CENTER
FOR
GLOBAL
DEVELOPMENT

Data Localization: A "Tax" on the Poor

David Medine

Abstract

Data localization refers to the ever-increasing trend by countries to restrict or prohibit the flow of certain types of data across their borders to other jurisdictions, with over 60 countries having some form of localization measures in place. This paper discusses what localization means, how it impacts trade agreements, its public policy pros and cons, the relevance of localization to Africa, its economic impact, three case studies of different types of stakeholders, and alternatives to data localization to minimize its impact on the poor.

WORKING PAPER 674 • JANUARY 2024

Data Localization: A “Tax” on the Poor

David Medine
Center for Global Development

The Center for Global Development is grateful for contributions from the Hewlett Foundation in support of this work.

David Medine. 2024. “Data Localization: A 'Tax' on the Poor.” CGD Working Paper 674. Washington, DC: Center for Global Development. https://www.cgdev.org/publication/data-localization-tax-poor

CENTER FOR GLOBAL DEVELOPMENT
2055 L Street, NW Fifth Floor
Washington, DC 20036

1 Abbey Gardens
Great College Street
London
SW1P 3SE

www.cgdev.org

The views expressed in CGD Working Papers are those of the authors and should not be attributed to the board of directors, funders of the Center for Global Development, or the authors’ respective organizations.

Contents

Foreword

David Medine's paper makes clear that data localization restrictions may have their greatest impact on smaller economies including many African countries, limiting access to the capacities, efficiencies and greater security of international cloud computing services, and that designing national data regulations to minimize these effects is vital in those countries.

The African Union has recognized this challenge. The AU Data Policy Framework, endorsed by the AU Executive Council in February 2022, sets out a shared continental vision to cooperatively enable data to flow across Africa and pave the way to the achievement of the Digital Single Market. The first recommendation is to "cooperatively enable data to flow on the continent while safeguarding human rights, data protection, upholding security and ensuring equitable sharing of the benefits" including coordination of regulation of data-driven business and personal data protection. The Framework also suggests "developing a Cross Border Data Flows Mechanism."

At the same time, smaller economies are often 'rule takers,' forced into compliance with regulatory regimes designed elsewhere because the cost of non-compliance would be too high—think of US Federal Aviation Authority regulations on airlines effectively implemented by all airlines that fly internationally, or European regulation of genetically modified crops and, indeed, data under the General Data Protection Regulation. While this is perhaps inevitable and sometimes beneficial, it is also inequitable. And it speaks to the need for global institutional structures governing decisions where discussion and agreement can be more inclusive.

The World Trade Organization is one such institution and yet the WTO Joint Statement Initiative on Electronic Commerce, designed to create a global agreement on issues from online consumer protection through cross-border data flows, now has 89 WTO members but only 7 African countries (although Nigeria has proposed data flow/localization carve-outs for developing countries and LDCs). Again, discussion of cross-border sharing of tax data with regard to data enterprises is limited to the G-24. As UNCTAD notes "global data governance would help enable global data-sharing," not least because data sharing rests on a foundation of trust.

Cross border flows of goods, services, people and (as this paper demonstrates) data are even more important to quality of life in smaller economies than they are in large economies. But that does not mean smaller economies should have no say in the mechanisms governing those flows. Stronger global data governance is one mechanism that would help ensure such an outcome.

Charles Kenny
Senior Fellow
Center for Global Development

Introduction

Data localization refers to the ever-increasing trend by countries to restrict or prohibit the flow of certain types of data across their borders to other jurisdictions, with over 60 countries having some form of localization laws, regulations or other requirements in place, doubling the number of localization measures over the past four years.[1] These policies have purported national benefits, though many of these benefits have been questioned. As the debate about this data policy spreads around the world, missing is a focus on the impact these localization policies have on the poor, particularly the extent to which localization imposes additional costs on firms providing goods and services to low-income consumers.

The use of global data technologies has increased the efficiency and reduced the cost of providing services, including critical financial services, to consumers who might otherwise be excluded because they are less profitable. Yet, data localization policies critically limit access to the efficiencies of international cloud computing services and reduce competition, offsetting the economic benefits cross border data flows would otherwise provide. Imposing technological restrictions and limiting or eliminating access to cross border cloud services results in increased costs on providers of services to low-income consumers, effectively imposing a "tax" on customers who are least able to afford higher prices. Another consequence of data localization is the potential of impeding anti-fraud, cyber protection and counterterrorism efforts because certain types of financial transaction information cannot be compiled and shared across national lines by law enforcement agencies or firms that operate internationally, such as payment processors, thus making low-income customers more vulnerable to financial losses.

This paper will discuss what localization means, how it impacts trade agreements, its public policy pros and cons, the relevance of localization to Africa, its economic impact, three case studies of different types of stakeholders, and alternatives to data localization to minimize its impact on the poor.

[1] Towards a Sustainable, Multilateral, and Universal Solution for International Data Transfers, A report by the UK Government's International Data Transfer Expert Council, November 2023, https://assets.publishing.service.gov.uk/media/655790a1544aea000dfb2fa6/towards_a_sustainable_multilateral_and_universal_solution_for_international_data_transfers.pdf; Gupta, Deepak, Data Localization Is Now a Big Part of Doing Business Globally, MarshMcLennan, October 21, 2021, https://www.brinknews.com/data-localization-is-now-a-big-part-of-doing-business-globally/ (over 100 countries). See also OECD, Svantesson, D. (2020-12-22), "Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines", OECD Digital Economy Papers, No. 301, OECD Publishing, Paris. http://dx.doi.org/10.1787/7fbaed62-en (Twenty-nine countries responded to the OECD questionnaire on data protection. Of these, 11 countries (38% of respondents) responded to the questionnaire saying that they have provisions in their data governance and privacy regulatory framework concerning data localization).

Localization

Localization is an umbrella term that covers a variety of national restrictions and requirements relating to cross border data flow, processing and storage. The strictest version, sometimes referred to as "hard localization", prohibits all cross border transfer of personal data. One example of this is found to some extent in the European Union's General Data Protection Regulation (GDPR) which prohibits data flows to certain countries[2] (subject to exceptions including for the relatively few countries whose laws offer adequate protection for the transferred data[3]). In China, certain types of data held by some controllers may not be transferred out of the country without government approval.

Another localization category is mirroring, the requirement that a copy of data must be *stored* in the home country. For instance, under a 2014 law the Russian Federation requires that data on Russians can be stored outside Russia only if a duplicate or mirror database is maintained in Russia. Similarly in 2022, Vietnam adopted a data localization regulation that requires companies to store personal data locally, thus facilitating the government's ability to inspect stored data. There can be a number of variations on the mirroring theme. In some cases, foreign *processing* of data might be permitted, so long as the data is stored in the home jurisdiction. There might be further limitations on which foreign jurisdictions can receive data if such jurisdictions do not provide adequate data protection.

Even if mirroring is not required, localization laws may impose other restrictions. In some cases, there might be a requirement that government regulators have access to data regardless of where it is stored. There may also be de facto prohibitions on cross border data flow where transfer compliance obligations are too burdensome. For instance, the law may require a country-by-country assessment of transfer risks including the strength of laws protecting data in the receiving country to ensure the presence of an independent supervisory authority and that the protections are essentially equivalent to home country protections. For instance, Tanzania's Personal Data Protection Act of 2022 requires that the receiving country have an adequate legal system for the protection of personal data. Such legal assessments can be costly, burdensome and still result in uncertainty about the risks posed. GDPR permits data to flow cross border if the receiving country provides adequate protection as determined by the European Commission. Notably, to date, no African country has been included on this list or, for that matter, Morocco's 2015 list of adequate countries.

Cross border sharing with mirroring might be allowed in some countries but with exceptions for certain types of sensitive information, such as health, financial and national security data which cannot be exported. Morocco requires companies engaging in activity of "vital importance" and using

[2] GDPR, Section 45.

[3] GDPR, Sections 46–50 (additional exceptions including data subject consent and binding corporate rules).

sensitive data to host their infrastructure on Moroccan territory. Likewise, Algeria mandates that cloud services' infrastructure be in the country, including website hosting.

In some cases, cross border data flows must be authorized by regulators: Kenya prohibits unauthorized transfers of public data; Nigeria subscriber data; Zimbabwe, Malawi and Tunisia restrict "personal information" flows; Sierra Leone telecom subscriber registration information without approval by the national telecommunications commission; and Zambia restricts "critical information".[4]

It is noteworthy that some countries have reversed the localization trend. In Saudi Arabia, effective September 2023, the strict prohibition on transfers of personal data outside the Kingdom have been amended. International transfers no longer require approval from the Saudi Authority for Data and Artificial Intelligence (SDAIA).[5] Even Switzerland (great protector of financial data) permits cloud usage in the financial sector![6]

Localization and trade

Trade agreements can be a forum for addressing localization issues. For instance, the United States has opposed including localization provisions in the United States-Mexico-Canada Agreement (USMCA), the 2019 North American Free Trade Agreement (NAFTA) replacement, as well as the 2019 US-Japan Digital Trade Agreement. Also, the United States-Singapore Joint Statement on Financial Services Data Connectivity states:

> "Consistent with these shared objectives, the United States and Singapore support allowing financial service suppliers to transfer data across borders and oppose generally applicable data localization requirements as long as financial regulators have access to data needed for regulatory and supervisory purposes. Data localization requirements can increase cybersecurity and other operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information. Data mobility in financial services supports economic growth and the development of innovative financial services and benefits risk management and compliance programs, including by making it easier to detect cross-border money

[4] CIPESA, Which Way for Data Localization in Africa?, November 2022, https://cipesa.org/wp-content/files/briefs/Which_Way_for_Data_Localisation_in_Africa___Brief.pdf.

[5] See https://www.mayerbrown.com/en/perspectives-events/publications/2023/05/saudi-data-protection-law-amendments#:~:text=M147%20of%205%2F9%2F1444H,Saudi%20DPL%20with%20the%20GDPR. Towards a Sustainable, Multilateral, and Universal Solution for International Data Transfers, A report by the UK Government's International Data Transfer Expert Council, November 2023, https://assets.publishing.service.gov.uk/media/655790a1544aea000dfb2fa6/towards_a_sustainable_multilateral_and_universal_solution_for_international_data_transfers.pdf ("countries that considered, but then shifted away from strict data localization requirement" include Indonesia, Brazil and Kenya).

[6] See https://pages.awscloud.com/fsi_switzerland.html.

> laundering and terrorist financing patterns, defend against cyberattacks, and manage and assess risk on a global basis."

The unratified Trans Pacific Partnership (TPP) would have prohibited data localization. The successor to the TPP, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) also prohibits requiring businesses to "use or locate computing facilities in that Party's territory as a condition for conducting business in that territory" but it does contain an exception for localization measures that a Party imposes to achieve "legitimate public policy objective[s]."[7]

In a surprise move, the United States government recently dropped its demand for free cross-border data flows in international trade agreements, to give it more room to regulate tech companies.[8] While some countries have begun to move away from localization laws, this new US position may give other countries a freer hand politically to enter into trade agreements that do not restrict localization, or to adopt new localization laws generally. In particular, this could result in countries with smaller economies imposing restrictions on cross-border data flows, ultimately imposing greater costs on their low-income consumers as discussed below.

Localization: For and against

The localization debate is quite complex due to the many real and unstated rationales. The following is a summary of the localization arguments—for and against—to put in context consideration of how resulting policies impact the poor.

Localization: In favor

Governments offer a variety of public policy bases supporting the adoption of localization laws including:

- **Cybersecurity and Cyberespionage:** Data can be maintained more securely, it is argued, if kept in the country since foreign actors would not have physical access to it.
- **Data Protection:** Data protection for citizens' data might not be safeguarded if subject to other countries' laws where the data is transferred and stored.
- **Law Enforcement/National Security/Government Agencies:** Domestic law enforcement might lose access to data stored in another country.

[7] Schweitzer, Frank, Ian Saccomanno, and Naoto (Nelson) Saika "The Rise of Artificial Intelligence, Big Data, and the Next Generation of International Rules Governing Cross-Border Data Flows and Digital Trade", 14 September 2023, https://www.whitecase.com/insight-our-thinking/rise-artificial-intelligence-big-data-next-generation-international-rules.

[8] Lawder, David, "US drops digital trade demands at WTO to allow room for stronger tech regulation," Reuters, October 25, 2023, https://www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25/.

- **Geopolitical Risks:** A concern that foreign intelligence services' surveillance will access data stored in their country.

  While likely a low risk, landlocked countries may have greater concern about data leaving the country because their country's cables could be cut, depriving them of access to the internet and their data. For example, Rwanda is land locked and has relied on data cables that run through Uganda and Tanzania, though earlier this year satellite internet access has begun to expand.[9] There is a theoretical risk that if those cables were cut or compromised, Rwanda could lose access to the internet and cloud storage—and its independence. Localization is a response to this risk, requiring local backups reduces this impact.

- **Competitive Advantages:** Requiring that data be stored in-country can give a competitive advantage to domestic data services providers.

- **Develop Domestic IT Capacity:** Requiring that data be hosted domestically could drive innovation and spur investments in local "hosting infrastructure if the right incentives for investment, the requisite skills, and enabling provisions on access to data and data use and reuse, are in place," though "not all African countries have the technological capacity or infrastructure, such as data centres, to meet the localisation demands mandated by their privacy laws."[10]

- **Combatting Neocolonialism:** Some see localization as a way to resist neocolonialism. The concern is that permitting data to flow outside the country into the hands of large international companies leads to those companies profiting from the data with a resulting loss of control by the home country. This may reflect particular concerns of indigenous peoples: "The threats of data colonialism are real," according to Tahu Kukutai, a professor at New Zealand's University of Waikato and a founding member of Te Mana Raraunga, the Māori Data Sovereignty Network. "They're a continuation of old processes of extraction and exploitation of our land—the same is being done to our information."[11] According to the founder of Terrastories, an open-source app co-created with Indigenous communities to map their land and share stories about it, a community in Guyana was emphatic about having an offline, on-premise installation of the app, because to members, "the idea of data existing in the cloud is almost like the knowledge is leaving the territory because it's not physically present."[12]

[9] Iriza, Diane, "Starlink deploys satellite internet in Rwanda, AfricaNews", February 20, 2023, https://www.africanews.com/2023/02/17/starlink-deploys-satellite-internet-in-rwanda//.

[10] CIPESA, Which Way for Data Localization in Africa?, November 2022, https://cipesa.org/wp-content/files/briefs/Which_Way_for_Data_Localisation_in_Africa___Brief.pdf.

[11] Caballar, Rina Diane, How Indigenous Groups Are Leading the Way on Data Privacy, June 7, 2023, Scientific American, https://www-scientificamerican-com.cdn.ampproject.org/c/s/www.scientificamerican.com/article/how-indigenous-groups-are-leading-the-way-on-data-privacy/?amp=true.

[12] Id.

One way to challenge neocolonialism is to use privacy enhancing technologies including decentralized storage on individual devices rather than centralized storage in an international cloud. The positive aspect of this approach is to give people greater protection and control over the use and sharing of their data; the downsides could include lack of disaster recovery tools and loss of the storage and processing benefits and efficiencies offered by cloud services.

Localization: Against

The following are some of the arguments against localization, pointing out the weakness of the arguments in favor and demonstrating that localization's benefits may exceed its costs.

- **Mirroring:** Meeting mirroring requirements means having to build domestic servers, thus adding capital and operating expenses, in addition to the cloud computing expenses incurred when data is stored and processed in other countries.

- **Data Protection:** Because encryption can be applied regardless of where data is stored, it is not necessary to rely on domestic data protection laws as data in foreign cloud servers will often be technically inaccessible to third parties, including cloud operators and foreign governments.

  Conversely, laws in other countries may compel disclosure of data even if stored in a country with a localization law which, at least, could set up a conflict between the two countries' laws. A law firm study found that "every single country [examined] vests authority in the government to require a Cloud service provider to disclose customer data in certain situations, and in most instances this authority enables the government to access data physically stored outside the country's borders, provided there is some jurisdictional hook, such as the presence of a business within the country's borders." It has been concluded that "a company cannot participate in the global market and avoid assertions of jurisdiction from countries outside of its home market."[13] As a result, "Data localization measures will likely not be effective to achieve" the goal of preventing foreign governments from accessing data held in a country.[14]

  Geopolitical risks can be mitigated as cloud service providers often offer a choice of which countries will—and will not—house data. Geopolitical concerns may also be addressed in a variety of ways, also including encryption of the data.

- **Cyber Resilience:** In many cases, offshore cloud service providers have greater technical expertise and tools to protect data than do local IT companies. Because cloud providers are large firms whose business, in large part, is to offer protection of data, they have the incentive and ability to invest heavily in cybersecurity.

[13] Pervaiz, Shanzay and Alex Joel, Data Localization and Government Access to Data Stored Abroad, CIPL/TLS Discussion Paper 2, March 2023, https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1089&context=research, at p. 9.

[14] Id. at p. 10.

- **GDPR Compliance:** Firms outside of the EU may need to comply fully or substantially with GDPR requirements, either because they operate in a country that has been found to have adequate data protections by the EU or due to contractual obligations. In some case, cloud service providers have their own GDPR compliance obligations but also offer services and resources to its customers to comply with GDPR.[15] Thus, to a degree, GDPR compliance burdens are shifted to the cloud provider. However, without access to cloud services, it may fall fully on domestic firms to determine what compliance efforts are required by GDPR and then implement appropriate measures, adding costs to their operations.

- **Defending Against Attacks:** In many matters, financial institutions are highly competitive with each other, carefully guarding their proprietary data. Yet, in the cybersecurity context, such institutions appreciate that the benefits of information sharing far outweigh the downsides. One example of this is the Financial Services Information Sharing and Analysis Center, the only global cyber intelligence sharing community solely focused on financial services. Its over 5,000 members in 70 countries, including banks, exchanges, FinTechs, and insurance companies, see the value of having access to threat reports which can alert them to the tools, methods and actors behind the attacks. With actionable information its members are in a better position to guard against such risks.

  Information sharing across borders is critical to defending against cyberattacks, money laundering, and fraud attempts. The ability to share and act on threat information is particularly important for developing countries whose financial institutions are increasingly the focus of cybertargets because developed world entities have built stronger defenses against such attacks. Being armed with threat information from other countries improves the ability to defend against attacks.

  Localizations laws that inhibit the movement of threat data across borders largely only hurt the countries that enact such laws by diminishing their ability to detect attacks. As the number and sophistication of threats increases, including the involvement of nation states with huge resources, financial entities in Africa and developing countries in other regions, need all the help they can get to repel attacks, whether cyber, fraud, or terrorism related. Failure to defend effectively leads to greater losses by financial institutions that, in turn, get passed along to consumers in the form of higher charges for their products and services. These added charges are also effectively "taxes" on the poor—taxes that could be reduced if domestic financial institutions do not have their defenses reduced due to localization laws.

- **Security Does Not Require Localization:** Anonymized data has identifiers stripped off; encrypted data is converted into a code to prevent unauthorized access. Financial institutions and other entities can both anonymize and encrypt their data, whether it is stored in their data centers or in the cloud. In other words, localization is not the key to

[15] https://aws.amazon.com/compliance/gdpr-center/ ("AWS is committed to offering services and resources to our customers to help them comply with the GDPR requirements that may apply to their activities").

security. In fact, attackers could probably be better able to break into an individual firm's data center because it would not be nearly as well protected as when it is in the cloud. As the OECD has noted, "in the light of the combination of encryption technologies, and the possibility of remote access, just as physical access does not guarantee actual access to the data, lack of physical access does not exclude the possibility of access to the data."

- **China:** There is some concern that China will be willing to subsidize installation of data centers in various countries as required by data localization laws. Even if not strictly economically justified, it could give China a means to access such data for intelligence purposes.[16] In addition, technology provided by China could enhance countries' ability to engage in surveillance activity of citizens which would inhibit free speech and make it more likely for those countries to adopt repressive digital governance policies such as those found in China. Furthermore, once Chinese technology is embedded, it may be difficult for competitors to challenge the Chinese presence in the future.
- **Hinders Dissent:** Localization restrictions could hinder political dissidents and human rights activists' ability to communicate with each other by facilitating government surveillance of communications and the ability to communicate with like-minded people in other countries. During a discussion at a Center for Global Development roundtable the following comments were made:

> "While policymakers often justify such measures on the grounds of strengthening law enforcement and national security, most participants believed that they are usually enacted to facilitate data surveillance and hinder foreign competition—often at great cost to domestic companies that rely on foreign cloud-based services that are cheaper and more secure than domestic alternatives."[17]

In June 2023, the Washington Post reported that Vietnam's localization requirements were enacted in support of government censorship: "The Vietnam country representative for the US-ASEAN Business Council, said the intention of the law was … straightforward: to pressure companies to tighten censorship. In private meetings, the government has told Meta it will be forced to localize data only if it breaks laws on content … In response, Meta has

[16] Montgomery, Mark and Eric Sayers, Don't let China take over the cloud—US national security depends on it," November 13, 2023, The Hill, https://thehill.com/opinion/national-security/4307002-dont-let-china-take-over-the-cloud-us-national-security-depends-on-it/#:~:text=Their%20cloud%20providers%20are%20heavily%20subsidized%20by,on%20price%20and%20expand%20their%20infrastructure%20globally (China's "cloud providers are heavily subsidized by the government, allowing them to undercut competitors on price and expand their infrastructure globally … . This is especially troubling as China's national intelligence laws make it incumbent on China's service providers to cooperate with any government requests—meaning Beijing can use gain access to stored data without the owner's consent").

[17] CGD, How Can Multilateral Organizations Strengthen Global Data Governance Practices?, December 2021 at p. 5.

mounted a renewed effort to toughen content controls."[18] This is an example of localization policy not based on stated reasons but instead based on unstated goals.[19]

- **Economic Burden:** As discussed in detail below, depriving domestic firms' access to international cloud computing services imposes costs on their ability to deliver services, particularly to the poor. One example is imposing the need to build and operate data centers, which at any given time will be more or less data storage than needed, whereas cloud computing easily permits firms to control the size of their data storage based on business demands. There are also indications that domestic firms may charge more for data storage than international cloud service providers.
- **Impact on Competition:** While localization can protect domestic firms from international competition, some argue that competition through international trade and data exchanges is likely to be more beneficial to the domestic economy.
- **Environmental Impact:** Cloud computing centers are as much as 72 to 98 percent more carbon efficient than company data centers, using more renewable energy sources and consuming less water for cooling purposes.[20] Localization mirroring requirements not only impose additional capital and operating expenses to operate local data centers, but they also have a negative impact on the environment.
- **Impact on Telework:** Strict localization requirements may restrict or prevent teleworking with participants in other countries, thus reducing employment opportunities for citizens.
- **Builds in Inefficiencies:** Many business functions are impacted by the ability to efficiently move data. One example is the insurance industry. To process insurance claims, it is necessary to gather data on the claimed loss from multiple sources. In many cases, the insurance companies operate in multiple countries. With localization, this would require duplicating the insurance facilities' need for processing. A similar inefficiency might result if companies hired a foreign firm to survey their own customers—including low-income customers—to improve the products being offered. Yet, with localization, the foreign survey firm might not be able to evaluate a larger population of customers if they are found in multiple countries.
- **Downtime:** Given the structure and redundancy features, it is likely that cloud services companies will be more reliable and experience less downtime than individual firms.

[18] "Facebook helped bring free speech to Vietnam. Now it's helping stifle it", by Rebecca Tan, June 19, 2023, https://www.washingtonpost.com/world/2023/06/19/facebook-meta-vietnam-government-censorship/.

[19] "Adding to the complications associated with mapping out the reasons data localisation requirements are introduced, countries may not always be entirely transparent as to their true motivations." OECD, Svantesson, D. (2020-12-22), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", OECD Digital Economy Papers, No. 301, OECD, Publishing, Paris. http://dx.doi.org/10.1787/7fbaed62-en.

[20] Bouwen, Yves, "Cloud computing: an opportunity for carbon reduction?", https://mcloud.devoteam.com/expert-view/cloud-computing-an-opportunity-for-carbon-reduction/#:~:text=Carbon%20benefits%20of%20cloud%20computing&text=Microsoft%20cloud%20is%20between%2072,lower%20carbon%20footprint%20%5B3%5D; Lavi, Hessam, "Measuring Greenhouse Gas Emissions in Data Centres: The Environmental Impact of Cloud Computing", April 21, 2022, https://www.climatiq.io/blog/measure-greenhouse-gas-emissions-carbon-data-centres-cloud-computing.

- **Database Expertise:** Data management may not be key to firms' business, thus making it more likely that cloud service providers will be in a position to know about and apply state of the art expertise to database management.
- **Credit Histories:** People spend decades developing a credit history in one country which is maintained in a credit reporting agency or with financial institutions. In some cases, the subjects of these histories voluntarily move to another country, to pursue work opportunities or for family reasons. In other cases, the cross-border moves are involuntarily, such as for displaced persons involved in conflicts. In either case, it can be very beneficial to carry one's credit history to another country whether it is a temporary or permanent home. For example, stays in refugee camps may drag out for years, necessitating the establishment of credit and other financial relationships for that duration. A strict data localization law could prevent the communication of credit histories to people who might desperately need them to benefit from financial inclusion opportunities.
- **Lost Opportunities:** ChatGPT, an AI chatbot, and other artificial intelligence (AI)/machine learning implementations rely on training on large datasets including those from multiple countries. If a country adopts a broad data localization law, AI training based on multiple countries' data might be prohibited. As a result, the country may be deprived from having its data included as part of an AI model's development system. If other countries take the same approach, AI models may suffer in their applicability and rigor. Of course, each country must decide whether, on balance, it is better off participating or not in improving AI development. Either way, it makes sense for this to be an intentional decision.

Relevance to the African experience

Africa is wrestling with how countries on the continent can maximize the benefits of cross-border data flows. How this challenge is addressed will be important for African countries as well as being a model for other regions around the world. One significant step toward a broad effort to harmonize data protection and facilitate the flow of data across Africa is the African Union's Convention on Cybersecurity and Personal Data Protection ("Malabo Convention"), adopted in 2014. On June 8, 2023, the Convention took effect after the 15th of 55 African Union member states ratified the agreement.[21] The Convention, among other things, provides for a framework to protect personal data and countries that adopt it are required to establish data protection authorities and ensure that

[21] The ratifying countries and dates of ratification are: Angola (11 May 2020), Cape Verde (5 February 2022), Côte d'Ivoire (3 April 2023), Congo (23 October 2020), Ghana (3 June 2019), Guinea (16 October 2018), Mozambique (21 January 2020), Mauritania (9 May 2023), Mauritius (14 March 2018), Namibia (1 February 2019), Niger (16 March 2022), Rwanda (21 November 2019), Senegal (16 August 2016), Togo (19 October 2021), and Zambia (24 March 2021). 28 Sep 2023. "The Malabo Convention entered into force on 8 June: Africa's move towards shared data and cybersecurity standards and rules," Digwatch, September 28, 2023, https://dig.watch/updates/the-malabo-convention-enters-into-force-africas-move-towards-shared-data-and-cybersecurity-standards-and-rules#:~:text=The%20Malabo%20Convention%2C%20also%20known,as%20required%20by%20the%20Convention.

personal data is collected, processed, and stored securely. It is too early to draw conclusions about how successful the Convention will be in harmonizing data protection in Africa, as there will be implementation challenges and a number of larger countries have not yet signed on, including Egypt, Nigeria, South Africa, Kenya and Ethiopia.[22] In addition, questions remain regarding some of the details of what the Convention substantively requires as well as its enforcement mechanisms.

While ratification of the Convention was pending, the African Union's Data Policy Framework, (Framework), dated February 2022, was endorsed by the African Union's Executive Council. The Framework's goal was to "ensure that data can flow across borders as freely as possible while achieving an equitable distribution of benefits and addressing risks related to human rights and national security." Meeting these goals will require, as a commentator has noted, "cooperation to ensure safe and effective cross-border data flows … to collaborate on complex issues around standards and safety, thus ensuring an inclusive playing field." The Framework notes that localization laws "limit the cross-border flow of information necessary for local value creation and establishment of the single market."

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) has noted that localization critics argue that localization can undermine data privacy by facilitating government agencies' access to citizens' data to conduct state surveillance, asserting that "data localisation policies are causing more harm than good" as "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."[23] Virtually all the countries in Africa that have adopted data localization requirements have done so without clear explanations, according to CIPESA which reports on the suggestion that:

> "the increased enactment of data localisation laws in Africa is attributed to the unfounded fears that sending citizens' data across borders could increase vulnerability to data privacy and security breaches. However, given the proclivity of many African governments for surveilling citizens, it is plausible that requiring data to be stored locally is also aimed at enabling easy access to that data by the state, including security agencies."[24]

The Framework recognizes that while laws can promote cyber security defenses, they can also be used to legitimize "systems of oppression and repression." Therefore, cyber policy aimed at strengthening data security should consider the impact on online human rights. In addition, instilling "a culture of trust in the data ecosystem" can be accomplished through effective cybersecurity and data protection rules.

[22] Id.

[23] CIPESA, Which Way for Data Localization in Africa?, November 2022, https://cipesa.org/wp-content/files/briefs/Which_Way_for_Data_Localisation_in_Africa___Brief.pdf, quoting Emily Wu, Sovereignty and Data Localization, https://www.belfercenter.org/publication/sovereignty-and-data-localiztion.

[24] Id.

A focus on economic consequences of data localization is required by the Framework: "While data localisation is often seen as an expression of state sovereignty, as a possible policy option, data localisation needs to be assessed on a cost-benefit basis." The Framework also comments on technical consequences of localization requirements:

> "Data localisation involves the artificial erection of legislative barriers to data flows, such as through data residency requirements and compulsory local data storage. Strict data localisation rules requiring the storage of all data locally, and not merely a copy, renders such data susceptible to security threats, including cyber-attacks and foreign surveillance. Some African countries face acute technological capacity constraints so that localisation capacity demands may vastly exceed national data centre capacity. Concomitantly, requirements for duplicate copies of data may place undue financial obligations on local companies."

Another opportunity to address these issues can be found in the context of the Africa Continental Free Trade Area (AfCFTA), covering the world's largest free trade area by bringing together the 55 countries of the African Union, 1.3 billion people, a combined GDP of $3.4 trillion and consumer and business spending valued at $4 trillion. While the AfCFTA digital trade protocol does not currently include provisions addressing cross-border data flows, they are the subject of ongoing discussions. A trade agreement would help address the impact of localization which Research and Policy Integration for Development (RAPID) and CUTS International have noted "typically increases compliance costs for companies, disrupts global supply chains, acts as a non-tariff barrier, and poses roadblocks to the path of digitally enabled growth. Trade agreements could be a forum for harmonizing data protection frameworks which would facilitate the free flow of data in the region as well as strengthen its negotiating power vis-à-vis other regions, included the European Union and the Asia-Pacific.

In addition, there are two organizations that could play a constructive role in harmonizing laws and practices throughout Africa. Smart Africa is an alliance of 32 African countries, international organizations, and global private sector players tasked with developing Africa's digital agenda with a vision to create a single digital market in Africa by 2030. The NADPA/RAPDP (Network of African Data Protection Authorities/Réseau Africain des Autorités de Protection des Données Personnelles) brings together 19 African national authorities whose mission is to promote the protection of personal data and privacy as a fundamental human right. They can play a role in promoting cross-border data flows to ensure that data localization requirements do not unduly interfere with cross-border communications.

Aside from continent-wide efforts, individual countries have been enacting national legislation. Senegal, for example, has adopted a data protection law that restricts cross border data transfers to countries that do not provide sufficient protection for the data, subject to some exceptions including consumer consent. These national laws could facilitate the cross-border flow of data, especially if trust for such transfers is developed.

Economic consequences

Studies have found that data localization can lower productivity, negatively impact trade output, and increase prices. When this occurs in emerging markets and developing economies, the poor suffer. These studies often do not specifically focus on the financial impact of localization from the perspective of low-income consumers. The goal of this paper is to focus on just that.

Macroeconomic

Before turning to the economic impact of localization on the poor, as background, a number of studies have asserted that data localization policy has or will have a negative impact on economies as a whole. The Information Technology and Innovation Foundation (ITIF) has found that a 1 percent increase in restricting data flow results in a 7 percent decrease in gross trade output, a 2 percent decline in productivity and a 1.5 percent hike in the price of goods.[25] The European Center for International Political Economy (ECIPE) projects that China's localization laws or legislative proposals would cost the economy up to 1.1 percent in gross domestic product (GDP), reduce domestic investment by 1.8 percent, exports by 1.7 percent along with a loss of 13 percent of salaries.[26] Localization restrictions are expected to reduce investment in Vietnam by 3.1 percent, Indonesia by 2.3 percent and India by 1.4 percent.[27]

More recently, in 2022, Research and Policy Integration for Development (RAPID) conducted a study of the economic impact on Bangladesh of adopting a localization law similar to laws found in India and Vietnam. RAPID estimates that this policy would decrease digital services exports (29 to 44 percent) and decrease GDP by 0.6 to 0.9 percent. Another report estimates that data localization would result in a 1.7 percent decrease in GDP for India and 0.5 percent and 0.1 percent for Indonesia

[25] Centre for Information Policy Leadership ("CIPL")," The 'Real Life Harms' of Data Localization Policies (Discussion Paper 1), March 2023, https://privacyacrossborders.org/wp-content/uploads/2023/03/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf; Cory, Nigel and Luke Dascoli, "How Barriers to Cross-Border Data Flows are Spreading Globally, What They Cost and How to Address Them," Information Technology & Innovation Foundation, July 19, 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

[26] Id.; Bauer, Matthias, Lee-Makiyama, van der Marel, Verschelde, the Costs of Data Localisation: Friendly Fire on Economic Recovery, European Centre for International Political Economy, 2014, https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf.

[27] Castro, D. and McQuinn, A., 2015. Cross-border data flows enable growth in all industries. Information Technology and Innovation Foundation, 2, pp.1–21; RAPID (Research and Policy Integration for Development) and CUTS International, Impact of Cross-border Data Flow Restriction on Bangladesh Economy, https://www.rapidbd.org/wp-content/uploads/2022/07/Impact-of-Cross-Border-Data-Flow-Restrictions-on-Bangladesh-Economy-Report-Two.pdf.

and Vietnam respectively.[28] Retaliation by trading partners would have an even greater impact.[29] The World Bank's World Development Report in 2020 concurs, finding that "restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies… Countries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies, whereas the benefits of reducing data restrictions on trade in services would on average be about 5 percent."[30] Missing out on technology that would increase productivity and decrease the cost of doing business will particularly impact small and medium size enterprises. All these negative economic consequences would undoubtedly have an oversize impact on the poor.

Impact on the poor

While regression models demonstrate that data localization laws have a statistically significant negative impact, the "impact [on economies] is particularly acute in small and less digitately developed ones,"[31] meaning oftentimes on the poor in those countries. Some of the costs, as discussed below, arise from the added localization compliance costs that companies face. Less apparent may be the cost of firms deciding to leave—or not even enter—a market due to higher compliance costs, such as having to set up duplicative data centers. Company capital could instead have been used to increase product offerings for consumers or charging lower prices in response to competition.

Restricting businesses' access to cloud computing is detrimental to the poor as cloud computing offers efficiencies and flexible data storage sizing that permits providers to invest in new products and hire additional personnel instead of building computer server farms that at any given time are either too large or too small for their needs. The ability to use cloud standardization procedures and formats means companies can focus their limited resources on things that provide value to their customers.

Under a localization regime, domestic firms would be required to invest capital in building their data storage capacity, costs that will often be passed onto consumers. By contrast, cloud services allow customers to dramatically expand or contract their data storage as needed, thereby freeing capital

[28] Enabling Cross Border Data Flow: ASEAN And Beyond. https://sgtechcentre.undp.org/content/sgtechcentre/en/home/blogs/cross-border-dataflow.html; RAPID (Research and Policy Integration for Development) and CUTS International, Impact of Cross-border Data Flow Restriction on Bangladesh Economy, https://www.rapidbd.org/wp-content/uploads/2022/07/Impact-of-Cross-Border-Data-Flow-Restrictions-on-Bangladesh-Economy-Report-Two.pdf.

[29] Dr. Abdur Razzaque et al., "Impact of Cross-Border Data Flows Restrictions on Bangladesh Economy" (Research and Policy Integration for Development (RAPID) and CUTS International, July, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION | DECEMBER 2022 PAGE 61 2022), https://www.rapidbd.org/wp-content/uploads/2022/07/Impact-of-Cross-Border-Data-FlowRestrictions-on-Bangladesh-Economy-Report-Two.pdf; Cory, Nigel, Luke Dascoli and Ian Clay, ITIF 2022 Report: The Cost of Data Localization Policies in Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam, December 12, 2022, https://itif.org/publications/2022/12/12/the-cost-of-data-localization-policies-in-bangladesh-hong-kong-indonesia-pakistan-and-vietnam/.

[30] World Bank, World Development Report (Washington DC; 2020), https://www.worldbank.org/en/publication/wdr2020.

[31] Cory, Nigel, Luke Dascoli and Ian Clay, ITIF 2022 Report: The Cost of Data Localization Policies in Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam, December 12, 2022, https://itif.org/publications/2022/12/12/the-cost-of-data-localization-policies-in-bangladesh-hong-kong-indonesia-pakistan-and-vietnam/.

to invest in new products or hiring. This flexibility also encourages innovation by allowing firms to expand capacity to test new products and simply reduce capacity if the test product does not catch on. It is likely that local data centers cannot offer the efficiencies of larger, international firms.

Local centers would also have to size their processing capacity for the maximum transactions per second during the day while leaving its processing capacity dormant in the overnight hours. With cloud, firms can configure not only their storage size but in some cases their processing rates by shifting non-urgent processing to times when processing rates per second are lower. Overall, these added processing and storage costs in many cases will result in product/services cost increases to the consumer. Importantly, for these purposes, the overhead and operational costs of maintaining data centers could price offerings above the level at which it is economical to serve the very poor. Furthermore, data centers themselves use little human capital meaning that the benefit of increased employment is not likely to offset the increase costs.

While this paper does not attempt to quantify the costs of localization to the poor, as they will vary greatly from company to company and country to country, as the OECD notes:

> "it appears settled that data localisation does indeed impose a considerable cost on those forced to abide by data localisation requirements. That cost comes, for example, in the form of 1) the cost of local employment and infrastructure investment, 2) the cost of efficiency losses such as disruptions to global consolidation plans and skill dilution compared to using the best equipped and most skilled staff wherever they are located; and 3) the increases in compliance costs and the legal uncertainty that stems from the unpredictability of scope and application of data many localisation requirements."[32]

Furthermore, the OECD paper notes the negative impact on smaller domestic companies that would be burdened with high compliance costs and thus lose out to dominant domestic firms that have the ability and can afford to comply. In turn, the resulting decline in competition is another factor in increased costs of services. Looking at the country-level economic impact of localization policy:

[32] OECD, Svantesson, D. (2020-12-22), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", OECD Digital Economy Papers, No. 301, OECD Publishing, Paris. http://dx.doi.org/10.1787/7fbaed62-en ("As commonly is the case, [localization] costs are ultimately passed on to consumers").

> “Put simply, if all countries introduce data localisation requirements, most organisations will find it too costly to comply with all countries’ requirements. They will then prioritise based on which markets they see as most profitable and other such considerations. Poorer less developed countries would be at risk of missing out both on e.g., the goods and services offered by the respective organisations. If correct, this scalability issue may mean that data localisation practises end up widening the gap between those countries that are dominant in the online environment (typically richer more developed countries) and those that are struggling to reach their potential (typically poorer less developed countries).”[33]

While all data centers are vulnerable to natural disasters, political strife or military conflict, international cloud services firms can more easily factor these considerations into the decision of where to locate their data centers given their broad geographic options. As a result, there would be a greater chance of domestic data service center disruptions which would often weigh more heavily on the poor. The impact of the need to build domestic data centers and address related regulatory compliance burdens imposes added costs on entering the market for startups or international firms considering investments. Mirroring requirements may present the worst of both worlds—paying for cloud services but still having to build a domestic data storage facility. Inability to access cloud services, especially in smaller countries with a less developed IT infrastructure may make it harder for financial institutions to offer more efficient remote bank account opening and use of banking services which would have a great impact on the poor’s access to financial services.

Perspectives

In order to gain an appreciation of the economic impact of data localization on the poor, a number of stakeholders were contacted. The boxes below relate the impact of data localization on a bank, a FinTech, and a cloud services provider.

[33] Id.

CASE STUDY 1.

South African bank TymeBank's goal is to offer more affordable, accessible banking services for all in South Africa. Without the cloud, TymeBank would struggle to achieve its goal of democratizing financial services and providing affordable banking to all South Africans. In fact, under TymeBank's business model, all eligible South Africans (over 16 years old) can afford a TymeBank account due to the Bank's technology and efficiency.

TymeBank is fully digital and is known for serving the full population, including low-income rural customers, through well-designed products, for example low-cost transactions and high-yield savings accounts. Most of TymeBank's customers choose to use the bank's services because they are affordable. As a result, even customers earning the least have a high degree of satisfaction with TymeBank services.

TymeBank onboards around 220,000 customers per month with about 85% coming through kiosks, at an estimated acquisition cost of US$4 per customer, and roughly 16,500 coming via the internet at approximately US$0.60 per customer for acquisition.[34] Since TymeBank started operations in 2018, it has expanded to 8.3 million customers. It offers "a compelling example of how challenger banks can leverage digital technology to reach excluded customer segments with more affordable and useful products."[35] This can be done, according to a case study by CGAP, due to:

> "TymeBank's ability to maintain low operational costs ... due to the bank's technology and microservice architecture, its branchless model, and digitally facilitated onboarding ... TymeBank serves a higher proportion of low-income customers than the typical bank in South Africa, and a significantly higher portion of the most financially excluded segment. Young, rural, low-income women comprise the most financially excluded and underserved segment in South Africa. This group forms 2.3 percent of South Africa's banked population but 7 percent of TymeBank's active base. 13 percent of TymeBank's active customers are first-time bank customers [suggesting] TymeBank customers disproportionately seem to come from traditionally unbanked and underserved segments."[36]

[34] Jenik, Ivo, TymeBank Case Study: The Customer Impact of Inclusive Digital Banking, CGAP, January 2022, https://www.cgap.org/research/publication/tymebank-case-study-customer-impact-of-inclusive-digital-banking.

[35] Id.

[36] Id.

Unlike many banks, TymeBank offers a wide range of financial services to its customers across the economic spectrum. The bank achieves this by keeping its customer acquisition costs low by using cloud computing and storage services. As the bank has scaled up, the use of cloud technology means its infrastructure costs do not significantly increase, allowing it to maintain a small staff and not have to build its own data center for customer data storage and processing, as well as incur labor costs, locating and hiring cybersecurity experts, and constantly upgrading operations to respond to security threats. It could not stay in business without use of the cloud.

Even though the bank operates in a country, South Africa, which has a large enough economy to support some cloud computing, without access to international cloud providers in other countries, TymeBank could not obtain the full range of cloud services available. Nonetheless, it can still decide which countries hold its data in the cloud, in case any particular countries raise political, legal or technical concerns.

The presence of data localization laws has kept the bank from submitting banking applications and starting operations in some countries due to the regulatory burden imposed by those laws. As a result, those countries are deprived of the affordable, accessible financial accounts that TymeBank makes available to South Africans.

Fraud prevention is a critical bank function. With localization, fraud prevention would be more expensive, since the bank might not be able to participate in fraud-related information exchanges and thus benefit from learning how other firms have been attacked and how they responded. Similarly, inability to share cyber threat information could lead to high levels of losses.

Security of customers' data is critical, so the bank uses several techniques to protect data, commonly including both anonymization and encryption, when data is stored in the cloud as well as when its data is in motion between the cloud and its offices. However, on its own, it cannot replicate the security services that cloud providers can offer. The ability to institute a fraud solution for all the countries in which the bank operates keeps fraud costs down—something that would not be possible if cross-border data flow was restricted.

While it has been argued that without localization financial regulators might not have access to bank records, TymeBank's regulators have full supervisory access to the bank's data—simply by supervisors logging on to the cloud from the bank's offices.

Bottom line: Without localization, the bank can serve the widest range of customers at lower costs meeting its goal of providing affordable financial services. With localization, that would be impossible.

CASE STUDY 2.

JUMO is a “banking as a service” platform, enabling real-time access to funds at the lowest possible operating cost. JUMO is a multisided platform for mobile network operators and banks. It combines behavioral data from mobile usage and predictive technology to deliver low-cost financial products to low-income consumers and “those who own micro, small and medium enterprises who have previously been excluded from traditional banking services.”[37] It helps mobile network and eMoney operators create additional revenue streams by attracting new customers and increasing customer activity and engagement. Lower operating costs permit fair product pricing.

Integrating into JUMO’s platform enables financial partners to offer loans, savings and a wide range of financial choices to a new group of customers. JUMO operates in 6 African countries (Ghana, Tanzania, Kenya, Uganda, Zambia and Côte d’Ivoire) and has operational and tech hubs in Cape Town and Nairobi. Its platform has two distinct capabilities which work together to provide a full digital banking service: 1) technology which provides end-to-end, next generation banking infrastructure; and 2) a learning machine which analyses data to reduce the cost and risk of lending. It has served over 22 million people and small businesses, disbursing over $5 billion through 160 million loans. JUMO’s ability to work across borders has not only increased its efficiencies, but it also has some intangible benefits as well. It improves the ability to manage portfolios and get a holistic view of the marketplace. Access to cloud providers enables JUMO to scale quickly and increase the reliability of its services.

The presence of localization laws has led JUMO to not enter some smaller markets because it was not economical due to associated greater compliance costs. For instance, the data protection law in Rwanda led JUMO to shut down its partnership with a local telecommunications provider in 2018, due to the burden of the restrictions imposed. Setting up a data service just for Rwanda would have been too expensive, including the hiring of twice the number of portfolio management team members, significantly pushing up costs in a small market.

Cloud makes JUMO’s infrastructure cost effective. With the biggest operational cost being staff, working across countries facilitates efficiencies. JUMO’s business operates at scale—setting up different processors for a larger market might be worth the investment; but for smaller countries, like Rwanda, it would not. As a result, cloud access can be make or break. Consumers in smaller countries have a lot to lose from localization. With cloud services, JUMO can serve lower asset classes due to its low overhead. It is also beneficial to share data across borders in all countries in which JUMO operates, providing not only greater efficiency, but also intangible benefits. For instance, if their team sees more of what is going on, it can spot patterns both of opportunities and risks.

Bottom line: Smaller countries will lose investments and services if localization laws are adopted.

[37] Finnfund, Finnfund invests in financial services technology platform Jumo, https://www.finnfund.fi/en/news/finnfund-invests-in-financial-services-technology-platform-jumo/.

CASE STUDY 3.[38]

AWS offers cloud services—from infrastructure technologies such as computing, storage, and databases—as well as emerging technologies, including machine learning and artificial intelligence, data lakes and analytics, permitting customers, quickly, easily, and cost-effectively move existing applications to the cloud.

Economics

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.

Economies of scale apply not only to technology, but also security personnel and processes, resulting in unprecedented return on investment as compared to traditional systems. The [cloud service provider] CSP takes on a major portion of the security "surface area," executing with professional focus and skill. As a result, customers can refocus their security professionals and resources on a much smaller part of the challenge such as application security. Public cloud infrastructure as a service (IaaS) workloads will experience fewer security incidents than those in traditional data centers. Gartner's research estimates at least 60% reduction in security incidents.

There are also cascading socio-economic costs to limiting data flows, specifically on trade competitiveness and workforce development. As cloud technology becomes ubiquitous and more strongly tied to economic advancement, digital trade (and reducing the barriers to it) will become a higher priority for governments. Countries allowing free data flows will be at an advantage by accessing leading edge technology, which will in turn impact the modernization of commercial and public sector services, improve worker productivity, and accelerate local job and skills growth across sectors.

[38] AWS' comments below are derived from: Data Residency, AWS Policy Perspectives, August 2020, https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf; Garman, Matt, AWS Digital Sovereignty Pledge: Control without compromise, November 27, 2022, AWS Security Blog, https://aws.amazon.com/blogs/security/aws-digital-sovereignty-pledge-control-without-compromise/; Does data localization cause more problems than it solves?, AWS Innovating Securely, https://d1.awsstatic.com/institute/AWS-Sovereignty-and-Data-Localization-2022.pdf.

Impact on cross-border trade/startups

As businesses grow and expand outside regional operations, it is vital that they have access to resources that have a global reach. Through the use of cloud, for example, individuals and small to medium enterprises (SMEs) are able to access IT resources at a cost and scale once accessible only to entities with far greater capitalization. SMEs are primary drivers for new job creation. Cloud computing lowers the barriers for business creation and market access, enabling more start-ups to form, ultimately creating more jobs.

Data centers lag behind

Countries enforcing barriers to data flows can limit their citizens ability to take advantage of innovative services that improve their quality of life and government services delivery. For example, artificial intelligence and machine learning (AI/ML) applications require customized infrastructure for optimal functioning, and while global CSPs continue to expand their data center footprint, it is unrealistic to assume that data centers will be established in every country. Hence, as AI/ML is increasingly used to improve services, such as health care prognoses and weather forecasting for emergency preparedness, citizens in countries with strict data residency requirements will lag behind in accessing technological breakthroughs for citizen-related services.

Physical vs. cloud security

The physical location of data has little to no impact on threats propagated over the Internet. Internet-connected systems expose an organization to a broad threat space, all of which are propagated from any location. Regardless of the physical location, if IT systems are in any way connected to the Internet (or other multi-party networks), even indirectly, they are at considerable risk. Thus, restricting CSPs to one jurisdiction does not better insulate data from governmental access.

An unintended by-product of in-country data residency requirements is that threat actors can gain better accuracy in targeting systems knowing the data resides in specific locations. Restricting operations to specific in-country requirements would inhibit service innovation [regarding security] and hinder the ability to compensate for threats, such as ones that target availability.

Bottom line: Data localization is an ineffective solution at best, and harmful at worst … data localization rules are unnecessary for security and for local economic development. AWS encourages governments to consider the following policies to meet the security objectives associated with data residency:

1. Develop policies and requirements that allow for the use of out-of-country data processing facilities if the data is processed and stored in a modern, highly secure, hyperscale cloud[39] environment. Customers can also choose locations with data protection laws consistent with their own and where data transfer agreements are already in place.
2. Align national policies and regulatory requirements to the principle of free movement of data cross-border to effectively balance security, economic, and IT modernization goals.

Alternatives

Localization is far from being the only answer to the legitimate policy concerns regarding cross border flows of data. The following represent alternatives for a policy tool kit that could reduce the negative impact of localization on the poor:

Transparency: Localization is often built on a weak policy foundation. As part of a healthy debate, it is time for policymakers to be more transparent about their motivations for adopting data restrictions. There are legitimate concerns about data protection, cyber security, national security, etc., which could be debated in light of the impact decisions would have on the poor.

Balancing: To avoid unnecessarily imposing a localization "tax" on the poor, policy debates should balance the interests of the poor with other policy considerations, imposing the minimum amount of localization necessary. Given the limited economic benefits and potential detriments of localization policy, this would instead shift the discussion to how trusted and permissioned data flows cross border can be provided.

Privacy Enhancing Technologies: While encryption and anonymization may not always be a panacea, they can be an effective way of preventing unauthorized access to and use of personal data by hackers and foreign governments. It is worth keeping in mind that the major cloud providers spend countless millions of dollars on data security for their systems as safeguarding information is key to having customers entrust them with valuable data. Rather than using the blunt instrument

[39] Large-scale, multinational cloud service providers (CSPs).

of data localization, laws and regulations could require that privacy enhancing technologies[40] be employed when data leaves the country. This could prevent foreign governments, as well as cloud providers, from accessing data stored in their country.

Contracts: GDPR has long relied on contractual commitments as one basis for insuring the adequacy of data protection. In the localization context, it would be possible to have all parties handling the data assume contractual liability for how it is used and shared. There would be enforcement, jurisdictional challenges and choice of law questions, but that is true of GDPR compliance contracts as well.

Liability: Companies that export data could be held legally liable for misuse of the data while abroad. This could provide a strong incentive to ensure the protection of the data while giving the exporter flexibility in how prevention of misuse can be managed.

Adequacy Findings: In some cases, to promote trusted and permissioned data flow, it would make sense to assign responsibility to regulators to create white or black lists of countries with which data could be shared.[41] Regulators may have a greater ability to evaluate legal regimes in multiple other countries than would small to medium size enterprises. The decisions authorizing or restricting data flow could be based on: legal environment and risks; data processing storage mechanisms; data security measures, past experiences, and access to judicial redress. It is worth monitoring regulators' use of this authority to prevent an overly protective approach that could become a de facto localization regime.

Free Data Zones: One option would be for Africa (and other regions) to create a free data zone among African countries that have data protection equivalency to allow for easy cross-border flows of data. It could also create a market demand for continent-wide cloud services. This might creative an incentive for African countries that don't have strong data protection laws to adopt or improve existing laws to meet an adequate standard of protection. Time will tell whether the Malabo Convention will provide a mechanism for achieving multi-country data protection adequacy. This might also spur a common digital market that would help shape a safe, inclusive, and equitable digital future for the continent.

[40] Examples of Privacy Enhancing Technologies beyond encryption and anonymization include: differential privacy, synthetic data, homomorphic encryption, federated learning, multi-party computing, zero knowledge proofs, and trusted execution environments. See Emerging Privacy Enhancing Technologies Current Regulatory and Policy Approaches, OECD Digital Economy Papers, March 2023 No. 351, https://www.oecd-ilibrary.org/docserver/bf121be4-en.pdf?expires=1698244450&id=id&accname=guest&checksum=C0A4876EB4CEEB0588FCFEF6A1D0E48F.

[41] See, e.g., State Bank of Pakistan Framework on Outsourcing to Cloud Service Providers, Section E, https://www.sbp.org.pk/bprd/2023/C1-Annix-A.pdf; https://propakistani.pk/2023/01/18/sbp-sets-criteria-for-outsourcing-regulated-entities-workload-to-cloud-providers/.

Provisions for Supervisory Access: Supervisors have a recognized need to review data held by supervised entities. If data is held by foreign cloud providers in a way that thwarts supervisory access, that would be problematic for the country's financial system and the protection of customers. Fortunately, there are secure ways to provide supervisors and other enforcement agencies with data access in this context, such as being able to log into the supervised entities' cloud accounts to review and download data. Providing such access could be a regulatory prerequisite to use of cloud services.

Conclusion

Localization policies impose costs—effectively a "tax"—on the ability to deliver affordable products and services to the poor. Localization is also built on a weak foundation. Many of the rationales on which it is based, such as data protection and security, are just pretexts for other interests, including state surveillance. Policymakers may think with data localization that they are boxing out big international firms when, in fact, they are really crippling startups and hindering innovation in their economic ecosystem. As the ITIF has observed, the "pursuit of control is costly and ultimately counterproductive."[42]

The growth of localization laws as been dramatic, though there is a hint of movement away from them, such as in Saudi Arabia. It is time to reverse the trend and move away from data localization laws which have a significant negative impact on the poor without comparable countervailing benefits. Instead, policymakers should consider other tools that address legitimate concerns about cross border data flow that provide trusted and permissioned data flow including potentially developing international standards and entering trade deals. Regulators often have a legitimate need to access customer data held by entities under their jurisdiction. Guarantees of access to such data—regardless of its location—should be put in place. Security concerns can be address through use of encryption and other technologies.

There is an exciting opportunity to take the efforts in Africa to establish a free trading zone and expand them to include creation of a free data zone as well which—if continent-wide—could create a powerful market for cloud services—including incentivizing African cloud service providers by creating a large market for their services. GDPR has demonstrated that a regional approach to data localization in the EU is more sensible for localization than individual countries. Creating a free data zone in Africa would establish a strong data market for the exchange of data with EU and APEC countries and encourage mutual recognition by those regions of the growing data protections in Africa. Free data movement should be included in all future trade agreements to create a safe, inclusive and equitable data environment for the continent.

[42] Cory, Nigel, Luke Dascoli and Ian Clay, ITIF 2022 Report: The Cost of Data Localization Policies in Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam, December 12, 2022, https://itif.org/publications/2022/12/12/the-cost-of-data-localization-policies-in-bangladesh-hong-kong-indonesia-pakistan-and-vietnam/.

Localization is usually the wrong answer to legitimate data policy issues. As a result, data transfer restrictions wind up imposing unnecessary costs on providers, such as banks, which effectively serves as a tax which is either passed along to the poor or, even worse, makes it uneconomical for firms to serve poor customers. At minimum, the impact of localization on the poor should be an integral part of the policy debate, along with consideration of alternatives that would mitigate its impact. The impact on the poor should be weighed heavily by policymakers in deciding whether to impose localization and, if so, impose the lightest version of localization only if it meets compelling national policies.