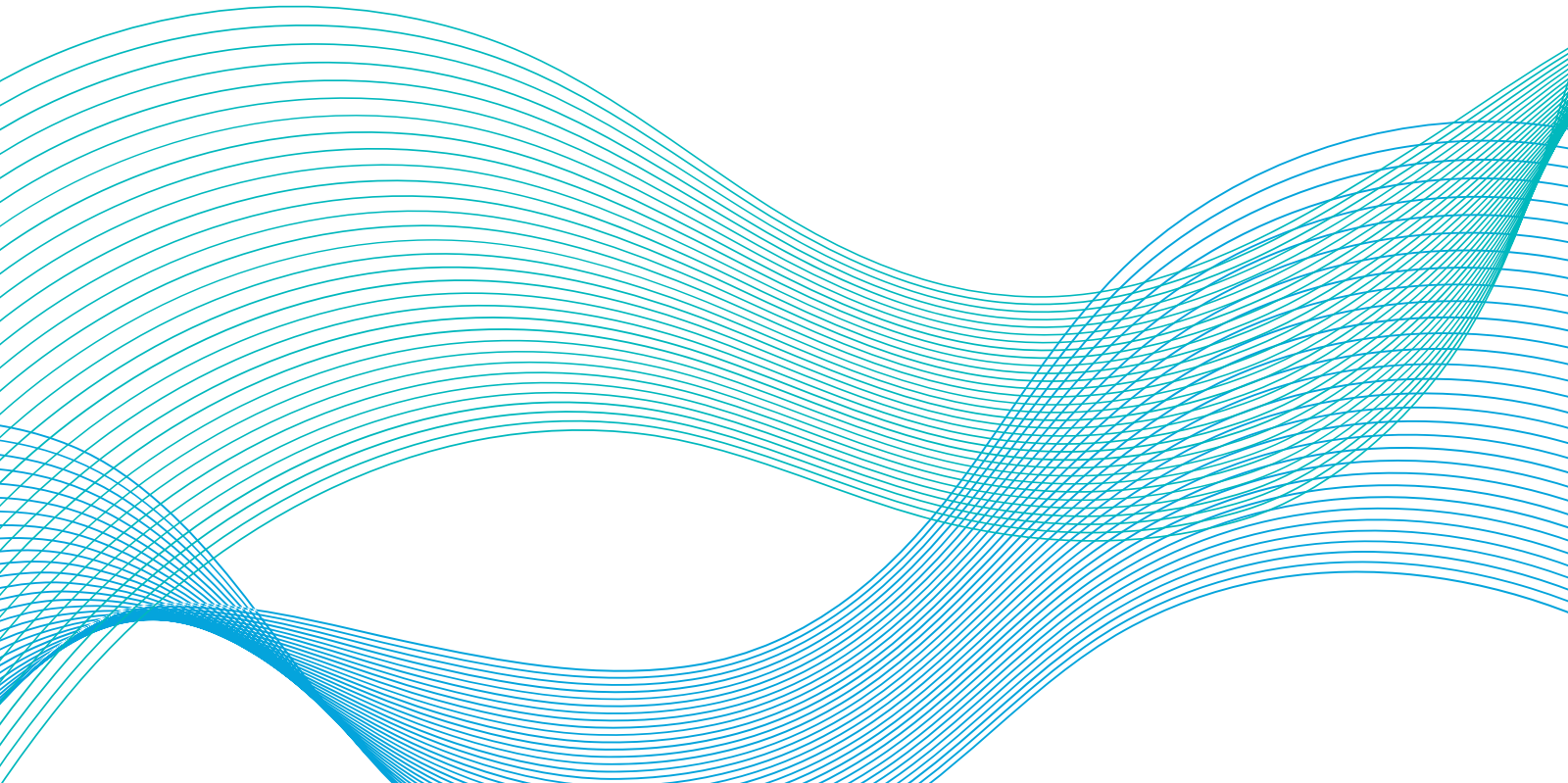
Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

PRIVACY ACROSS BORDERS

The "Real Life Harms" of Data Localization Policies

Discussion Paper 1

March 2023



The "Real Life" Harms of Data Localization Policies

March 29, 2023

The Centre for Information Policy Leadership (CIPL) and Tech, Law & Security Program (TLS) have been collaborating on a project regarding data localization policies. As data localization is increasingly gaining traction, we seek to understand the different dimensions of the impacts and effectiveness of these policies. As part of this collaboration—CIPL has published the present paper on the "real life" business, societal, and consumer impacts of data localization policies and TLS has published another paper on whether data localization measures are legally effective in achieving one of their main ostensible purposes, i.e., to prevent foreign government access to data.

I. Executive Summary

Data underpins the digital transformation of our economies and society. It can be considered one of the most valuable economic assets – responsible use of data enables economic growth and brings benefits and progress to people, governments, and societies at large. Data is also central to governmental and societal interests, such as national security, cyber security, data protection, privacy, and other individual rights.

As policymakers around the world have come to understand both the substantial opportunities and risks associated with data use and innovation, some have started pursuing "data localization" policies, including explicit requirements to store data in the jurisdiction it was collected in and restrictions on transferring data to other jurisdictions. Many of these policies purportedly enable new or increased government access to or greater control over data—particularly personal data, but increasingly also non-personal data. Taken to their logical extremes, certain data localization approaches could result in the interruption or termination of cross-border data flows and create substantial harm to individuals and society in the process. Simply put—the benefits that governments are seeking from data localization policies do not outweigh the harms, and localization may not even achieve the objectives for which it is instituted.

Before continuing down the path of data localization, it is vital for policymakers to recognize the consequences of such policies, and to better understand the economic and societal harms that terminating or severely limiting cross-border data flows could bring about. It is particularly important to consider these harms not only in the abstract, but in terms of the tangible degradation or loss of many digital services and business functionalities that rely on cross-border data flows.

To provide evidence of the unintended consequences of such excessive data localization policies, the Centre for Information Policy Leadership (CIPL) has been working with businesses, scholars, and other privacy and data leaders to better understand the potential functional and operational harms that could arise if more and more countries adopt data localization approaches that interfere with cross-border data flows. This is the first in a series of CIPL papers that we expect to publish in 2023 that discusses the impacts of data localization approaches, the motivations behind them, and how to respond to and move beyond them.

Based on these discussions, CIPL offers the following considerations:

1. Data localization reduces the effectiveness and viability of **business functions** that are critically important for organizations and the people they serve. These include:
    - **Cyber security-related tools and services**, such as threat detection, which rely on cross-border data flows that include personal data;
    - **Human resources systems** necessary for day-to-day operations of multinational companies;
    - **Fraud prevention services**, such as anti-money laundering, counter-terrorism financing, anti-bribery and corruption, and know-your-customer;
    - **Manufacturing operations** and end-to-end lifecycle management solutions to monitor for issues and update products; and
    - **Customer services** that enable round-the-clock support.
2. **Data localization creates impediments to individuals' access to beneficial products, services, and activities, such as:**
    - **Cloud computing services** that offer cost efficiencies and data protection resilience;
    - **Financial services** such as banking, lending, and payment services, including mobile payment applications;
    - **Cross-border research collaboration,** such as medical studies, which sometimes requires identifiable personal information;
    - **5G telecommunications infrastructure** that rely on a multi-cloud strategies and specialized tools and skills;
    - **Social media services and communication tools**, including video conferencing and audio translation, that allow people across the world to communicate and connect; and
    - **Modern farming technology**, which allows farmers around the world to connect with each other and share insights that help them respond to various challenges, including extreme weather.

II. Data Localization on the Rise

The concept of "data localization" in this paper refers to a range of policies requiring or causing data to stay in the jurisdiction in which it was created or collected. Policies can vary in the kind of data they target;

some countries have strict policies requiring that all data originating in the country remain on servers in the country, while others focus on personal data. [1] This paper is directed at policies targeting cross-border flows of personal data, including those that do not explicitly require localization of personal data but could result in the restriction or elimination of cross-border flows of personal data.[2] Thus, this paper uses "data localization" as an umbrella term for:

> (i) requirements in laws, regulations, or policies to store and manage data only locally, or prohibit international data transfers;[3]
>
> (ii) requirements in laws, regulations, or policies to store data in the original jurisdiction, but allow copies of the data to be transferred if certain requirements are met;[4] and
>
> (iii) de facto localization requirements, i.e., laws, regulations, or policies that impose restrictions and conditions on the data transfers, which make it difficult or impossible to transfer data outside the jurisdiction. Such conditions include the use of certain prescribed transfer mechanisms, or a demonstrated absence of transfer risk.[5]

---

[1] For example, Article 37 of the Cybersecurity Law of the People's Republic of China read in conjunction with Article 40 of the Personal Information Protection Law requires critical information infrastructure operators to store personal data *and* important data generated from critical information infrastructure in China. Also, the Data Act, proposed by the European Commission, places rules on the access and international transfer of certain non-personal data.

[2] This includes strict interpretations by courts or data protection authorities of the conditions under which personal data may be legally transferred across borders—for example, a requirement that individual organizations undertake "transfer risk assessments" or "local law assessments" to determine whether the destination jurisdictions provide an essentially equivalent level of protection for personal data as the originating jurisdiction. Transfer risk assessment requirements may lead organizations to stop data transfers for a number of reasons, including administrative burdens, legal uncertainty, or out of an abundance of caution. This may cause the unnecessary cessation of compliant cross-data flows.

[3]Article 29 of the Kingdom of Saudi Arabia's Personal Data Protection Law (PDPL) prohibits the transfer of personal data outside of the Kingdom unless the transfer does not prejudice national security or vital interest of the Kingdom, there are sufficient guarantees for preserving the confidentiality of data, the transfer is limited to the minimum personal data needed, and the competent authority approves the transfer. Proposed amendments have postponed the PDPL from entering into full effect; amendments include additional grounds to allow the transfer of personal data outside the Kingdom. See Saudi Arabia Issues Amended Data Protection Law for Consultation, Brian Meenagh & Lucy Tucker, Latham & Watkins Global Privacy & Security Compliance Law Blog, 24 November, 2022.

[4] For example, Russian Federal Law No.242-FZ requires that the processing of personal data of citizens be performed through database servers located in the Russian Federation. Nevertheless, the regulator has published a non-binding opinion that duplication or mirroring databases can be located outside Russia if the original databases are located in Russia and all other conditions for cross-border transfer of data are met (e.g., obtaining consent from data subjects or having a data transfer agreement in place).

[5] For instance, the EU General Data Protection Regulation (GDPR) contains a restriction on transfers of personal data to third countries. *See* Chapter V, GDPR. Furthermore, in C-311/18 "*Data Protection Commissioner v Facebook Ireland Limited and Schrems*" (*Schrems II Judgment*), the European Court of Justice decided that while the controller-processor Standard Contractual Clauses (SCCs) are valid, the transferring entity must conduct an impact assessment in advance on a case-by-case basis to verify that transferred data will be adequately protected in the recipient country. This includes an assessment of the laws of the third country, the existence of any independent supervisory authority, any international commitments made by the country, and technical measures used to protect the

It is important to acknowledge that some of the underlying objectives that governments use to justify data localization are understandable. Countries cite national security, economic interests, and "digital sovereignty" as justifications for data flow restrictions.[6] In short, data localization can be seen as reflecting countries' desires to ensure that their own rules and values are the ones governing cyberspace within their own borders.

Motivations notwithstanding, data localization policies have had limited utility in achieving their stated objectives and can instead impede economic and societal progress, by curtailing production and delivery of many digital products and services that are valuable and important to people around the globe.

Numerous studies over the past decade have described the harms of data localization in terms of economy-wide impacts such as output, trade, and productivity.[7] In a global economy that is being rapidly digitalized and that depends on cross-border data flows, data localization clearly has significant economic costs for a variety of reasons.[8] They range from businesses having to duplicate staff, data sets, data center infrastructure, and other technology in each of the localizing jurisdictions, to costs of lost business opportunities, and contraction of the available markets as a result of diminished data flows.

In this paper, we move beyond economy-wide analyses to explore more visible, common and concrete impacts of impediments to cross-border data flows on businesses and individuals. We examine how data localization affects critical business functions such as cybersecurity and fraud or crime prevention, as well as cases where it may *degrade or impede production and delivery of service*s that people value and rely upon, such as ride-sharing applications, communications platforms, and around-the-clock customer service.

---

transferred data. *See also* Chapter V of the Brazilian General Personal Data Protection Act (LGPD) which provides for a similar transfer mechanisms as the GDPR.

[6] Digital sovereignty refers to a country's ability to control its economic, security, law enforcement, and other interests vis-à-vis digital technology. See France's Macron lays out a vision for European 'digital sovereignty', Ryan Browne, CNBC, 8 December, 2020), available at https://www.cnbc.com/2020/12/08/frances-macron-lays-out-a-vision-for-european-digital-sovereignty.html. See also Country's Data Sovereignty Cannot Be Compromised: Ravi Shankar Prasad On Data Localisation, Kritti Bhalla, *Inc42, 23* September, 2019, available at https://inc42.com/buzz/countrys-data-sovereignty-cannot-be-compromised-ravi-shankar-prasad-on-data-localisation/.

[7] For instance, the Information Technology and Innovation Foundation (ITIF) has found that a 1-point increase in a nation's data restrictiveness results in a 7 percent decrease in its gross trade output, a 2 percent decrease in its economy-wide productivity, and a 1.5 percent increase in its prices of goods and services among downstream industries. Additionally, research conducted by the European Center for International Political Economy found that enacted or proposed data localization policies in China would cost as much as 1.1 percent of its Gross domestic product (GDP), reducing domestic investment by 1.8 percent, exports by 1.7 percent and welfare by the equivalent of 13 percent of each citizen's salary. *See* Erik van der Marel, Hosuk Lee-Makiyama, Matthias Bauer, "*The Costs of Data Localisation: A Friendly Fire on Economic Recovery,*" Europe Center for Information Political Economy, May 2014. *See also* Nigel Cory 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.

[8] Digital Globalization: The New Era of Global Flows, McKinsey Global Institute, 2016, available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.

III. Use Cases of Data Localization's Harms

Data localization disrupts and undermines critical business operations, like cybersecurity and fraud detection, and degrades or eliminates various digital products and services. Even if some organizations can adjust to the onerous requirements imposed by data localization policies, many are not able to.[9] Organizations leaving a jurisdiction take expertise and investment capital with them, along with their product and service offerings.

While this paper focuses on data localization policies that target personal data, it is not always possible to separate personal from non-personal data and, in those cases, organizations may be compelled to apply the transfer restrictions to the entire data set. Because of this, organizations handling large amounts of non-personal data may also be impacted by data localization rules centered on personal data. Finally, some jurisdictions have been considering cross-border requirements and conditions for transferring non-personal data, following similar approaches to those used for personal data.[10]

The following sections highlight select examples and case studies of key business functions, as well as products and services that may be undermined, degraded, or eliminated by data localization. The examples are not intended to be comprehensive but rather to demonstrate the breadth and diversity of impacts.

A. ***Degrading of Critical Business Functions***

Data localization would have a negative impact on the following critical business needs and functions, as it would significantly degrade their effectiveness and ultimately reduce their viability:

Cybersecurity:

- Data localization will limit the effectiveness of cybersecurity-related tools and services, such as threat detection systems. For example, Cloud Service Providers (CSPs) generate trillions of signals obtained through various data sets worldwide that enable them to identify bad actors and specific malicious actions, e.g., botnets and malware.[11] Many CSPs monitor a range of personal data, including IP addresses and user activity (like password resets and account privilege modifications). They need the ability to collect, analyze, gather insights, and share that information within their own organizations, with clients, with other CSPs, and in some cases with law enforcement across multiple jurisdictions in order to effectively identify and address cyber threats.

[9] A business will assess whether revenue potential can cover the cost of compliance to determine whether it can continue operations in a jurisdiction with data localization requirements. See *Case studies: a balancing exercise of the cost of compliance against revenue opportunities,* "How the trend towards data localization is impacting the financial services sector", International Regulatory Strategy Group, 49, December 2020, available at https://www.irsg.co.uk/assets/Reports/IRSG_DATA-REPORT_Localisation.pdf.

[10] For examples, *see* Article 27 of the proposed EU Data Act and the draft National Data Governance Framework Policy in India.

[11] *See* "*The Effects of Data Localization on Cybersecurity*", Peter Swire and DeBrae Kennedy-Mayo, Georgia Tech Scheller College of Business Research Paper, pages 7-8, 18 February 2022, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4030905.

- An information system's security depends on a plethora of controls and a system's overall reliability and resiliency, not simply on the physical location of a data center. Data localization rules may impede organizations' ability to access state-of-the art cybersecurity applications. The International Regulatory Strategy Group (IRSG) shared the example of a company that was prevented from deploying its preferred data loss prevention software in Luxembourg because the provider was located outside the country and the company would have had to transfer and store data outside Luxembourg.[12]

Human Resources Data:

- Data localization interferes with the operations of multinational companies that must be able to transfer human resources (HR) data across borders to their central HR department, to their centralized IT systems, to internal and external payroll and other service providers. Data transfers of HR data are indispensable for recruitment and management of a global workforce—without ability to share data, companies would not be able to operate in multiple jurisdictions and bring economic and societal value to multiple countries.

Fraud Prevention:

- Data localization rules compromise the tools and services used by financial institutions to detect and prevent payment fraud, money laundering, and other financial and transactional crimes. The effectiveness of anti-money laundering, counter-terrorism financing, anti-bribery and corruption, know-your-customer, and other functions depends on access to comprehensive personal data distributed across multiple jurisdictions. Cutting these services off from global data flows will diminish their accuracy and dependability. This will have profoundly damaging ramifications for the safety and security of individuals who rely on financial services and institutions.[13]

- Data localization can also prevent businesses from using certain fraud prevention tools, like spam detection and human verification tools, because their functionality may require cross-border data transfers. Effective fraud detection tools require global data sets in order to perform accurate data analytics, or at least some level of cross-border data transfers. If a localizing country does not allow any personal data from within to be included in global fraud detection tools, anti-fraud measures will become less reliable. As data needs to be analyzed together as a whole in order to spot patterns of fraud, leaving out data from the analysis will deprive the models of the training required to accurately detect fraud and potentially create even greater vulnerability in the localized jurisdiction. The creation of data-walls around more countries and the promotion of prohibitions on the transfer of data will ultimately mean that each country will only be able to identify local patterns of fraud, and will be blind to wider fraud patterns and threats. Localizing

[12] *See* "How the Trend Towards Data Localisation is Impacting the Financial Services Sector," International Regulatory Strategy Group (IRSG), 54, December 2020, available at https://www.irsg.co.uk/assets/Reports/IRSG_DATA-REPORT_Localisation.pdf.

[13] *See* Financial Data Localization: Conflicts and Consequences, Future of Privacy Forum, December 2017, available at https://fpf.org/wp-content/uploads/2017/12/FPF_Bank-Regs_illo_01.pdf#:~:text=Modern%20banking%20customers%20are%20global%2C%20and%20expect%20on-demand%2C,result%20in%20unintended%20consequences.%20Let%27s%20take%20a%20look%3A.

countries risk becoming safe havens for bad actors whose personal data may be protected from global fraud detection tools. Because the nature of the internet allows illicit actors to harm individuals anywhere in the world, bad actors in localizing countries could operate under the radar. This will decrease individual trust on digital platforms around the world. Concerns about such abusive use of computing infrastructure motivated, in part, the United States' January 2021 Executive Order on Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-enabled Activities.[14]

Manufacturing:

- Data localization requirements would restrict manufacturers' ability to use end-to-end lifecycle management solutions by limiting information exchange (including the personal data of employees) among project teams located across the globe. For example, an automobile manufacturer would be unable to use thorough customer usage information, including personal information such as location and biometric data, to coordinate the maintenance and development of its vehicles.[15] Additionally, airplane, truck, and bus manufacturers collect and analyze data from international operations to monitor for maintenance purposes and reduce transportation's environmental impact. While much of this data is non-personal, data sets that commingle non-personal and personal data may be subject to privacy-related localization requirements. As a consequence, manufacturers could face production delays and their customers would experience reduced quality and longer waiting periods.[16]

Customer Service:

- Customers in a wide range of services—including banking, insurance, travel, online retail, and health care, among others—expect customer and tech support to be available 24 hours per day, seven days per week. Data flows enable organizations to establish geographically dispersed customer service facilities to provide support at times most convenient to customers and customer service employees located across a variety of time zones.

B. Impediments to Beneficial Products, Services, and Activities

Data flows are critical to many products, services, and activities—some obvious and some perhaps more surprising. This section describes how obstacles to cross-border data flows would deprive people of many basic benefits and services that they have come to rely on and may ultimately cause harm.

---

[14] Federal Register: Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber- Enabled Activities, 25 January 2021, available at https://www.federalregister.gov/documents/2021/01/25/2021-01714/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious.

[15] *See* Data in Your Car, National Automobile Dealers Association and Future of Privacy Forum, 2017, available at https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf.

[16] For in-depth discussion of specific examples, see this roundtable hosted by the Wilson Center and Coalition of Services Industries on Redefining Manufacturing: The Service Sector's Role in Boosting U.S. Competitiveness and Resilience, 19 June 2017, available at https://www.wilsoncenter.org/event/redefining-manufacturing-the-service-sectors-role-boosting-us-competitiveness-and-resilience.

Cloud Computing Services:

- Data localization rules, which require the storage of data on local servers, may prevent businesses and individuals from accessing and enjoying the full benefits of global cloud computing technologies.[17] Global CSPs offer individuals and organizations several benefits, including cost efficiencies, resilience, and high-standard cybersecurity protections.[18] For example, global CSPs are configured with operational flexibility to work around disruptive events like power outages that can impact broad geographic areas. Local services unable to re-route data to back-up servers distributed around the world could be compromised by a similar situation.[19] In addition to these vital redundancy benefits, cloud computing services enable geographically distributed business to exchange data seamlessly across a shared infrastructure. CSPs also enable smaller businesses to access powerful data storage, processing, and analytics tools that would otherwise be unavailable to them.

- In situations of geopolitical conflict, consolidation of data in one region or country can elevate risks from physical attacks. The Ukrainian government took action to address such vulnerability just before Russia's invasion in February 2022. Previously, Ukrainian law required data localization of certain government and private sector data. Anticipating an escalation, the Ukrainian parliament passed legislation to allow this data to be moved to the cloud. This allowed the Ukrainian government to work with private cloud service providers to transfer critical government, tax, banking, education, and property data to the cloud. Rather than keep Ukraine's critical data in servers in Ukraine, which were in direct danger of disruption or destruction, cloud service providers have been able to distribute this data securely and safely around the world.[20]

[17] For instance, the French National Cybersecurity Agency's revised cybersecurity certification and labeling program (SecNumCloud) limits corporate ownership by specifying that non-EU shareholders cannot possess more than 39 percent of a company providing cloud services in France. Beyond SecNumCloud, a cloud provider must also have its servers physically in France. See, "Sovereignty *Requirements in France - And Potentially EU - Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade and Digital Cooperation Among Likeminded Partners*", Nigel Cory, Cross-Border Data Forum, 10 December 2021, available at https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi/.

[18] In some cases, officials who have expressed a preference to use local cloud service providers have determined that only global CSPs are currently able to offer requisite cybersecurity protections. See Politico Pro Morning Tech, Gian Volpicelli, 2 March 2023, available at https://pro.politico.eu/news/politico-pro-morning-tech-adieu-rt-microsoft-and-the-hub-tiktok-clapback (access requires subscription).

[19] Due to regulatory and compliance requirements, some global cloud service providers have started localizing personal data within certain jurisdictions, including through ventures with local partners. However, these solutions are more feasible in major economic regions, like the EU, where cloud service providers can reliably establish new data centers and recruit employees to support region-based operations and support needs. Even in those instances, such requirements place significant financial burdens on businesses, which may ultimately impact access. The quality of potential local partners may vary, as well, with potential impacts on the range of services or functionalities available to end users.

[20] See Defending Ukraine: Early Lessons from the Cyber War, Microsoft, 5, 22 June 2022, 5, available at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

Financial Services and Inclusion:

- Cross-border data flows enable individuals around the world to access a wide range of financial services, from banking, to lending, to payment services such as credit cards, and phone-based payment applications. Networks that banks and payment systems use to interoperate, such as SWIFT, depend on cross-border data flows to function. Data flows are also critical to the functioning of blockchain and other distributed ledger technologies[21] which have found diverse financial service applications.[22] For example, blockchains are finding numerous applications for fostering global trade, with specific uses for trade finance, supply chain finance and management, and customs operations. Early evidence suggested that the COVID-19 pandemic accelerated the adoption of blockchain-based trade solutions.[23]

- Data flows have played an especially important role in developing countries in fostering financial inclusion, including facilitating cross-border remittances, access to finance, e-commerce, and development of new products and services, as profiled in the World Bank's *World Development Report 2021*.[24] Blocking data flows puts these benefits at risk for consumers and entrepreneurs in developing countries.

E-Commerce:

- E-commerce enables businesses of every size to reach customers, and customers to discover and purchase goods that they might be unable to find otherwise. This is especially true for customers and businesses connecting as research suggests that online marketplaces reduce "information frictions" that would otherwise create substantial blockers to cross-border trade.[25] These barriers are especially pronounced for small businesses that lack the resources to connect with overseas customers through their own channels.

Education, Medicine, and Research:

- **Education Tools and Services** – Data localization requirements could negatively affect educators and students at schools and universities using education technology ("EdTech") applications, which often rely on a global network of providers to support, maintain, and secure their services. For instance, service providers, at minimum, require the contact details of students, teachers and

[21] *See* CIPL Discussion Paper on Digital Assets and Privacy, January 2023, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_discussion_paper_on_digital_assets_and_privacy__19_jan_2023_.pdf.
[22] *See* Blockchain, U.S. Government Accountability Office (GAO), March 2022, available at https://www.gao.gov/assets/gao-22-104625.pdf; see also Blockchain for Financial Services, IBM, available at https://www.ibm.com/blockchain/industries/financial-services.
[23] *See* Blockchain & DLT in Trade: Where Do We Stand?, Deepash Patel and Emmanuelle Ganne, November 2020, available at https://www.wto.org/english/res_e/booksp_e/blockchainanddlt_e.pdf.
[24] *See* "World Development Report 2021: Data for Better Lives," World Bank, Chapter 3, available at https://openknowledge.worldbank.org/server/api/core/bitstreams/11590f3a-690f-5337-b2dd-fe0bfc1481c2/content.
[25] *See* "There Goes Gravity: How Ebay Reduces Trade Costs," Andreas Lendle, Marcelo Olarreaga, Simon Schropp, and Pierre-Louis Vézina, CEPR Discussion Paper No. DP9094, 28 September 2012, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2153544.

faculty members using the service to provide a platform for exchanging image, audio or text messaging. Additionally, popular education platforms access personal data to monitor for fraud and address technical issues. Finally, the rapid adoption of online education services and distance learning has brought easier access to education in many communities around the world. With geographically dispersed students, teachers, resources and tools, these services are, by default, relying on cross-border data flows and could not operate otherwise.

- **Medical Tools and Services** – Similarly, restrictions on data transfer would likely undermine the use of critical medical tools and services, such as 24/7 X-ray analysis, remote surgery, and collaboration among medical professionals and institutions across the globe. Some medical devices, including some cardiac monitors, depend on cross-border data flows to do real-time monitoring and analytics to predict and prevent health crises.[26] In the absence of free data flows, users from countries with data localization policies might be unable to access some of these services.

- **Research** – Data localization may hamper academic and scientific research by restricting access to personal data from jurisdictions that require localization. While anonymized or deidentified data sets are useful for many research purposes, some medical research requires the use of identifiable personal information. Unfortunately, data localization policies are already affecting innovative medical studies, including studies involving patients in dire need, by creating obstacles to cross-border transfers of personal data. For example, researchers from the European Union and European Economic Area ceased to cooperate in a research consortium led by the U.S. National Institutes of Health's National Cancer Institute due to concerns that doing so would involve cross-border data transfers inconsistent with the GDPR.[27]

Telecommunications Infrastructure Services:

- By eliminating cross-border data flows, data localization rules would undermine the operation and maintenance of 5G telecommunications infrastructure. 5G technology requires specialized tools and intellectual skills that cannot always be found in a local jurisdiction. For example, since networks are dynamic, scalable, largely software-driven and decentralized, many operators use a multi-cloud strategy and cloud-native network functions, often procuring services from multiple vendors across the globe. Data localization could prevent users from accessing cutting-edge services dependent on such infrastructure. Even if infrastructure providers invest in local data centers, such compliance efforts will eventually hurt users by increasing prices and limiting certain features.

Communication Platforms:

- **Social Media Services** – Data localization could impact individual choices and access to social media applications by limiting the availability of certain applications or services within localizing countries. This would effectively prevent people from maintaining and participating in global

[26] *See* "Medical Technology," Global Data Alliance, available at https://globaldataalliance.org/sectors/medical-technology/ (accessed 24 March 2023).
[27] *See* "International Sharing of Personal Health Data for Research," ALLEA, EASAC and FEAM, 25, April 2021, available at https://allea.org/wp-content/uploads/2021/03/International-Health-Data-Transfer_2021_web.pdf.

social networks, from general interest networks to specialized ones, e.g., for specific affinity groups or dating. The harms include inability to build and maintain personal and professional relationships across national borders, engage in free expression on global platforms, and access information from diverse global viewpoints. Social media allows people around the world to connect with friends, colleagues, and family; data localization would weaken these connections. Additionally, small businesses increasingly rely on social media platforms to reach and communicate with customers. Data localization will hinder the ability of small businesses to leverage cost-effective resources that are available to them on global social media platforms and thus endanger their access to new and wider markets and customers.

- **Video Conferencing** – Data localization rules would undermine the effective use of video conferencing platforms around the world, which routinely exchange personal data such as names and IP addresses. Individuals may no longer be able to register for global online webinars, record online meetings, or access certain video conferencing tools, nor would they be able to rely on these tools operating smoothly and securely.

- **Audio Translation –** Data localization rules would create unnecessary and prohibitive costs for video conferencing platforms that offer translation services in real time. Currently, translation service providers convert live speech into translated text by relying on a central database of languages. By restricting global data flows, data localization rules would require platforms to create a separate speech database within each localizing jurisdiction. As a result, individuals may experience a decrease in quality and accuracy of audio translation services, or lack of availability altogether.

- **Content Moderation** – Online service and application providers utilize certain tools and instruments to comply with their content moderation obligations and the growing body of law regulating online content and safety, such as the EU's Digital Services Act, the United Kingdom's Online Safety Bill, and Australia's Online Safety Act. These tools may become less effective through the proliferation of data localization. For example, in the United States, service providers are required to report Child Sexual Abuse Material to National Center for Missing & Exploited Children and share the relevant information with law enforcement.[28] In that regard, service providers generally rely on information sharing and tools that may not be available domestically. Under data localization regimes, service providers would not be able to effectively use their existing global content moderation systems, including globally distributed teams that help provide 24/7 moderation, and information sharing channels to detect and monitor illegal content.[29]

Streaming Entertainment:

- **Audio and Visual Content Services:** Cross-border data flows enable people around the world to enjoy movies, television shows, music, podcasts, and other audio and video content delivered over streaming services. Multi-country services have enabled audiences to explore content from

[28] 18 U.S. Code § 2258A.

[29] *See* supra note 11, at 23.

other cultures that was previously difficult to access—as in the United States, where streaming services have spurred the growth in popularity of television dramas from Korea.[30]

- **Video Games:** Data localization risks fragmenting the global video game industry, limiting the ability of video gamers to interact with players in other countries. Modern video game companies collect various types of personal data to deliver their services as safely and effectively as possible. Also, game developers would have difficulty providing access to their game in countries with strict data localization policies because foreign developers will need to maintain access to certain kinds of personal data to detect technical and security glitches and monitor for cheating or illegal or harmful behaviors.

Travel and Ride-Sharing Applications:

- **Ride-Sharing Applications** – Data localization would prevent users of a ride sharing app from using its features when traveling to another jurisdiction because trip history, user ratings, and user preferences could not be transferred. This would impair the application's effectiveness and user friendly design of the service; users would need to re-establish their accounts (including their trustworthiness and preferences) in each jurisdiction, and drivers would be unaware of prior customer history and account suspensions. Moreover, transfer restrictions might undermine key customer security and safety features, such as the ability to access customer reviews and driver ratings through one global application and derive insights from pooled historical data.

Farming:

- Data localization requirements could prevent farmers, large and small, from enjoying the benefits of global digital farming platforms that provide agricultural advice (e.g., which fertilizer to use and at what frequency). While farming has historically been a fragmented endeavor, modern technology allows farmers around the world to connect with each other and share insights that help them respond to various challenges, including extreme weather.[31] Although much of this data may be non-personal, it is often commingled with personal data such as location and end-user device information. Data localization will limit the benefits of digital farming platforms by preventing farmers in localizing countries from connecting with farmers outside their country and accessing insights that may benefit their harvest and livestock. Conversely, farmers in non-localizing jurisdictions will be unable to access information from countries with data localization policies. This can unnecessarily cause loss of harvest and livestock and financial harm to farmers.

[30] *See* These Black Women are Obsessed with Korean TV Dramas. Here's Why, Soo Youn, *Washington Post*, 14 September 2022, available at https://www.washingtonpost.com/lifestyle/2022/09/14/black-women-korean-tv-drama-k-drama/.

[31] *See* "Farm to Table: John Deere and Data in Precision Agriculture," C. Williams, Harvard Business School Digital Initiative, 12 November 2019, available at https://d3.harvard.edu/platform-digit/submission/farm-to-data-table-john-deere-and-data-in-precision-agriculture/; *see also* Project FarmVibes, Microsoft, available at https://www.microsoft.com/en-us/research/project/project-farmvibes/articles/; and *see* Yara and IBM, IBM, available at *https://www.ibm.com/services/client-stories/yara.*

IV. The Way Forward: Debunking Myths and Crafting Solutions that Foster Trust

Considering the many disadvantages of data localization policies overall, why do countries continue to adopt them? One explanation is that policymakers continue to see data localization as the most effective means to achieve the policy goals related to sovereignty, security, and economic growth mentioned at the beginning of this paper. It is not clear, however, whether in most cases the substantial tradeoffs relating to commonly used digital services and business functions that inherently rely on global data flows have been taken into full consideration. This paper seeks to encourage such consideration of the "real life" costs of data localization. In future papers in this series, CIPL will examine the range of motivations for data localization in greater depth and why alternatives may offer more effective means to achieve them.

We will also explore solutions to fostering data flows with trust. As CIPL wrote in a recent op-ed[32], policymakers, the business community, civil society, and scholars must work together to forge solutions that build the trust required for free data flows. Above all, it is the erosion of trust that imperils access to the data flow-based services upon which we all depend. To address it, we must act with creativity, pragmatism, and the open-minded dialogue of all stakeholders. CIPL looks forward to helping advance this process.

[32] *See* International data transfers: Time to rethink binding corporate rules, Bojana Bellamy, IAPP, 8 March 2023, available at https://iapp.org/news/a/international-data-transfers-time-to-be-bold-and-rethink-binding-corporate-rules/.