilities of AWS provide the ability for customers to take advantage of the best, most up-to-date technology while maintaining full control over their data with regard to the physical location of where it is stored.

2) Customers care deeply about privacy and data security. AWS continually monitors the evolving privacy regulatory and legislative landscape to identify changes and determine what tools our customers might need to meet their compliance needs.

3) AWS implements rigorous contractual, technical, and organizational measures to protect the confidentiality, integrity, and availability of customer data regardless of which AWS Region a customer selects.

4) The AWS Compliance Program helps customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud.

Contents

Drivers of data localization policies and ways cloud service providers address them

The recognition that data has value underpins many of Wu's findings regarding countries' desire to implement data localization policies. How data is collected, stored, used, and transferred can have a significant impact on civil society, economic growth, geopolitical relationships, industry growth, and national security. Countries' desire to protect that value for their national interest and on behalf of their citizens often drives data localization policies.

Wu addresses the drivers leading to data localization policies globally. She asserts that data localization is an ineffective solution at best, and harmful at worst, concluding that data localization rules are unnecessary for security and for local economic development. Amazon Web Services (AWS) agrees with Wu's conclusion. Overall, it's important that our customers have the freedom to build services quickly, securely, and efficiently using world-leading technology. Customers can use AWS services with the confidence that their customer data stays in the AWS Region that they select.[1] AWS implements rigorous contractual, technical, and organizational measures to protect the confidentiality, integrity, and availability of customer data regardless of which region an AWS customer selects. We also offer a large network of AWS partners who can support customer's compliance needs.

In this short review, we grouped the issues that Wu identified as drivers of data localization policies into four inter-related themes: data security, economic competitiveness, national values, and privacy and data access.

Data security

Wu lists improved security as a rationale that governments use for data localization policies but she argues that local data storage does not equal improved data security: "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."

At AWS, we leverage insights gained from our global footprint, applying lessons learned to improve security against cyber incidents throughout our infrastructure, including at the local level. After a customer picks the geographic region or regions in which they want to store their data, cloud infrastructure provides far greater resiliency and availability than organizations can achieve using on-premises infrastructure. In the cloud, rather than concentrating risk, data can be automatically distributed among multiple servers in the same location, and customers have the option to store their data in multiple locations.

[1] A small number of AWS services involve the transfer of customer data, for example, to develop and improve those services, where you can opt-out of the transfer, or because transfer is an essential part of the service (such as a content delivery service). We prohibit, and our systems are designed to prevent, remote access by AWS personnel to customer data for any purpose, including service maintenance, unless access is requested by you, is required to prevent fraud and abuse, or to comply with law. See https://aws.amazon.com/compliance/privacy-features/ for an overview of key privacy features of AWS Services which you can use to perform data transfer assessments in accordance with the Schrems II decision of the Court of Justice of the European Union, and the European Data Protection Board Recommendations on measures that supplement transfer tools.

We design typical cloud-based applications to operate across multiple physically isolated and redundant locations in a single AWS Region associated with a particular metropolitan area and country. These distinct but closely interrelated locations within a Region are called Availability Zones. This mitigates risk in the event of an incident and offers strong continuity and back-up options. Customers benefit from data centers and a network designed to support customers' security and compliance requirements.

Additionally, AWS offers robust privacy and security services and features that let our customers implement their own controls, including advanced access, encryption, and logging features. We make it easy to encrypt data in transit and at rest using keys either managed by AWS or fully managed by customers.

Economic competitiveness

A second driver Wu identified is the use of data localization policies to support economic aims, improve domestic economic competitiveness, generate economic activity and local investment, or help address worries of falling behind in the emerging tech race. However, Wu finds that localization constraints can deter innovation and hurt local economies by limiting which services are available to them, or increase costs given there is a smaller number of service providers to choose from. Citing a report by the Leviathan Security Group estimating that efficiency losses from data localization can increase the costs of data hosting by 30 to 60 percent, Wu concludes that data localization can "raise the barriers for market entry, which suppresses entrepreneurial activity and reduces the ability for an economy to compete globally."

Data localization policies are especially challenging for companies that trade across national borders. Whereas international trade used to be the remit of big corporations, data-driven efficiencies in shipping and logistics mean that international trade is open to companies of all sizes. There has been particular growth for small and medium enterprises involved in services trade (of which cross-border data flows are a key element). In a 2016 worldwide survey conducted by McKinsey, 86 percent of tech-based startups had at least one cross-border activity. The same report showed that cross-border data flows added some US$2.8 trillion to world GDP in 2014.

But, as countries are expanding their competitiveness through trade, data localization can serve to shrink competitiveness gains. A study by the European Center for International Political Economy examines the impact of recently proposed or enacted data localization and security regulations in seven economies found that data localization rules would lower GDP in all seven cases.

Included in the economic driver argument is the belief that data localization laws help a country's position in a global emerging tech race or even prevent it from becoming too dependent on countries who are global leaders in data technologies. However, this strategy is counterproductive because it ignores the benefits local economies receive from participating in the global economy and the associated efficiencies and innovations created by the free flow of data.

As the McKinsey report observes:

> "[D]ata flows support both productivity improvement and increased capital and labor inputs… [S]o far, data flows and digitization have raised net employment within countries rather than reducing it…[D]ata flows enable innovation, remote work, and new types of economic activity that did not exist before."

The availability of cloud services supports secure and efficient cross-border data flows, which in turn contribute to national economic competitiveness. Deloitte Consulting's report, "The cloud imperative – Asia Pacific's unmissable opportunity," estimates that by 2024 cloud will contribute $260B to GDP across eight regional markets with more benefit to come in the future if done right. The 2018 WTO World Trade Report estimated that digital technologies, including advanced cloud services, will contribute to an approximately 34 percent increase in global trade by 2030.

In addition to the impact on national economies, cloud customers can realize business value at the enterprise level including cost savings, increased business agility, productivity, and operational resiliency. An IDC study of 27 organizations from across industries and geographic regions found that, per 100 users, using AWS saved each organization an average of $21,621 in IT infrastructure costs annually. Also, each organization gained $32,316 in productivity benefits from fewer IT outages and $120,986 in improved agility and performance benefits. This data indicates that the decision to forego the use of cloud technology because the physical infrastructure is outside a given country can have a major negative impact on business inside that country.

National values

Related to economic competitiveness, Wu also cites a linkage between national data governance policies and concerns that movement of data outside national borders can diminish control over national values. However, the technology, storage capacity, and compute power provided by hyperscale cloud service providers like AWS empower local entrepreneurs to innovate. They are free to use the most effective tools for processing data while also meeting stringent local standards to protect national values and citizens' rights, such as the General Data Protection Regulation (GDPR) and forthcoming Artificial Intelligence Act (AI Act) in Europe.

Privacy and data access

Wu also highlights governments' desire to protect citizen's privacy as a justification for data localization policies. However, many countries institute strict privacy laws reflecting national or regional values and preferences and still allow the flow of data at the same time, making it possible to both protect citizens' data and privacy while still participating fully in the global economy. For example, AWS provides advanced encryption and key management services that customers can use to protect their content. We have industry leading encryption services that give our customers a range of options to encrypt data in-transit and at rest, and to manage encryption/decryption.

Other reasons cited by Wu for the persistence of data localization laws include data access requests by governments for legal or regulatory purposes. However, as Wu points out, local data storage is not the only way to ensure access for local law enforcement or regulators nor does it prevent lawful foreign government access requests. Any in-country provider who is subject to legal jurisdiction in any other country is subject to the same lawful order risks as an out-of-country provider. This is true for almost all but the smallest and most local of businesses.

AWS rigorously limits requests for data coming from any country without a compelling legal basis. For example, AWS will challenge law enforcement requests for customer data from governmental bodies, whether inside or outside the European Economic Area, where the request conflicts with EU law, is overbroad, or where we otherwise have any appropriate grounds to do so. AWS also commits that if it is ever compelled by a valid and binding legal request to disclose customer data, AWS will disclose only the minimum amount of customer data necessary to satisfy the request and we will continue to notify customers before disclosing content.[2]

Contents

[2] For more information on the AWS commitment to protecting customer data, see https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/ and https://aws.amazon.com/blogs/security/aws-and-the-cloud-act/

Other ideas worth exploring

Wu's paper concludes that "data localization is proving ineffective" for meeting intended national goals and offers practical alternatives for policy makers. Whereas Wu focuses on a US policy maker audience, several of her recommendations also have global resonance. These include:

- Continued **investment in cybersecurity** by industry and government. Partnership between industry and government will ensure that national and international policy makers have the most effective and up-to-date tools at their disposal.
- Support and encouragement for **industry-led initiatives to develop shared standards and protocols**. These are especially valuable for sectors that handle sensitive data such as health and financial services.
- Promotion of **international cooperation** around data privacy, sovereignty, and innovation among countries with shared values of privacy, security and rule of law.

Whereas effective multinational cooperation can take several years to achieve, investing in cybersecurity and working with international partners to develop standards and protocols for data-based technologies today can help create a more collaborative environment for innovation in the medium term.

In the longer term, alignment of domestic and international rules about how data should be collected, shared, transferred, processed, and stored could support international trade competitiveness, reduce the cost of compliance, and still maintain a high bar of data security. Creating an international regime to support data movement will depend on harmonization (where possible) and mutual recognition (when there are unavoidable national differences).

As Wu concludes, aiming 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" may prove to be sound policy making, a sensible procurement approach, and good for business.

The role of cloud services

Cloud providers invest heavily in cybersecurity capabilities and redundancy. Countries can realize similar objectives to those intended by data localization policies by using cloud services. AWS continually monitors the evolving privacy regulatory and legislative landscape to identify changes and determine what tools our customers might need to meet their compliance needs. AWS is constantly working to ensure that our customers can enjoy the benefits of AWS everywhere they operate. This allows AWS customers to take advantage of the economic benefits and the support for innovation provided by cloud computing while improving their ability to meet core security and compliance requirements.

AWS implements rigorous contractual, technical, and organizational measures to protect the confidentiality, integrity, and availability of customer data, regardless of which AWS region a customer selects to store their data. Finally, the AWS compliance program is available to help customers understand the robust controls in place at AWS to maintain security and compliance in the cloud.

Connect with us for more information.

Further reading

AWS Data Privacy:
https://aws.amazon.com/compliance/data-privacy/?nc1=h_ls

AWS Data Residency:
AWS Policy Perspectives, August 2020:
https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf

AWS GDPR Center: https://aws.amazon.com/compliance/gdpr-center/

Wu, Emily, "Sovereignty and Data Localization," Belfer Center, Harvard, July 2021: https://www.belfercenter.org/publication/sovereignty-and-data-localization#toc-9-0-0

Contents