

Data Localization: Costs, Tradeoffs, and Impacts Across the Economy

December 2020

Data localization measures are spreading around the globe and threaten to undermine many of the efficiencies and economic opportunities of the digital economy. Current policy debates about data localization may not take into account the full costs these measures inflict across the entire economy nor the other policy options available in the pursuit of greater privacy, security, and digital opportunity. International financial services, and many other industries, rely on well-designed frameworks for data to continue delivering innovative, efficient, and valuable services to individuals, households, and corporations. Greater exploration of the impacts of data localization and sharing the broad-based costs and lost opportunities is important as society contemplates new rules for the digital economy.

I. Data Flows Are Integral to The Economy

The global economy is increasingly driven by data. The free flow of this resource has powered incredible innovation around the world beginning with the internet economy and communications. Today, healthcare is being transformed by machine learning algorithms for vaccine development, drug discovery, and rapid low-cost disease diagnosis. Manufacturing automation and safety benefits from training and setup algorithms being constantly updated by new data. In financial services, the rapid flow of data prevents fraud in real time and offers potential solutions to money laundering and terrorist financing by revealing patterns of criminal misuse of the system before it happens. Data flows help enable public cloud computing, which has emerged as a key tool for digital transformation and innovation in financial services and the economy as a whole. Customers across all industries have come to expect the instant on-demand services that are made possible by access to massive data sets of quality at scale and speed.

Connectivity and data flows are also powering global economic growth. Recent estimates on the size of the digital economy conclude that it is equivalent to the gross domestic product of a G7 country and is growing six times faster than major emerging markets¹. In trade, the rise of digital services is even more dramatic with nearly half of cross-border trade now enabled by digital connectivity². Global data flows in the year 2000 were negligible compared to current volumes. There was an important inflection point in 2016 noted by a McKinsey study, “Digital Globalization: The new era of global flows.” It estimated “cross-border data flows may have raised world GDP by roughly \$2.8 trillion in 2014. This surpasses the \$2.7 trillion impact of the global goods trade. In just a decade, global data flows have generated as much economic value as trade networks formed over the course of centuries.” Now, digital trade is growing even as global GDP growth rates are falling³, and the COVID-19 crisis has emphasized the value of digital services and

¹(2019) United Nations Conference on Trade and Development (UNCTAD) Digital Economy Report.

²(2017) United Nations Conference on Trade and Development (UNCTAD), “International Trade in ICT Services and ICT-enabled Services”, Technical Note no. 3, 2015; see also Nicholson, Jessica and Ryan Noonan, “Digital Economy and Cross-Border Trade: The Value of Digitally Deliverable Services”, Current Politics and Economics of the United States, Canada and Mexico, vol. 19, no. 1, 2017.

³ World Bank Global Outlook.

connectivity as economies struggle to maintain operations in the face of the pandemic. A recent IIF Economic paper has highlighted 2020 QoQ growth of e-commerce in the U.S. at 30% as it accelerates toward accounting for one third of all retail sales.⁴

Data localization laws are regulations that require data generated in a country be stored on servers physically located inside the borders of that country. Some go further to require all processing and derivative use of data remain within national boundaries. These measures are a significant and growing threat to the global connectivity, innovation, and growth the digital economy delivers. Access to global value chains, new customers, virtual goods markets, cloud computing, advanced algorithms, and modern payments systems are all improved with good data policy while they can be disrupted by poorly conceived localization requirements.

II. Constraints on The Flow of Data Are Spreading

The past five years have seen a steady rise in the number of countries introducing data localization measures as well as broader interpretation of those measures in licensing and enforcement. This trend, which began in the BRIC countries and centrally controlled economies, has spread into more developed markets including the E.U.

Countries adopting or planning to adopt data localization policies have generally laid out four reasons: first, to ensure the security of a country's data and to prevent data from leaving the country; second, to support law enforcement by enabling national authorities to access data needed for investigation of crimes; third, to develop the indigenous IT skill base, create a data center economy, and develop the local digital economy; and fourth, to protect or improve citizens' individual privacy. While localization seeks to address growing pains in our transforming economy, walling off the global internet and requiring duplicative infrastructure and systems is an extreme and blunt instrument. It adds significant costs and comes with tradeoffs that are not generally discussed in policy debates while also being unlikely to achieve the stated goals for the digital economy.

Understanding some key attributes of data and its economics are helpful:

- Oil is finite, while data is not a limited resource nor is its value consumed when it is used.
- Because data is not constrained, the same data element can be used almost infinitely and simultaneously by many in different locations around the globe adding value in many places in parallel.
- The value of data is created when it is used, analyzed, manipulated, and shared to produce insight. Subsequent and frequent use of the same data element could greatly increase its value.
- Storing data without use, or requiring unnecessary duplication of data, has an economic and ecological cost to society.

Misperceptions of data economics could be misleading policy considerations. For years “data is the new oil” has been a high profile catch phrase popping up in media around the globe. This analogy was an understandable attempt to communicate the potential value of a new resource and the central role it would play powering the next era of innovation and the global economy. Unfortunately, it may also have contributed to flawed understanding of the best way to manage this resource in order to ensure that a country and its citizens could benefit. Hoarding data within national borders will not maximize its value nor boost local economies. Data's value is maximized

⁴ Brooks and Fortun (July 2020) IIF GMV – A Painful and Slow US Labor Market Recovery

when it can flow with trust and permission across companies, sectors, and national borders to be used.

China's great firewall had long been the prime example of data localization. In 2014, Russia enacted new data localization requirements and has added enforcement measures over the years. Turkey passed laws in 2014 and 2016 and soon there was a steady trend emanating from these countries with an increasing number of data localization policies emerging in Brazil, Bulgaria, Denmark, Hungary, India, Indonesia, Jamaica, Kazakhstan, New Zealand, Nigeria, Poland, Sweden, Uruguay, and Vietnam.

In recent years, the EU and large members Germany and France have advanced an increasing number of measures that constrain the flow of data. During the IIF Annual Membership Meeting in October 2020, Kay Swinburn, Vice Chair, Financial Services, KPMG UK said that "the EU's growing focus on digital sovereignty" was another example of the "growing threat of protectionism in the digital economy."⁵ The current direction of travel seems to be moving toward even greater restriction and perhaps broader de facto data localization.

- The EU strategy for artificial intelligence and data released in early 2020 called for the EU to boost its data sovereignty and adopt measures that "lead to more data being stored and processed in the EU." It further posited that European AI algorithms should be trained on European data.
- Gaia-X, a new cloud service provider (CSP), is being incubated by the EU in hope that it can replace foreign headquartered firms. Stricter localization and licensing requirements may be designed to further advance this effort.
- German Economic Minister Altmaier had said that Europe needs "a data infrastructure that ensures data sovereignty."
- Danish Bookkeeping Act requires firms to store financial data of Danish citizens in either Denmark or another Nordic country for five years.
- An April 5, 2016 French government ministerial circular on public procurement outlined that all data from public administrations has to be treated as archives, and therefore stored and processed in France, ruling it illegal to use a non-"sovereign" cloud (i.e., foreign cloud provider) for data produced by public administration.

EU's privacy chief, Wojciech Wiewiórowski, has told journalists he has "some preference" for data processing to stay in Europe. New draft positions encompassed in the "Digital Services Act" and the "Digital Markets Act" under the leadership of European Competition Commissioner Margrethe Vestager and European Commissioner for Internal Markets Thierry Breton reflect the overall direction of travel for tighter and more localized control of data; however, the COVID-19 pandemic has shown some of the limitations these policies could have. In March 2020, an unnamed EU official was quoted talking about unforeseen consequences to the EU Data Strategy: "Now with coronavirus, if you're working on something like a vaccine and you want to move quickly, there is a realization you need to rely on a much broader set of data."⁶ A full and balanced debate on the costs and tradeoffs is critical at this moment when threats of data protectionism could derail digital economic growth and inclusive global connectivity.

This drift in Europe coupled with the measures already in place in the BRIC markets and other Asian countries start to tip the global balance away from open markets and could provide a negative signal and reinforcement on data nationalism to policy makers around the world.

⁵ IIF Annual Membership Meeting (2020) "Future of Finance in a Post-Pandemic New World"

⁶ Javier Espinoza (March 2020) "Coronavirus prompts delays and overhaul of EU digital strategy" Financial Times

In addition to the geographic spread of data localization, there has also been an expansion of different kinds of measures that constrain the flow of data. Some laws require businesses to retain only certain citizen data, particularly to do with financial services, inside national borders. They can also limit cross-border data transfers for processing or require local hosting of some information on local technology infrastructure. Data localization measures do not always emerge in clear legislation, they can also take the form of licensing provisions, contractual requirements broadly imposed by public entities, and additional requirements on data being transferred across borders. When these measures extend beyond storage of data, to regulate how and where data can be processed, it can be an even greater constraint on the ability to keep pace with global developments, leverage the best new technology, and benefit from digital growth. Furthermore, data localization requirements are constantly changing and are frequently found in complex sector-specific regulations rendering compliance more difficult, further eroding the efficiency of new technology, and obscuring their impact. Increasingly, privacy legislation is also including measures that drive data localization and constraints on processing.

III. The Costs of Restricting Data Flows

Proponents of data localization talk about retaining the value of their citizens' data and creating economic opportunity; however, the measures put in place reflect a misunderstanding of what makes data valuable and who ultimately bears the cost of localization requirements.

Data's value is maximized when it can flow with trust and permission across companies, sectors, and national borders to be used. That trusted and permissioned flow, with economic and legal frameworks to ensure safety, security, and equal access opportunity, should be the goal of data policy. It is laudable that governments are seeking greater privacy, security, and economic opportunity for their citizens in an economy increasingly dominated by hyper-scale technology companies; however, the data localization requirements currently spreading as a popular response, are constraining the flow and use of data while adding significant costs and tradeoffs that are not generally understood or discussed.

The costs of data localization are borne out by entire economies. While global big tech or telecommunications firms bear direct costs, such as the resources needed to build duplicative data centers; the impact of localization is transmitted across the entire economy, both in the form of direct costs as

Data Localization Has Economy Wide Costs

- Reduced connections to digital trade, negative impact on economic growth and development, and constrained ease of doing business.
- Weakened fraud prevention, cyber security defense, and potential new AML solutions.
- Slowed scientific discovery, health diagnostics, and telemedicine.
- Reduced access to the best and newest cloud-based software, technology, and future cloud first technologies such as quantum computing.
- Undermined cost effectiveness of cloud-based computing.
- Blocked innovation and competition through curtailed access to the public cloud, a key enabler to the development of fintech and other innovative startups by providing low entry costs, scalable platforms, and embedded services.
- Derailed fast payments, low-cost remittances, and other services individuals, households, and small business need to function in the digital economy.
- Weakened resilience of the financial system. The ability to have seamless failover redundancy systems and storage outside geographical borders could be essential in the case of a natural disaster, war, or other catastrophic event.
- Added hard costs of redundant local data infrastructure that can run \$350 million to \$800 million (Lafferty).

well as consequences such as less efficient systems, reduced connections to global value chains, and less opportunity to leverage global data and technology resources. In fact, SME and gig economy workers may actually suffer some of the greatest impacts from data localization requirements.

Undermining Trade and Economic Growth

A 2018 OECD report noted that “digitalization is linked with greater trade openness, selling more products to more markets and in less concentrated baskets.” It noted that a 10% increase in bilateral digital connectivity raised trade in services by over 3.1%.⁷ A 2014 study of data localization impact by European Centre for International Political Economy (ECIPE) estimated that such requirements could take up to 1.7% off gross domestic product (GDP) in the countries they studied.⁸

There is a scarcity of good cross-country data sources on the impact of data localization on digital trade, and our researchers found it difficult to appropriately model impact on GDP in a cross-country analysis; however, there are two reports which may help indicate the general direction of impact. One was published by ECIPE (2017/18)⁹ and another by the Fletcher School of Johns Hopkins University (2019). They use indexes to rank countries by their openness to digital trade, using data localization measures as one metric.

Across these studies of larger economies, findings pointed consistently to a small number of countries imposing thick digital borders to reduce the flow of data in and out of the country, while other countries that maintain free data flows score highly on digital trade indices. The US and the UK appear as countries most open to digital trade; the EU, and member states Germany and France, have more restrictive digital trade policies. Meanwhile, China, Russia, India, Vietnam, and Indonesia have introduced data localization policies and Brazil has also adopted strong data localization measures. Countries that achieve a high score on the Digital Trade Restrictiveness Index (DTRI) tend to receive a low score on the Ease of Doing Digital Business Index. Taken together, these studies indicate a general impact of data localization. One might also conclude that more developed economies contemplating data residency and localization requirements could risk impacting their ease of doing business and economic opportunity for their populations.

E-commerce is a growth engine built on the free flow of data. The continued rise of this sector makes it increasingly important to maintain real-time data connectivity across the economy. Both as a subset of cross border trade and an important component of domestic retail, it has become an essential sector. In 2019, global retail e-commerce sales reached \$3.53 trillion, almost double the 2016 figure of \$1.548 trillion and a rise of 18.5% from the \$2.982 trillion figure in 2018. As e-commerce sales grow, they account for an increasing proportion of overall retail sales. The global e-commerce share of retail in 2015 stood at 7.4% and doubled to 14.1% in 2019. Once 2020 numbers are finalized, we expect to see a dramatic global acceleration of these trends. This is illustrated by current year data on US e-commerce retail sales, which stand at \$211.5 bn, with a QoQ growth rate in 2020Q2 of over 30%, which is the highest QoQ growth rate on record.¹⁰ When data localization laws and data residency requirements are put in place, it raises barriers to participation in the growing global ecosystem of e-commerce and global value chains by increasing costs, slowing payments, and blocking fraud prevention.

⁷ OECD (2019), “Trade in the Digital Era”, OECD Going Digital Policy Note, Paris

⁸ ECIPE (2014), “The Costs of Data Localisation: A Friendly Fire on Economic Recovery”, <https://ecipe.org/publications/dataloc/>

⁹ ECIPE 2017/2018 Digital Trade Restrictiveness Index, <https://ecipe.org/dte/>

¹⁰ (2019) US Census Bureau Data

Slowing the Digital Ecosystem

Milliseconds matter. When data is mandated to stay inside national borders, it must temporarily be separated from a global data pool, adding additional costs and slowing services. To many in the policy debate, the slight incremental slowing of data flows might not seem like a significant impact; however, measured studies indicate that it can make a world of difference. Research by Google in 2016 found that 40 percent of smartphone users would leave a site that takes longer than three seconds to load, and that time has likely shrunk in the last four years. A 2020 study by Deloitte Ireland “Milliseconds Make Millions”¹¹ showed that a mere 0.1s change in mobile page load time can influence every step of the user journey: “With a 0.1s improvement in site speed, retail consumers spent almost 10% more, while lead generation and luxury consumers engaged more, with page views increasing by 7% and 8% respectively.” Customer expectations are now set for instant, secure, and amazing digital services across the economy and frequently that requires the public cloud and free flowing data to deliver.

These citizen expectations for faster payments, easy onboarding, open banking, and effective fraud prevention rely on the falling cost of storing and processing data remotely along with high-speed global networks. More and more countries are introducing faster or instant payment schemes to meet these expectations. Regulators have also played a role in driving competition and innovation through fintech, which in turn has transformed financial service onboarding and verification of customers to meet KYC, KYB, and AML rules. Digital services in the cloud allow remote account opening and digital identity services for consumers and businesses. Ironically, data localization regulation creates new barriers to these other regulatory initiatives and citizen benefits.

Localization will also lead to internet fragmentation. The internet was designed with an end-to-end decentralized architecture. It has been a driver of amazing growth and rapid innovation because it provides platforms with efficient data storage and processing as well as access to leading global talent and cutting-edge data analytics. If global service companies are unable to freely access global infrastructure, the power of the model is significantly weakened. Local operators may start drifting toward different standards and protocols and over time, the connectivity and interoperability that have been such powerful drivers of growth in the digital economy could be fractured. Once divergence sets in its tracks, it can be very difficult and slow to steer back toward harmonization. This fragmentation would lower productivity gains, slow digital transformation, hinder global trade, and undercut economic growth potential while imposing significant barriers and additional costs to financial services and others attempting to intermediate global trade in an increasingly services-based world.

Undermining Fraud Prevention and Cyber Security Best Practices

Real time global data flows at scale have been coupled with the latest AI and machine learning tools to achieve amazing results in fraud prevention. These new tools are developed by experts in a few tech centers around the world but are blocking the majority of fraud attempts globally while monitoring near instant payments on a vast scale and citizens have benefited. This has been a great success story in financial technology innovation of the last decade and some impressive examples and impact numbers are starting to be shared. The instant free flow of data is essential for delivering these service levels while meeting customer expectations for safe, secure, instant payment in the coffee shop line or walking through mass transit turnstiles.

¹¹ Deloitte Digital / Deloitte Ireland (May 2020), “Milliseconds Make Millions”

Cyber security is undermined by data localization. The accelerating arms race in cyber warfare requires increasingly sophisticated and constantly evolving defense solutions. Public cloud service providers (CSP) and cloud based cyber security firms have delivered incredibly valuable common solutions where the economies of scale, access to scarce talent resources, and the ability to monitor global networks in real time have provided an essential solution to enterprises trying to cope and to regulatory supervisors looking for workable solutions. Data localization would undermine these solutions and weaken common global defenses while breaking a best practice of cyber defense. Storing all data within one geographical region undermines the security of data by exposing it to physical threat and targeted cyberattacks. Often, businesses and institutions will use two or more cloud providers for added security. The best practice offered by cloud computing is to have failover redundancy storage inside and outside geographical or time zones, so data can be instantly moved from a center under attack to another center.

Blocking the Advantages of Cloud Computing

Cloud computing has become an essential tool. Digital transformation of the economy, and financial services in particular, relies on the efficiency of public cloud computing and free flow of data. The opportunity to leapfrog legacy systems and catch up with the digital world by accessing economies of scale in data storage, analysis, and cyber defense has emerged as a critical solution for the modernization of banking, insurance, payments, and asset management. This is even more critical when you take customer needs and expectations for the future of finance into account. As financial intermediation is embedded in other digital services and transactions, it is becoming essential to keep pace with the broader economy and provide added value.

Scarce and expensive tech talent is being accessed through the advanced services offered today on public cloud. In addition to the cyber experts mentioned before, entrepreneurs and enterprises of all sizes benefit from globally scarce talent when systems can operate efficiently across borders. They link the best data architects, solution engineers, and AI Machine Learning developers to all through their work building and running platform solutions in the public cloud. Free flowing data, connected systems, and economies of scale support elite talent in tech hub cities and are delivering distributed use and benefit around the world in real time, but this model breaks down with localization requirements and fragmentation of systems.

Data localization could choke innovation. Start-up ventures frequently rely on public cloud services to launch. It is a democratizing technology. With negligible starting fees—frequently less than twenty USD—it offers ventures of all sizes access to global cutting-edge platforms for development and operation, the ability to set-up instantly, and uses only the capacity they currently need while retaining the ability to rapidly scale. Less than a decade ago, the same specifications for local servers would have cost well into the six figures USD.

Cost efficiencies of cloud computing are undermined by unnecessary duplication of infrastructure and fragmented compliance standards. The cost of data center construction is expensive, with Mastercard reported to spend \$350 million to build a new data center in India.¹² For larger data operators such as Amazon, the cost of a tier one data center is in the range of \$800 million. However, there are two other major costs. One is the cost to transition, which involves more than a rebuild. First, local data must be separated out from the global data set, and two separate systems engineered. There is also a cost of re-integration of two datasets for anti-fraud monitoring. Localized setup of risk and compliance measures on a country-by-country basis also

¹² Prasad (May 2019) “Mastercard claiming compliance with RBI norms, begins deleting transactions data stored overseas” EMTracker

contributes to costs. Fragmenting standards and privacy regulation would further complicate operations and drive costs.

Cloud storage and processing are much more expensive for businesses in countries with data localization restrictions. Where there are no data localization requirements, companies can use globally competitive cloud providers and buy storage and processing power at the lowest prices. When data localization restrictions are in place, extra costs are added and some of them flow to the end users. Averaging figures across processing and storage, the following overall pattern of comparative extra costs by country against a baseline of the US emerges with India +13.7%, Germany +21.6%, France +18.4%, and Brazil +74.6%¹³. Other factors may come into play on relative pricing; however, a general pattern of higher costs seems clear.

Small and medium enterprises (SMEs) may be especially hard hit by the impacts of data localization. The increased costs, constrained access to the resources of the public cloud, reduced opportunities to participate in global value chains, and barriers to the growing digital economy may be most acutely felt by this sector. This area of impact is critical because SMEs employ between 60 and 90 percent of the workforce, yet they account for only one percent of global exports with only 28 percent selling beyond their borders. In sharp contrast, a World Trade Organization (WTO) report found that 97 percent of internet-enabled SMEs export.¹⁴ These opportunities need to be expanded. The COVID-19 pandemic has disproportionately disrupted SMEs, so improving their access to global data flows and plugging into digital markets would seem to be a priority, but new data localization measures may do the opposite.

IV. A Better Way Forward – Alternate Approaches for Addressing Data Concerns

There are better solutions for many of the issues driving data localization. Leading voices are beginning to outline new approaches to ensure safety, security, and equal access to opportunity from data generated in national markets. New legal and economic frameworks to enable trusted and permissioned flow of data across borders are a much better solution to the issues driving data localization.

A global framework for data connectivity and digital trade would solve many of the concerns driving data localization. At the IIF Annual Membership Meeting in October 2020, Ravi Menon, Managing Director of the Monetary Authority of Singapore (MAS), shared a call to action and excellent perspective on the overarching issue driving data localization, privacy laws, and new digital taxation efforts. He said, “Digital connectivity and data connectivity...we do need to have better harmonization of protocols and standards, ... Basically, we need to remake the world that was forged after Bretton Woods—with the WTO and others setting the rules of the game for international trade and international finance. We have not set the rules of the game for international digital flows, international e-commerce.... because we don’t have rules of the game there is not enough trust, there is not enough confidence that data is secure, that data is confidential, and rules of the game are followed, because we haven’t set those rules. I think this is going to be one of the big important tasks for the global community.”¹⁵ Caroline Atkinson, Senior Fellow at the Peterson Institute for International Economics and former Deputy National Security

¹³ Lafferty Group May 2020

¹⁴ WTO Secretariat (2016) “World Trade Report 2016: Levelling the playing field for SMEs, World Trade Organisation”

¹⁵ IIF Annual Membership Meeting (2020), “In Conversation (with Ravi Menon)”

Advisor for President Obama, echoed the call during the same event when she said, “We need new international standards and cross-border interoperability for data.”¹⁶

In 2019, the Japanese G20 Presidency sought to raise these issues and spark action when they launched the Osaka Track, a process to promote efforts on international rule-making for data free flow with trust (DFFT). It outlined an architecture for data governance that provides principles to inform global standards. There is some hope that the upcoming U.K. Presidency of the G7 will pick up some of these issues and that the U.S. might engage on these topics in this forum more directly.

New technology in digital identity and data tracing are poised to play a role as well. Regulations such as the E.U.’s General Data Protection Regulation (GDPR) and other privacy laws create conditions where technology that could track data origin, custody chains, and usage—while linking to next generation personal and legal entity identifiers—indicates a much better vision. This point of arrival for ensuring security, privacy, and economic benefit from data will require work on many fronts. The Open ID Foundation, IIF Open Digital Trust initiative, and The Trust over IP (ToIP) Foundation, are all forums where technology leaders and industry are working to forge new open standards for the trusted exchange of data.¹⁷ Central bank digital currencies (CBDC) and related consumer digital wallets are another adjacent technology development with the opportunity to upgrade digital identity and modernize frameworks for data sharing and privacy.

In the absence of global frameworks, forward looking bilateral trade agreements have begun addressing digital trade, the flow of data, protection, privacy, and new standards for digital identity and records.

The Australia-Singapore Digital Economy Agreement (DEA), signed on 6 August 2020, is the most advanced example of these agreements. It addresses a comprehensive set of issues for the new digital economy while moving in the exact opposite direction of data localization efforts that claim to have similar objectives.

The DEA provides “more robust rules that ensure businesses, including in the financial sector, can transfer data across borders and will not be required to build or use data storage centres in either jurisdiction; improves protections for source code; establishes new commitments on compatible e-invoicing and e-payment frameworks; and delivers new benchmarks for improving safety and consumer experiences online. The DEA also delivers a range of new trade rules, and a comprehensive framework for bilateral cooperation, to help businesses and consumers capitalise on the digital economy. Australia and Singapore have negotiated cutting-edge new rules and signed a series of MoUs on areas including data innovation, artificial intelligence, e-invoicing, e-certification for agricultural exports and imports, trade facilitation, personal data protection, and digital identity. DEA also includes closer cooperation to support the harmonization of key standards to support digital trade. ... ten areas to align on international standards: artificial intelligence, distributed ledger technology, smart cities, digital identities, e-payments, e-invoicing, Internet of Things, data protection and privacy, cross-border data and data

¹⁶ IIF Annual Membership Meeting (2020), “International Economic Cooperation and Institutions: Reform, Revitalize, or Reimagine?”

¹⁷ <https://openid.net/foundation/>

portability.”¹⁸ This agreement lays out an excellent model for bilateral efforts and an outline of the major issues for discussions about global standards.

United States-Mexico-Canada Agreement (USMCA), the 2019 NAFTA replacement, also began tackling some of these issues with an entire chapter on digital trade and prohibitions of data localization laws, tariffs on digital goods, and discrimination against foreign suppliers of digital goods and services. This agreement was essentially duplicated in the 2019 US-Japan Digital Trade Agreement. One of the positive developments of these efforts should be the adoption of a “whole of economy view” for good data governance across sectors and jurisdictions.

Conclusion

Data localization requirements impose costs and inefficiencies broadly across the economy in ways that are not fully quantified or broadly discussed. The impact is especially acute in those areas where future growth and opportunity lie including digital trade, e-commerce, global value chains, digital services, and fintech innovation. Data localization is looking at one dimension of the changing landscape, while many related threads are running on parallel tracks separated by industry and sectoral silos with rules established for a world based on physical goods and analogue services. These frameworks are proving unfit for purpose in the digital economy. Greater examination of the full costs of data localization measures should proceed in the hopes that this accelerating and expanding policy trend can be rethought before global productivity, economic growth, and broad-based opportunity suffer the consequences. We encourage the pursuit of better approaches to address cross-border data issues—trade agreements and multilateral frameworks to enable trusted and permissioned flow of data—as a priority for the global community and look forward to engaging in the work ahead.

¹⁸ Australian Government, Department of Foreign Affairs and Trade (August 2020). “Australia-Singapore Digital Economy Agreement” <https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement>

Lead Author



Conan French
Senior Advisor, Digital Finance
cfrench@iif.com

Other Contributors



Brad Carr
Managing Director, Digital Finance
bcarr@iif.com



Clay Lowery
Executive Vice President, Research and Policy
clowery@iif.com

Lafferty Research – This paper incorporates analysis performed for the IIF by Lafferty Global Advisory Services.