November 14, 2017

Central Bank of Brazil
Department of Financial System Regulation,
SBS, Quadra 3, Block "B", 9th floor,
Headquarters Building, Brasília (DF), CEP 70074-900.

Dear Sir or Madam:

On behalf of the Information and Technology and Innovation Foundation (ITIF), we are pleased to submit these comments in response to the Central Bank of Brazil's request for public comments on the draft resolution (57/2017, dated September 19, 2017) on cybersecurity policy and requirements for contracting processing, data storage, and cloud computing services for financial institutions and other institutions authorized to operate by the Central Bank of Brazil. ITIF is grateful for the opportunity to provide input.

ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation, and pro-technology public policy agenda that spurs growth, prosperity, and progress. ITIF is based in Washington, DC and frequently engages with policymakers from Brazil and around the world.

Yours sincerely,

Dr. Robert D. Atkinson
President and Founder, Information Technology and Innovation Foundation
ratkinson@itif.org

Nigel Cory
Senior Trade Policy Analyst, Information Technology and Innovation Foundation
ncory@itif.org

CONTENTS

OVERVIEW

Data is central to the modern economy, whether firms are in goods sectors (such as agriculture, manufacturing, and mining) or in services. Of the latter, the financial sector is among the most data intensive, as technological innovation has fundamentally changed how people access and use financial products and services. As such financial services firms, especially ones with operations in more than one nation, require the ability to move data between nations. Combined with the fact that a country's financial sector plays a crucial intermediary role in its broader economy, this means that elements of this draft resolution on cybersecurity that limit cross-border financial data flows have the potential to exert negative impact across the Brazilian economy.

The proposal raises a number of major concerns for Brazil's financial sector, not to mention Brazil's broader potential to develop a data-driven economy (appendix lists relevant provisions). The main issue is that the cybersecurity proposal would force firms to store their data locally (article 11). There are also concerns with its requirement for firms to indicate where the actual data centers are located (article 12:1) and the requirement for cloud companies to provide the Brazilian Central Bank with physical access to the data centers (article 12:7).

The draft proposal's focus on geography—by forcing financial firms to use or setup local cloud services, a concept known as "data localization"—would negatively affect Brazilian firm competitiveness and productivity, and would actually raise potential cybersecurity risks. Financial firms, and the sector as a whole, would be less competitive as the rules would potentially cut them off from cheaper and better global cloud service providers. This would ripple throughout the Brazilian economy by reducing productivity, as any increase in financial firms' information and communications (ICT) costs would likely be passed onto users, whether these are individuals, companies, or the government. From a cybersecurity perspective, this local data storage requirement may force financial firms to use local cloud services that are not best-in-class in using the

latest protective measures. Furthermore, forcing firms to store data locally may also increase cybersecurity risk as it forces firms that operate across multiple countries to spread their data across more data centers—losing the benefits of centralized and more effective management.

This submission outlines why the notion at the heart of this proposal—that data must be stored domestically to ensure that it remains secure and private—is false and how the Central Bank's focus should be on ensuring that financial firms use best-in-class data storage cybersecurity measures (regardless of where the data is stored). Likewise, the Central Bank should be focused on ensuring the regulatory framework provides the transparency and accountability about how firms manage their ICT infrastructure and data management so that they're able to fulfil their reporting responsibilities (in terms of providing data to authorities), rather than focusing on the location of data and physical access to data centers.

THE IMPORTANCE OF GLOBAL AND FINANCIAL DATA FLOWS

Data flows—which were practically nonexistent just 15 years ago—now play a key role in global economic and trade activity.[i] Indeed, in the globally integrated digital economy, an organization's ability to collect, analyze, and act on data is critical to driving innovation and growth. Fully half of all global trade in services is enabled by ICTs, which depend on cross-border data flows.[ii] As the Organization for Economic Cooperation and Development (OECD) notes in a recent report on the data economy:

> The free flow of information and data is not only a condition for information and knowledge exchange, but a vital condition for the globally distributed data ecosystem as it enables access to global value chains and markets…. The data ecosystem involves cross-border data flows due to the activities of key global actors and the global distribution of technologies and resources used for value creation. In particular, ICT infrastructures used to perform data analytics, including the data centres and software, will rarely be restricted to a single country, but will be distributed around the globe to take advantage of several factors; these can include local work load, the environment (e.g., temperature and sun light), and skills and labour supply (and costs). Moreover, many data-driven services developed by entrepreneurs "stand on the shoulders of giants" who have made their innovative services (including their data) available via application programming interfaces, many of which are located in foreign countries.[iii]

The global flow of data is only growing as new ICTs and processes facilitate cheaper and better services. Modern businesses find cloud-computing benefits so compelling that more than 60 percent of the world's server workloads now take place on cloud servers, up from 8 percent five years ago.[iv] Cloud computing can deliver the massive scalability needed to store and process big data at a fraction of the cost. Today, 85 percent of new software is being built for the cloud.[v] One company found that a database query that once took 21 days at a cost of $150,000 on one platform can now run on a cloud cluster in just one hour for $900.[vi] With the increasing use of cloud computing, where the data is stored isn't important; what matters are the rules and management of that data.

In the past decade, Brazil's digital economy has grown exponentially in size and importance, as can be attested by the growing size of associated subscriptions, value added, output, and employment.[vii] While Brazil's digital economy holds enormous promise, it has a long way to go to catch up to countries at the frontier of digitalization, and provisions in this proposal could hold it back further. There is an opportunity cost associated with countries that limit their participation in the global digital economy, through policies such as the local data storage requirements in this proposal. A McKinsey study examined the size of this unrealized opportunity by calculating the value that countries realized by increasing participation in a range of data flows relative to the size of their economies from 2003 to 2013 (the latest year for which there are global data for all flows). Brazil could have added some $1.4 trillion to its GDP over the past ten years, making its economy 60 percent bigger by 2014, by accelerating its participation in all types of global data flows.[viii] The formation of a ministerial working group for a Brazilian Digital Strategy earlier this year is a welcome step in the right direction in realizing the potential benefits, but there are many outstanding issues for Brazilian policymakers to address to help it catch up, such as by eliminating local content requirements for local telecommunications infrastructure as well as local content requirements for software in government procurement.[ix] Adding a local data storage requirement for financial data would only add to this list of policies which hold Brazil back.

This provisions in this proposal could be particularly damaging as data, and its ability to move freely, is critical to modern finance. Personal and corporate finance have been revolutionized by the Internet. Users can easily access online financial services to engage in e-commerce, such as to buy physical or digital goods and services. A tourist can use a credit card overseas and use the Internet to log onto their financial institution to check on the payment. In this way, financial services are a critical facilitator of the entire modern economy. At the international level, for international financial firms, the free flow of financial data is critical. They rely on the free flow of digital information to support customers and operations in virtually every sector of the economy in countries all around the world. For example, Citibank's global banking operations show the importance of the global free flow of data. More than 60 percent of Citibank's customers—it has over 200 million customer accounts—conduct their banking online. These processes are facilitated through 20 regional data centers, which are purpose-built using servers, storage, and networks that are environmentally controlled and highly secured to provide the highest-possible resilience for the bank's services and customer support.[x]

THE COSTS OF FOCUSING ON GEOGRAPHY

Regulators concerns over how to ensure it has proper oversight over the cybersecurity measures at financial firms is justified, but the approach as outlined in the proposal is mistaken in a number of ways. Enacting these regulations would likely impose economic costs and negatively impact the innovation capacity of enterprises in Brazil.

Maximizing the value of data requires its ability to move. Innovation and economic growth are increasingly driven by how firms collect, transfer, analyze, and act on data. Absent policy-created "data protectionism," digital trade and cross-border data flows are expected to continue to grow much faster than the overall rate of global trade. Cutting off cross-border data flows would undermine the innovative technologies that are central to the financial sector's competitive position. The benefits the financial services sector derives from cloud

computing, big data analytics, and other innovative technologies at the heart of the data economy are only fully realized when based upon ready access to large volumes of information, such as anonymized customer purchase data. Financial service innovations, whether in personal remittance services, business-to-business payments, or elsewhere, will be put at risk if barriers to the free flow of financial data become the norm.[xi]

A local data storage requirement in Brazil would likely raise the cost of all financial service firms, who would pass these costs on to the many consumers, corporations, and governments who use financial services on a daily basis, creating an inefficiency that detracts from economic growth. As ITIF reported in "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost the World?," there is a growing body of research that estimates the cost of barriers to data flows in terms of lost trade and investment opportunities, higher information technology costs, reduced competitiveness, and lower economic productivity and GDP growth.[xii] While these studies do not focus specifically on the costs of data localization for financial data in Brazil, the economic costs are indicative of the impact.

For example, a 2015 Leviathan (an information security company) study shows that local companies could have to pay significantly more for cloud services in Brazil if data localization policies had cut them off from the most cost-competitive global cloud providers.[xiii] The study looks at the change in per-hour costs for cloud services if data localization policies forced local companies to use the local cloud services from one of the seven major providers covered in the study. The study considered like-for-like services (focusing on memory allocated to services, with 1GB, 2GB, 4GB, 8GB, 16GB, and 32GB server categories) from global leaders in public infrastructure-as-a-service cloud companies: Amazon Web Services, DigitalOcean, Google Compute Engine, HP Public Cloud, Linode, Microsoft Azure, and Rackspace.

The Leviathan study shows that if Brazil had enacted data localization as part of its "Internet Bill of Rights" in 2014, companies would have had to pay an average of 54 percent more to use cloud services (of all categories) from local cloud providers compared with the lowest worldwide price. For example, for 1GB equivalent services Brazilian customers would have had to pay 37.5 percent more, while for 2GB services the increase would have been 62.5 percent.[xiv]

In addition, a 2014 European Center for International Political Economy (ECIPE) study estimated the economic costs related to proposed or enacted data localization requirements and related data-privacy and security laws in Brazil and other countries, such as China, the European Union, India, Indonesia, South Korea, and Vietnam.[xv] The study aimed to analyze the impacts on exports, gross domestic product (GDP), and consumer welfare (lost consumption due to higher prices and displaced domestic demand). ECIPE estimates that policies that increase data-processing costs negatively impact economic growth through higher prices on data services. The estimated results are significant and negative: an economy-wide data localization requirement would reduce GDP by 0.8 percent, domestic investment would decrease 4.2 percent, and higher prices and displaced domestic demand would lead to consumer welfare losses of $15 billion.

Moreover, the proposed regulations appear to be based on the view that cloud data storage is a commodity with only data storage being the service offering. In fact, global leading cloud provides provide scores of different kinds of services that go beyond simple storage of data. These services include analytics, networking, management tools, computing services, security tools and a host of other applications. Financial services firms in Brazil should have the freedom to choose the highest quality and best value cloud services, regardless of their location, provided that they meet Brazilian government security standards.

FOCUS ON THE MEASURES USED TO PROTECT AND MANAGE DATA AND ON LEGALLY MANDATED ACCESS TO DATA, NOT GEOGRAPHY

At the heart of the proposal's focus on geography is the mistaken belief that data must be stored domestically to ensure that it remains secure, private, and accessible to government. This is false. With regards to security, while certain laws may impose minimum security standards, the security of data does not generally depend on where data is stored, only on the measures used to store it securely. As ITIF writes in "The False Promise of Data Nationalism," data localization mandates do not increase commercial privacy or data security.[xvi] What matters are the technological and procedural methods of storing and transferring data when determining how safe data is, not the geographical location where the data is stored.[xvii] A secure cloud server in Colombia is no different from a secure cloud server in Brazil. Inadvertent disclosures of data (e.g., security breaches) highlight this point as security breaches can happen no matter where data are stored—data centers everywhere are exposed to attacks. Data breaches are the result of security failures, not the location of the data.

Data security depends on the technical, physical, and administrative controls implemented by the service provider, which can be strong or weak, regardless of where the data is stored. For example, in a practice that protects both data privacy and security, some cloud-computing companies have upgraded security controls, so that customers retain the keys used to encrypt data before it is uploaded, thereby preventing third parties, including the cloud companies themselves, from accessing their data.[xviii] While cloud computing does not guarantee security, and organizations should investigate the terms of service and security practices of any service provider, cloud computing will likely lead to better overall security because implementing a robust security program requires resources and expertise, which is what many small and mid-sized organizations lack, but large-scale cloud-computing providers can offer. This highlights the central point that should guide the Central Bank's efforts to improve cybersecurity—what is of critical importance is that the financial firm and its cloud storage service (whether it's a company with its own network or a third-party cloud provider) be dedicated to implementing the most advanced methods to prevent such attacks.

The proposal's focus on locating data centers in Brazil and on providing the Central Bank with physical access to data centers is similarly mistaken. From a prudential oversight perspective, what should matter is how a firm or its cloud supplier manages its IT and data managements systems, how it provides the Central Bank with information on this as part of prudential reporting, and that it can provide timely access to data requested by the Central Bank (as part of its oversight activities). The proposal should solely focus on those provisions which provide the legal framework so that the Central Bank has the confidence that financial firms are properly managing their data and that if need be, they can provide data upon request. In addition to the

U.S. example (below), the European Commission's (EC) efforts are a useful reference point for the Central Bank on this issue around access to data. As part of efforts to build a digital single market, the EC is working to remove barriers to the transfer of company data, tax data, book-keeping data, and financial data and instead asking that member states focus on mandating access.[xix] For example, in 2015, Denmark changed its local data storage requirement for accounting data so that companies can store their data anywhere as long as Danish authorities have easy access to these upon request.[xx] This is where the focus should be—putting in place the legal framework to ensure that companies must provide data to regulatory authorities in a timely manner.

If the worry is that firms will avoid regulatory oversight by simply shifting data overseas, this is similarly mistaken. Financial firms doing business in Brazil would need to be approved by the Central Bank, which thereby means they have to have "legal nexus" in Brazil, which puts them under the Central Bank's jurisdiction. As such, the firm must comply with whatever rules the Central Bank has on data regardless of whether it stores the data in the host country, in the home country of the foreign company, or even in a third country. In this way, just as consumer safety and other laws apply to tangible goods that flow in and out of a country as part of international trade, cybersecurity and other rules apply to data and the financial firms that move and store data in another nation.

A LESSON FOR BRAZIL FROM THE UNITED STATES

Similar to Brazil, the U.S. Treasury and financial regulators recently considered a policy that would have allowed data localization for financial data, but thankfully, these agencies have since recognized that such policies were not needed. As ITIF reported in "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements," these U.S. agencies wanted financial data to be excluded from the Trans Pacific Partnership (TPP) trade agreement's provisions that prohibited member countries from enacting barriers to data flows, because they wanted to reserve the right to force financial firms to store data locally.

U.S. regulators concerns were due to issues American regulators faced during the global financial crisis when they had issues getting access to data in a key bank's (Lehman Brothers') IT system during bankruptcy proceedings. The U.S. Federal Reserve and Federal Deposit Insurance Corporation's (FDIC) ability to use and analyze Lehman's IT system and data was reportedly hindered as the bank's network became fragmented: overseas subsidiaries were sold off; some IT systems in overseas subsidiaries were turned off; some key IT staff departed; and restrictions on data flows were imposed due to insolvency filings in other countries, as was the case when the United Kingdom's financial regulator took over Lehman Brothers' European division.[xxi] This made it difficult for the regulators to access the data needed to unwind positions and ascertain what money was owed to whom.[xxii] However, subsequent reforms addressed these concerns by focusing on how companies disclose to regulators how they manage their IT and data as part of regular prudential compliance activities so that regulators know, that in the event of a crisis, the company will be able to provide the data regulators want.

Following the crisis, the United States enacted the Dodd-Frank Act (in 2010), which outlined extensive new rules that require "systemically important financial institutions" (SIFIs) to prepare "resolution plans"—also known as "living wills"—that specify a company's strategy for "rapid and orderly resolution in the event of material financial distress or failure of the company."[xxiii] More than 100 large financial firms are now required by law to periodically submit these living wills to the Federal Reserve and FDIC for review and feedback. U.S. livings wills achieve this by requiring firms to meet stringent requirements about how their IT systems are organized and how data is stored, accessed, and managed on an ongoing basis (as part of periodic compliance activities) and in the event of a crisis.[xxiv] In a similar way, Brazil could look to emulate the U.S. review process whereby regulators check companies' contingency plans and provide advice to individual firms about how to improve how they manage and report on their IT and data management systems. If there are systemic issues about how firms are organizing and reporting their IT and data systems as part of their living wills, the Federal Reserve has the ability to issue additional sector-wide advice for all firms, as it does for other issues.[xxv]

The U.S. FDIC essentially admitted that data access concerns were resolved through the Dodd-Frank Act, thereby removing the misguided excuse for potential forced data localization policies. In a retrospective study into how the resolution of Lehman Brothers would have been different had the Dodd-Frank Act been in place, the FDIC detailed how living wills would mean the FDIC would already know where and how the firm would access data needed in the case of bankruptcy.[xxvi] As the FDIC states, "had the Dodd-Frank Act been enacted sufficiently far in advance of Lehman's failure, undoubtedly much more supervisory information would have been available in March 2008. Both the Federal Reserve and the FDIC would have had the detailed information present in Lehman's statutory required resolution plan."[xxvii] This report stated how the FDIC would work with foreign financial regulators to coordinate efforts to manage Lehman Brothers' receivership across jurisdictions, based on the information in its U.S. living will and its local variants in other jurisdictions.[xxviii]

BRAZIL SHOULD REDOUBLE EFFORTS TO ENGAGE WITH INTERNATIONAL FINANCIAL FORUMS

The Central Bank's proposal highlights why Brazil should join with regulators from around the world in working to improve cooperation, including by addressing any remaining concerns about cross-border data flows and jurisdiction over financial data, especially during a crisis. The United States and other leading economies have worked hard in the wake of the global financial crisis to improve oversight of how firms that are designated SIFIs manage their IT systems and data, especially how these firms plan to store and retrieve data in the event of bankruptcy. The International Monetary Fund and the Financial Stability Board (FSB) have already devoted considerable effort to issues pertaining to the collection, reporting, and management of financial data since the crisis.[xxix] In their joint report on "The Financial Crisis and Information Gaps" to G-20 finance ministers and central bank governors in 2009, they pointed out that "the recent crisis has reaffirmed an old lesson—good data and good analysis are the lifeblood of effective surveillance and policy responses at both the national and international levels."[xxx] One clear outcome from the global financial crisis has been the need to improve the governance of financial information and data.[xxxi] Resolving these issues now is clearly preferable to facing them again during a crisis, when the immediacy of emotion and political expediency wins out over measured policy responses.[xxxii]

While some progress had been made, there is still more to do to improve prudential regulations around the world, as European Central Bank President Mario Draghi remarked in 2014.[xxxiii] The FSB remains a key forum as it develops best practices for members to adopt, including for such important functions as resolution and recovery plans, which cover how financial firms manage critical shared services across multiple jurisdictions. After reviewing many leading economies, a recent FSB report identified bank resolution plans for bankruptcy, which includes living wills, as an area where further international cooperation is needed. The FSB outlines some of the remaining challenges for regulators: a lack of relevant bank data; a lack of experience about how to use and filter large amounts of bank data; the development of realistic bank failure scenarios; the absence of harmonized criteria; and poor coordination protocols for resolution.[xxxiv] It should be noted that the FSB report did not raise the location of data as an issue for regulators. So it is incumbent on Brazil and others to join in these efforts. The FSB's periodic peer review mechanism could be a useful tool to assess how members manage data access issues and as a way to identify where further work is needed to develop relevant international financial standards and policies.

CONCLUSION

The Central Bank's concerns over cybersecurity in the financial sector are understandable. However, focusing on geography is not the best way to ensure that financial institutions in Brazil are enacting best-in-class cybersecurity measures. In addition, as it relates to prudential oversight, the Central Bank should revise the proposal to build the framework and processes so that financial firms are showing regulators that they are committed to protecting their IT and data management systems, and as part of prudential oversight, are able to provide data to authorities upon request. The location of the data should be irrelevant.

If enacted, the forced local data storage provisions in this proposal would continue a worrying trend whereby a growing range of countries around the world are enacting barriers to data flows. If regulators in every country followed the Central Bank's local data storage requirement, it would inevitably lead to a balkanized and weaker global economy and Internet, and ultimately, make the Central Bank's regulatory job harder by trapping data they might want behind borders. The distributed nature of the Internet and the critical need for the free flow of data shows why Brazil and its regulators should work with counterparts around the world to address issues that inevitably arise when data crosses borders so that the actual issue at the heart of a problem (whether privacy, cybersecurity, or regulatory access to data) is addressed while allowing data to flow freely.

APPENDIX

The below outlines the main provisions of interest to this submission, as detailed in draft proposal 57/2017 in the Central Bank of Brazil's public consultation system.[xxxv]

Article 9: The institutions mentioned in art. 1. The contracting of data processing and storage services and cloud computing services shall:

1. to adopt practices of corporate governance and management proportional to the relevance of the service to be hired and the risks to which they are exposed;
2. require the contractor to ensure:
    a. the access of the contracting institution to data and information processed or stored by the contractor;
    b. the confidentiality, integrity, availability and retrieval of data and information processed or stored by the contractor;
    c. the audit of the services rendered and their compliance with the regulations; and
    d. the access of the contracting institution to the instruments for monitoring and managing the controls provided by the company contracted to provide the services; Datacenter companies must grant access, to its clients, to the data and information "processed" (art. 9).

Article 11: Cloud services cannot be provided from abroad;

Article 12:1: The need to indicate the physical location of the datacenters;

Article 12, provisions 8 and 9: Keep a security copy of the data and information stored by the datacenters, as well as information on its processing, and grant to the Central Bank the liberty to access this data;

Article 12:7: Grant to the Central Bank access to the contracts, deals, documents and information referring to the services provided by the datacenters, as well as to the physical facilities;

Article 17:5: Make available for a period of 5 years the data, registers and information referring to the mechanisms of control of the cybersecurity policy;

Article 20: The Central Bank of Brazil may impose restrictions for the hiring of data processing and storage services and cloud computing when it finds, at any time, the inadequacy of the service to the terms of this Resolution, establishing a deadline for the adequacy of said services.

i. Jacques Bughin, Dhruv Dhingra, Susan Lund, James Manyika, Kalin Stamenov, and Jonathan Woetzel, "Digital Globalization: The New Era of Global Flows" (McKinsey Global Institute, February 2016), http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/Digital-globalization-The-new-era-of-global-flows; United Nations Conference on Trade and Development (UNCTAD), *Information Economy Report 2009: Trends and Outlook in Turbulent Times* (New York and Geneva: United Nations Conference on Trade and Development, United Nations, 2009), http://unctad.org/en/docs/ier2009_en.pdf; Hosuk Lee-Makiyama, "Digital Trade in the U.S. and Global Economies" (speech submission to the USITC investigation, European Centre for International Political Economy, accessed April 6, 2016), http://www.ecipe.org/app/uploads/2014/12/USITC_speech.pdf.

ii. *Information Economy Report 2009*.

iii. Organisation for Economic Co-operation and Development (OECD), "Data-Driven Innovation, Big Data for Growth and Well-Being," (Paris: OECD, October 2014), 73, http://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf.

iv. Peter Cowhey and Michael Kleeman, *Unlocking the Benefits of Cloud Computing for Emerging Economies—A Policy Overview*, (paper, University of California San Diego, 2008), https://www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/unlocking_benefits_e.pdf.

v. IBM, *2013 IBM Annual Report* (annual shareholder's report, IBM, New York, 2013), http://www.ibm.com/annualreport/2013/bin/assets/2013_ibm_annual.pdf.

vi. Business Roundtable, "Putting Data to Work: Maximizing the Value of Information in an Interconnected World" (Business Roundtable, Washington D.C., February 2015), http://businessroundtable.org/sites/default/files/reports/BRT%20PuttingDataToWork.pdf.

vii. Organisation for Economic Co-operation and Development (OECD), *OECD Digital Economy Outlook 2015* (Paris: OECD, 2015), http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm

viii. *OECD Digital Economy Outlook 2015; Digital Globalization: The New Era of Global Flows.*

ix. "Ministerial working group established to develop Brazil's 'Digital Strategy'," Smart Cities World Forums website, accessed November 9, 2017, http://www.smartcitiesworldforums.com/news/smart-cities-south-america/finance-policy-sa/208-ministerial-working-group-established-to-develop-brazil-s-digital-strategy; Robert Atkinson, "High Taxes and Tariffs Hold Back Brazil's Digital Economy," Estadao, April 22, 2015, http://economia.estadao.com.br/noticias/geral,o-brasil-ancorado-no-seculo-20-imp-,1673720.

x. Ibid., 6; Charles Johnston, "Investigation Number 332-531, Digital Trade in the U.S. and Global Economies, Part 1" (submission by Citi to a United States International Trade Commission investigation, March 14, 2013), http://www.uscib.org/docs/Citi_TC_030713.pdf.

xi. World Economic Forum (WEF), *The Future of FinTech: A Paradigm Shift in Small Business Finance* (Geneva: WEF, October 2015), http://www3.weforum.org/docs/IP/2015/FS/GAC15_The_Future_of_FinTech_Paradigm_Shift_Small_Business_Finance_report_2015.pdf; the United States International Trade Commission (USITC), *Digital Trade in the U.S. and Global Economies, part 1* (Washington D.C.: USITC, July, 2013), https://www.usitc.gov/publications/332/pub4415.pdf.

xii. Nigel Cory, "Cross Border Data Flows: Where Are The Barriers and What Do They Cost?" (Information Technology and Innovation Foundation, May, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

xiii. Brendan O'Connor, "Quantifying the Cost of Forced Localization" (Leviathan Security Group, June 2015), http://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization.

xiv. O'Connor, "Quantifying the Cost of Forced Localization."

xv. The study uses a computable general equilibrium model (CGE) called GTAP8. The effect on productivity is created using a so-called augmented product market-regulatory index for all regulatory barriers on data, including data localization, to calculate domestic price increases or total factor productivity losses. Matthias Bauer, Hosuk Lee-Makiyama, Erik can der Marel, Bert Verschelde, "The Costs of Data Localisation: Friendly Fire on Economic Recovery" (European Centre for International Political Economy, March 2014), http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

xvi. Daniel Castro, "The False Promise of Data Nationalism" (Information Technology and Innovation Foundation, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

xvii. Castro, "The False Promise of Data Nationalism."

xviii. Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law" (Information Technology and Innovation Foundation, March 2016), http://www2.itif.org/2016-unlocking-encryption.pdf.

xix. Julia Fioretti, "EU looks to remove national barriers to data flows," *Reuters,* September 29, 2016, http://www.reuters.com/article/us-eu-data/eu-looks-to-remove-national-barriers-to-data-flows-idUSKCN11Z19Q.

xx. "Requirements for Exemption to Store Electronic Accounting records Abroad Will Be Abolished," Horten's website, accessed November 9, 2017, http://en.horten.dk/News/2015/February/Requirement-for-exemption-to-store-electronic-accounting-records-abroad-will-be-abolished.

xxi. Rosalind Wiggins and Andrew Metrick, "The Lehman Brothers Bankruptcy: The Effect of Lehman's U.S. Broker Dealer" (Yale Program on Financial Stability Case Study 2014-3E-V1), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2588556; Administrative Office of the United States Courts, *Report Pursuant to Section 202(e) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010* (Washington, DC, July 2011); Lemieux, "Financial Records and Their Discontents"; "Lehman Brothers International (Europe) in Administration: Joint Administrators' Progress Report for the Period 15 September 2008 to 14 March 2009," Pricewaterhouse Coopers, accessed April 4, 2016, http://www.pwc.co.uk/en_uk/uk/assets/pdf/lbie-progress-report-140409.pdf.

xxii. "Lehman Brothers International (Europe)."

xxiii. "Resolution Plans," Board of Governors of the Federal Reserve System, accessed April 4, 2016, https://www.federalreserve.gov/bankinforeg/resolution-plans.htm.

xxiv. These "living wills" are required to provide a broad range of information relevant to resolution planning and implementation including, for example, detailed descriptions of organizational structures, credit exposures and cross-guarantees, and supporting data. The relevant section on IT and data states: "Management Information Systems; Software Licenses; Intellectual Property. Provide a detailed inventory and description of the key management information systems and applications, including systems and applications for risk management, accounting, and financial and regulatory reporting, used by the covered insured depository institution (CIDI) and its subsidiaries. Identify the legal owner or licensor of the systems identified above; describe the use and function of the system or application, and provide a listing of service level agreements and any software and systems licenses or associated intellectual property related thereto. Identify and discuss any disaster recovery or other backup plans. Identify common or shared facilities and systems, as well as personnel necessary to operate such facilities and systems. Describe the capabilities of the CIDI's processes and systems to collect, maintain, and report the information and other data underlying the resolution plan to management of the CIDI and, upon request, to the FDIC. Describe any deficiencies, gaps, or weaknesses in such capabilities and the actions the CIDI intends to take to promptly address such deficiencies, gaps, or weaknesses, and the time frame for implementing such actions."

xxv. For example, on April 13, 2016, the Federal Reserve and FDIC ordered five big U.S. banks to make significant revisions to their living wills or risk potential regulatory sanctions. Furthermore, both agencies provided additional guidance on resolution plans to three foreign banking organizations after reviewing their 2015 submissions. One of the action items was for these firms to improve how they are able to ensure they have the operational capabilities for resolution preparedness, such as the ability to produce reliable information in a timely manner.

xxvi. Federal Deposit Insurance Corporation (FDIC), "The Orderly Liquidation of Lehman Brothers Inc. under the Dodd-Frank Act" *FDIC Quarterly* 5, no. 2 (2011), https://www.fdic.gov/bank/analytical/quarterly/2011_vol5_2/lehman.pdf.

xxvii. Ibid.

xxviii. Ibid.

xxix. The Financial Stability Board (FSB) is an international body that monitors and makes recommendations about the global financial system. The FSB brings together senior policy makers from ministries of finance, central banks, and supervisory and regulatory authorities for G20 members and four other key financial centers—Hong Kong, Singapore, Spain, and Switzerland. Financial Stability Board (FSB), "Second Thematic Review on Resolution Regimes," (Basel, Switzerland: FSB, March 18, 2016), http://www.fsb.org/wp-content/uploads/Second-peer-review-report-on-resolution-regimes.pdf.

xxx. Financial Stability Board and the International Monetary Fund, "The Financial Crisis and Information Gaps: Report to the G20 Finance Ministers and Central Bank Governors" (Sydney: Financial Stability Board and the International Monetary Fund, October 2009), http://www.fsb.org/wp-content/uploads/r_091029.pdf?page_moved=1; Financial Stability Board and the International Monetary Fund, *The Financial Crisis and Information Gaps: Implementation Progress Report* (Sydney: Financial Stability Board and the International Monetary Fund, September 2015), http://www.imf.org/external/np/g20/pdf/2015/6thprogressrep.pdf.

xxxi. The Dodd-Frank Wall Street Reform and Consumer Protection Act created the Financial Stability Oversight Council and Office of Financial Research to monitor threats to financial stability in the United States. Also, the Federal Reserve Board established a new Office of Financial Stability Policy and Research. The Federal Deposit Insurance Corporation established a new Office of Complex Financial Institutions.

xxxii. Panagiotis Delimatsis and Pierre Sauve, "Financial Services Trade After the Crisis: Policy and Legal Conjectures," *Journal of International Economic Law* 13, no. 3 (2010): 837.

xxxiii. European Systemic Risk Board, "Flagship Report on Macro-Prudential Policy in the Banking Sector" (Frankfurt: European Systemic Risk Board, March 2014), https://www.esrb.europa.eu/pub/pdf/other/140303_flagship_report.pdf.

xxxiv. FSB, "Second Thematic Review."

xxxv "Public Consultation System," Banco Central Do Brasil website, accessed November 9, 2017, https://www3.bcb.gov.br/audpub/HomePage?5.