Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements

BY NIGEL CORY AND ROBERT D. ATKINSON | APRIL 2016

The special treatment of financial services data within the TPP sends a dangerous message—that local data storage is necessary for regulatory oversight—that will embolden countries looking to enact digital protectionism policies.

In today's economy, data is to global trade what manufactured goods were in the post-War Bretton Woods system—its lifeblood. However, the data-driven economy is under increasing threat as countries impose a slew of nontariff trade barriers that limit the flow of data across borders. Some of these measures stem from privacy and security concerns, but many constitute naked protectionism. This trend should be of particular concern to the United States, because it holds a leadership position in many of the technologies at the heart of the data economy. Yet the United States has effectively undermined its own interests in one of the most significant trade deals in a generation, the Trans-Pacific Partnership (TPP), by pushing for the financial sector to be exempted from the agreement's prohibitions on measures that would force data to be stored within a country's geographic borders, a practice known as "data localization." This carve-out for financial data sends the wrong message to other nations and creates a policy loophole that other countries could misuse to justify further data protectionism.

Making a special case out of financial data in the TPP is problematic for two key reasons:

- Giving countries a free pass to require certain data to be stored inside their borders will raise costs for financial services firms, and the firms will have to pass those costs on to the businesses and customers they serve.

- The special carve-out validates the false belief that storing data outside a nation is somehow inherently riskier than storing it locally. Such a belief may embolden data mercantilists and undermine U.S. efforts to push back against such measures in places such as China, Indonesia, India, Nigeria, and Russia.

This report first explains why the free flow of data is vital in the modern economy, and why carving out the financial sector will be a mistake. The report then delves into the faulty rationale for the carve-out and explains why it is unnecessary and unwarranted from a data security and financial regulatory oversight perspective, and why it is redundant as a matter of both U.S. law and global trade policy.

In the globally integrated digital economy, the ability of organizations to collect, analyze, and act on data is critical to driving innovation and growth.

Finally, the report offers five recommendations for addressing this issue in the TPP and forging future trade agreements:

1. The United States should work with other parties in the TPP to narrow this loophole through side agreements;
2. The United States should work to exclude this carve-out in future trade agreements, such as the Trade in Services Agreement (TiSA) and the Transatlantic Trade and Investment Partnership (T-TIP);
3. The U.S. government should focus more time and attention on hiring, developing, and consulting with people with relevant digital economy and information technology expertise during future negotiations;
4. The United States should redouble efforts to use international financial forums to address jurisdictional concerns over data access during a financial crisis; and
5. The United States should step up its efforts to build a multilateral policy framework to support the free flow of data.

Free-Flowing Data Drives the Whole Modern Economy

Data flows—which were practically nonexistent just 15 years ago—now play a key role in global trade.[1] 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 information communication technologies (ICT), which depend on cross-border data flows.[2] To paraphrase cyberspace advocate John Perry Barlow, who once said "information wants to be free," today it is fair to say, "information wants to be global." 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.[3]

Indicative of the enormous room for growth in financial data is the estimate that 85 percent of global consumer transactions were still paper-based in 2013.

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.[4] 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.[5] 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.[6] With the increasing use of cloud computing, where the data is stored isn't important; what matters are the rules and management of it.

The United States holds a distinct leadership role in the fast-growing data economy owing to its role as a pioneering innovator and early adopter of ICT. As of 2010, U.S. firms held a 26 percent share of the global IT industry and were the world's largest producers of ICT goods and services.[7] Of the top-20 enterprise cloud-computing service providers in the world, 17 are headquartered in the United States.[8] Of the top 10 Internet firms, 7 are headquartered in the United States.[9] The digitally enabled services that these firms provide have become a key growth engine for the U.S. economy, with exports reaching $356 billion in 2011 (the most recent year for which data are available), up from $282 billion just four years earlier.[10] The economic benefits from the data revolution will only increase as the public and private sectors alike become more data driven.[11] Indicative of the enormous room for growth in financial data, in particular, is the fact that an estimated 85 percent of global consumer transactions were still paper-based in 2013.[12]

Carving Out Financial Data Will Be Costly

Financial services firms are among the most data intensive and thus data dependent of any industry. They rely on the free flow of digital information to support customers and operations in virtually every sector of the economy for 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.[13]

For the United States, allowing other nations to dictate how these networks are designed and built would be harmful to its domestic economy and to its international trade competitiveness. Any trend toward the localization of data and servers will move business activity from the United States to other nations and will raise costs for U.S. financial services firms, who will 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. These additional costs also make the U.S. financial services sector less competitive in foreign markets, especially against local financial firms that do not compete outside their home markets and therefore do not face the additional costs caused by multiple forced localization measures.

International trade law provides ample security for countries to regulate financial markets for both macro- and micro-prudential reasons.

For financial services firms themselves, a trend toward greater data localization actually increases cybersecurity risks as they would have data spread across more data centers—losing the benefits of centralized management. This risk is especially high if firms are forced into using local data storage providers that lack the latest cybersecurity technologies and management practices. Some countries use data localization policies for naked protectionism—to protect and support inefficient and uncompetitive local data center operators—as they are operating under the misguided notion that data centers create large numbers of jobs and investment over the long-term, which they do not.

Cutting off cross-border data flows will also undermine the innovative technologies that are the U.S. financial sector's competitive advantage. 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 consumer 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.[14]

Free Trade in Data Is Under Threat

Free flow in data is under serious threat as an increasing number of countries erect digital barriers, including China, India, Indonesia, and Russia. These nations, for a variety of motivations—some related to privacy and security concerns, many related to naked protectionism—are putting in place policies that balkanize the data economy by limiting cross-border data flows.[15] Such barriers typically involve legal requirements on companies to either store and process data locally or to use only local data servers as a condition for providing certain digital services. In a recent survey by the U.S. International Trade Commission, localization requirements were the most oft-cited digital trade barrier, creating obstacles for 82 percent of large firms and 52 percent of small- to medium-sized enterprises (SMEs) in the digital communications sector.[16] U.S. efforts to push back against these barriers will be undermined by its approach to financial data in the TPP.

In many ways the TPP is an important step toward creating rules against data localization given the growing list of countries that have adopted such measures. Yet, with the carve-out for financial data, regulatory oversight may now be added to the list of public policy objectives misused as justification for data localization policies. In essence, the TPP carve-out for financial services signals that the United States thinks that storing certain kinds of commercial data outside a nation's borders creates risks. But it is a slippery slope between saying that financial services data flow can be restricted but not others; first perhaps health and educational, then all commercial data may follow. If it's needed to protect financial information, why doesn't other information deserve the same treatment?

Yet, as ITIF has written in "The False Promise of Data Nationalism," it is the technological and procedural method of storing and transferring data that determines how safe it is, not the geographical location where the data is stored.[17] 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 companies that move data overseas. For example, if countries pass laws that impose minimum security standards, then those standards follow the data wherever a company might decide to transfer or store it; companies are not able to escape their obligations to abide by the security standards any more than they can escape their obligations to abide by other laws. The same is true for privacy. Organizations cannot escape a nation's privacy regulations just by moving data to another nation. With privacy and cybersecurity laws in place, what then becomes important is effective enforcement to ensure that companies are following the rules for how a country wants to manage and protect data.

The Rationale for the Financial Services Carve-Out Is Faulty

U.S. financial regulatory agencies appeared to have argued for a financial services carve-out for two reasons. First, it appears that they believed that the security of data is affected by its location. Second, some agencies, such as the Federal Reserve, claimed that the carve-out for financial services data in the TPP is necessary to protect the stability of the U.S. financial system and individual financial firms and consumers, particularly in crisis situations such as the 2008 financial collapse. But the truth is that measures recently enacted in the Dodd-Frank Wall Street Reform and Consumer Protection Act have given regulators adequate and more appropriate tools to achieve the same end goal.

The proximate cause of U.S. financial regulators' angst appears to be their experience with the Lehman Brothers' bankruptcy in September 2008.[18] Lehman Brothers was a global business, with its main headquarters in New York, regional headquarters in London and Tokyo, and other offices throughout North America, Europe, Asia, the Middle East, and South America—and within this structure it had thousands of different IT systems. Its main data centers (with approximately 26,000 servers) were in New York, London, Tokyo, Hong Kong, and Mumbai. Given the geographic dispersion of the firm's IT infrastructure, ownership of core IT systems and the data therein became unclear and in dispute when Lehman Brothers declared bankruptcy.[19]

Regulators' angst was focused on both access to data and failures in Lehman Brothers' broader IT system. The 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.[20] This made it difficult for the regulators to access the data needed to unwind positions and ascertain what money was owed to whom.[21]

Yet while these sorts of issues at one time may have represented legitimate regulatory concerns, the United States and other leading economies have worked hard in the wake of the financial crisis to improve oversight of how firms that are designated "systemically important financial institutions" (SIFIs) manage their IT systems and data, especially how these firms plan to store and retrieve data in the event of bankruptcy. This is why the Dodd-Frank Act outlined extensive new rules that require 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."[22] 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. The argument that it was necessary to carve financial data out of the TPP to ensure regulatory access to data is thus faulty, as these living wills require 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 compliance activities) and in the event of a crisis.[23]

U.S. financial firms now need to prove to oversight agencies how they store and plan to retrieve data in the event of a financial crisis.

The Lehman Brothers' experience has made U.S. regulators sensitive to the risk that, in the event of a financial crisis, foreign governments could hold locally stored data out of reach for U.S. authorities. However, if this was the underlying motivation for the exemption of financial services data from rules prohibiting data localization, the issue could be resolved by making the TPP the first building block in a broader framework of agreements that include reciprocity provisions to ensure access to financial data. Regulators could build such a framework over time, with the end objective that U.S. financial firms could only store data in a country that has signed a reciprocity agreement.

Proponents of the carve-out have not explained why regulators cannot use living wills to address any remaining concerns about access to financial data. After reviewing companies' contingency plans, regulators could provide advice to individual firms about how to best 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 could issue additional sector-wide advice for all firms, as it does for other issues.[24] Where these concerns relate to data stored overseas, agencies could ensure that firms make clear what mechanisms are in place to allow the sharing of data in the event of a crisis, just as they would for data stored in Oklahoma. The European Union's approach could be illustrative, as EU regulators require SIFIs to describe in detail how they manage the sharing of information with foreign regulatory authorities.[25] Such a requirement in the United States would help address the underlying fear that U.S. regulators have about data being withheld by another country.

The irony is that the FDIC has essentially admitted that data access concerns were resolved through the Dodd-Frank Act. 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.[26] 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."[27] 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.[28]

"Prudential Exceptions" in Trade Agreements Make the Carve-Out Doubly Redundant

Another reason why a carve-out for financial data is unwarranted is the fact that the TPP already includes a provision that allows countries to take regulatory action in the banking and financial system, even if this action contravenes other parts of the trade agreement, thereby making the carve-out redundant. If U.S. regulators needed a financial institution to store data locally during its bankruptcy proceedings, it could do this and not violate the TPP's rules against data localization.

Countries have long been sensitive to how trade agreements impact their sovereign ability to regulate financial and banking services, including during emergency situations, such as a financial crisis.[29] This is why, ever since the World Trade Organization's (WTO's) Uruguay Round of multilateral trade negotiations in the 1990s, countries have agreed to a wide-ranging so-called "prudential exception" in new trade agreements. It is a standard exception that allows them to contravene other parts of an agreement if doing so is necessary for legitimate, domestic regulatory purposes.[30] The text of the WTO language on domestic regulation states:

> Notwithstanding any other provisions of the Agreement, a Member shall not be prevented from taking measures for prudential reasons, including for the protection of investors, depositors, policy holders or persons to whom a fiduciary duty is owed by a financial service supplier, or to ensure the integrity and stability of the financial system. Where such measures do not conform with the provisions of the Agreement, they shall not be used as a means of avoiding the Members' commitments or obligations under the Agreement.

This provision's inclusion in the TPP provides ample security for countries to regulate financial and banking systems for both macro-and micro-prudential reasons, including the hypothetical scenario where regulators required a financial institution to store data locally as part of bankruptcy proceedings.[31] While the provision sets out a number of specifically allowed measures, the reference to "ensur[ing] the integrity and stability of the financial system" is broad in scope and therefore not limited to these specific examples.[32] The definition was intentionally left open-ended to avoid constraining regulatory authority. Further evidence that it gives regulators broad latitude is the fact that the provision must be "for" prudential reasons, without any of the limiting or narrowing language that is often used in other WTO-based exceptions, such as phrasing that the measures must be "necessary."[33] These differences are important, as there has been considerable debate at the WTO about the difficulty of using exceptions that include such a "necessity test." The prudential exception would not face this challenge if regulators breached TPP rules prohibiting forced localization requirements if they did so for legitimate regulatory purposes, such as for an SIFI's bankruptcy proceedings.

U.S. regulators have not explained why this prudential rule was sufficient for past trade agreements but not for the TPP, especially given the trade policy decisions that the United States has made since it entered TPP negotiations back in 2008.[34] In WTO discussions on the provision, United States Trade Representative (USTR) officials have said that, "the exception in the GATS provided Members with wide latitude to impose prudential regulation."[35] Thus, the North America Free Trade Agreement (NAFTA) included the WTO's prudential exception language, with only a minor addition.[36] The template for the U.S. Bilateral Investment Treaty (BIT), which protects private investment between two countries, included the provision when it was last reviewed by the State Department and USTR in 2012.[37] The same is true of the United States-Korea Free Trade Agreement (KORUS), which entered into force in 2012.[38]

U.S. regulators could push for financial services data to be exempted from future trade agreements that also try to prohibit barriers to cross-border data flows.

Regulators also have not explained why this overly broad approach is preferable to other negotiated outcomes, such as an additional provision within the TPP that seeks agreement between members on how they would cooperate with national regulators on their concerns over access to financial data. The Bipartisan Congressional Trade Priorities and Accountability Act of 2014 shows that a majority of the U.S. Congress wanted the TPP to prohibit barriers to cross-border data flows—without exception.[39]

POLICY RECOMMENDATIONS TO SUPPORT GLOBAL DATA FLOWS

The special treatment of financial data in the TPP touches upon two digital economy issues that are in fundamental tension—the free flow of data and government access to it. Unless nations can put in place a reasonable and consistent framework to govern lawful government access to data, they will be more likely to restrict cross-border data flows, and thus trade and commerce will suffer. Indeed, the growing range of issues pertaining to government access to data underscores the importance for the United States and others to take a more strategic approach to address these issues, both in terms of advancing new trade regimes to establish enforceable rules for free trade in data and in crafting international standards for government access to data.

While the focus of the current debate around data flows has largely been on national security and privacy, the carve-out shifts the focus to domestic financial regulations. This underscores the need for the United States to change not only its current approach, but also to pursue broader international rules around the free flows of and access to financial data.

Recommendation 1: Craft Side Agreements in the TPP to Limit the Risk That the Carve-Out Will Become a Gaping Loophole Ripe for Misuse

Given the TPP has already been signed, the United States should pursue side agreements with TPP member countries on the technical details of an agreement that would specifically address concerns over access to financial data during a financial crisis. As Treasury Secretary Lew has recognized, this requires "threading the needle" in terms of balancing U.S. efforts to push back against data localization policies around the world and regulatory requirements around data access.[40] While it may be tricky, the United States' success in negotiating with the EU on the sharing of criminal and terrorist information (the Umbrella Agreement) and broader commercial exchanges (the Privacy Shield) shows what is possible when political leaders and government agencies are willing to pursue specific data protection agreements.[41]

As a starting point, the United States needs to cut the link between data access and geography and to focus on a mechanism that addresses the actual regulatory concern. In the era of cloud computing, the concern is not about geography but the rules that travel with the data. Regulators should instead recognize how cloud computing can act as an enabler of greater data access, not as a risk. The side agreement should stipulate the steps that respective regulators would take to ensure that SIFIs in TPP countries are readily able to provide access to data, especially as it relates to firms going through bankruptcy proceedings (given that is the focus of U.S. regulators). Regulators in TPP countries should agree to allow such data flows. Transparent, detailed, and technical steps on the enactment of this data access mechanism would address regulatory concerns while limiting the potential for it to be misused by other countries as a mask for digital protectionism as prudential concerns can potentially cover a wide range of issues.

The United States needs to cut the link between data access and geography and to focus on a mechanism that addresses the actual regulatory concern.

The centrality of the U.S. financial system to the global economy means that the Treasury Department and Federal Reserve retain significant influence over global financial issues even after the signing of the TPP. The United States should fully use the financial services committee established as part of the TPP's Financial Services chapter as a forum to implement and monitor any side agreement.[42] Such country-level arrangements would act as the natural complement—and in some regards as an overlapping measure—to the firm-level changes on data management and reporting as under the Dodd-Frank Act.

Recommendation 2: Eliminate Financial Data Carve-Outs Altogether in Future Trade Agreements

The United States should stop pursuing this carve-out in future trade agreements. It is counterproductive to broader efforts to push back against data localization measures, and not only provides a loophole for other countries to misuse prudential concerns to target financial data, but also gives mercantilist-inclined nations cover to extend their protectionism to other kinds of data. The U.S. government should fully embrace its role as a leader in the global digital economy and embed strong cross-border data flow protections in trade agreements for all sectors. The next opportunity to build better rules for data flows will be the Trade in Services Agreement (TiSA) and the Transatlantic Trade and Investment Partnership (T-TIP). TiSA includes 23 countries that represent 75 percent of the world's $44 trillion services market. Similar to the claims made in the TPP, if the T-TIP is truly going to be a "21st-century trade agreement," it must give data flows the same level of consideration it would have given manufacturing in a 20th-century agreement.

Recommendation 3: Step Up International Engagement in Financial Forums

U.S. financial service regulators should redouble efforts to use international financial forums to address remaining concerns about jurisdiction over financial data during a crisis. 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.[43] 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."[44] One clear outcome from the global financial crisis has been the need to improve the governance of financial information and data.[45] 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.[46]

While some progress had been made, there is still a good deal of work to do to improve prudential regulations around the world, as European Central Bank President Mario Draghi remarked in 2014.[47] 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.[48] 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 the United States to lead these efforts if it sees data accessibility as an issue that needs better international coordination. 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.

Recommendation 4: Develop and Deploy Technical Expertise

The United States should work to develop the technical negotiating and analytical expertise to analyze and understand how firms use cloud computing when reporting their "living wills" and fulfilling their other reporting requirements. Such expertise would help regulators assess the living wills to ensure they adequately outline how firms would facilitate data access in the event of bankruptcy. Such an assessment could include test scenarios of what firms outline in their reporting. Technical expertise is critical to keeping regulators and trade negotiators current with ongoing changes in technology and financial business models and services. These changes will continuously affect firms' activities and information management systems that feed information into the reports required by oversight bodies.

Recommendation 5: Champion a Multilateral Framework for Data

The carve-out issue again highlights the need for cooperation on the framework around the global transfer of data. Regional and bilateral trade agreements and thematic agreements (if progress was made at the FSB on financial data rules) should be seen as stepping stones toward a broader multilateral framework that ensures the free flow of global data. As data is so critical to the modern global economy, the United States should push further to protect the free and unfettered movement of data across the globe—for example by championing a "Data Services Agreement" at the World Trade Organization, as ITIF proposed in "Cross-Border Data Flows Enable Growth in All Industries."[49] Such an agreement would commit participating countries to protect cross-border data flows and prevent signatory countries from creating barriers to them. It would be akin to the Information Technology Agreement (ITA)—which 54 countries commendably agreed to expand with 201 new product lines exempted from tariffs earlier this year—but for cross-border data flows instead.

This multilateral agreement would establish specific rules against data localization (as well as rules for government transparency), create better cooperation for legitimate government data requests, and limit unnecessary access to data on foreign citizens. It would also settle questions of jurisdiction when companies encounter conflicting rules, assist nations in reassuring individuals at home and abroad that the era of mass electronic surveillance unencumbered by effective judicial oversight is at an end, and better hold nations accountable for respecting basic civil liberties. And just as the principles of the Geneva Convention are taught to soldiers in basic training, the principles of a Geneva Convention for Data should be taught to network administrators and IT professionals worldwide, thereby ensuring that the ethics and mechanics of the agreement are embedded at all levels of industry and government.

The United States should dispel the misguided notion that data must be stored domestically to ensure that it remains secure, private, and under effective prudential oversight.

CONCLUSION

In many nations, trade negotiators are realizing the importance of the free flow of data across borders and have started working to build an international consensus and enforceable regime to protect these flows. However, at the same time, some governments have sought to erect barriers to cross-border data flows. Extending carve-outs to particular kinds of commercial data sends a dangerous message to nations around the world that cross border data flows are inherently risky.

Just as economic nationalism inevitably leads to lower productivity for firms and higher costs for consumers, "data nationalism" will similarly lead to poor economic outcomes. As a natural leader in the global digital economy, the United States must change its approach to the management of financial data, and dispel the misguided notion that data must be stored domestically to ensure that it remains secure, private, and under effective prudential oversight. The United States should be working to build a global norm of ensuring that rules travel with the data and not a norm of data having to be resident within a country's borders for rules to apply. Just as with privacy and security concerns, regulatory powers over financial institutions should not be hindered by where the data is stored.

The overarching goal should be the establishment of a global framework of interoperable national legal and regulatory regimes that allow cross-border data flows. As part of this, local data center restrictions should be prohibited and data processing should be allowed in whichever locations support optimal security, resiliency, confidentiality of customer information, and technical and operational support. The mixing of post-financial crisis issues with concerns about transatlantic financial data flows (given the demise of Safe Harbor and rise of Privacy Shield agreements to manage data transfers between the United

States and Europe) simply underlines how important it is for the United States to work with TPP parties, European counterparts, and others to ensure the free flow of data.[50]

Beyond the risk of other countries adopting and misusing similar rules for protectionist purposes, it is critical that this approach to financial data not become the global norm through TiSA and T-TIP. However, this is complicated by reports that the United States is unwilling to negotiate financial services regulations as part of T-TIP.[51] It seems unusual that an issue that has featured so prominently in the TPP would not also be a high priority in T-TIP. T-TIP would be an ideal forum to resolve these and other related data flow issues as these two regions have the most complex financial systems, and both of them have highly sophisticated regulatory rules and institutions. The United States should be doing the very opposite and instead seize the opportunity presented by these two agreements to create important new rules to support the global flow of data.

ENDNOTES

1. James Manyika et al., “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; *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.
2. *Information Economy Report 2009*.
3. 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.
4. 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.
5. 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.
6. 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.
7. National Science Board (NSB), Science and Engineering Indicators 2012, (appendix table 6-13, value added of ICT industries, by region/country/economy: 1990–2010; accessed April 18, 2016), http://www.nsf.gov/statistics/seind12/appendix.htm.
8. International Trade Administration (ITA), *2015 Top Markets Report Cloud Computing* (ITA, April 2016), http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf.
9. Shobhit Seth, “World’s Top 10 Internet Companies,” Investopedia, accessed March 4, 2015, http://www.investopedia.com/articles/personal-finance/030415/worlds-top-10-internet-companies.asp.
10. Stephen Ezell, “Digital Trade Act of 2013 Instrumental to Protecting and Empowering the Global Digital Economy,” *Innovation Files*, December 12, 2013, http:// http://www.innovationfiles.org/digital-trade-act-of-2013-instrumental-to-protecting-and-empowering-the-global-digital-economy/
11. Daniel Castro and Travis Korte, “Data Innovation 101: An Introduction to the Technologies and Policies Supporting Data-Driven Innovation” (Center for Data Innovation, November 4, 2013), http://www2.datainnovation.org/2013-data-innovation-101.pdf.
12. Michael Corbat, “CEO Michael Corbat’s Keynote at the Mobile Word Congress,” (speech presented at Mobile World Congress, Barcelona, 2014), www.citigroup.com/citi/news/executive/140225Ea.htm.
13. 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.
14. 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; Johnston, “Investigation Number 332-531,” 6.
15. *Hearing on International Data Flows: Promoting Digital Trade in the 21st Century before the House Judiciary Committee Subcommittee on Courts, Intellectual Property, and the Internet*, 114th Congress (2015) (testimony of Robert D. Atkinson, Founder and President, the Information Technology and Innovation Foundation), http://www2.itif.org/2015-atkinson-international-data-flows.pdf.
16. U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2* (Washington, DC: U.S. International Trade Commission, August 2014), https://www.usitc.gov/publications/332/pub4485.pdf.
17. 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.
18. Data requirements for state-level insurance laws and the Bank Secrecy Act have also been raised in defense of this carve out, but these do not enforce localization, only requiring access to data upon request. For example, the Bank Secrecy Act contains anti-money laundering requirements that financial firms

assist U.S. government agencies in these investigations, including keeping records of cash purchases and other transactions. The law says nothing about where data should be stored, only that it be readily accessible.

19. Lehman Brothers ran a centralized IT system where data from different products and different departments comingled. This was seen as an advantage prior to the crisis, but with bankruptcy, it posed serious challenges to data preservation and the de-coupling of systems as the system fractured. Lehman Brothers had 26,666 servers worldwide. Lehman's largest data centers were in New York, London, Tokyo, Hong Kong, and Mumbai. Lehman's IT department had approximately 6,000 employees (2,900 in the United States, 1,500 at Nomura Europe, 700 at Nomura Japan, and 900 at Nomura India). On top of this, Lehman used approximately 2,700 home grown, third-party, and off-the-shelf software programs to run its global operations. "Lehman Brothers Holdings Inc Plan Trust: Form 8-K," Edgar Online, accessed April 4, 2016, http://www.barchart.com/plmodules/?module=secFilings&filingid=6236156&type=CONVPDF&popup=1&override=1&symbol=LEHKQ; Victoria Lemieux, "Financial Records and Their Discontents," (working paper, School of Library, Archival, and Information Studies, The University of British Columbia, Vancouver, 2012), http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/VC_Lemieux_27_A_1530.pdf.
20. 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.
21. "Lehman Brothers International (Europe)."
22. "Resolution Plans," Board of Governors of the Federal Reserve System, accessed April 4, 2016, https://www.federalreserve.gov/bankinforeg/resolution-plans.htm.
23. 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."
24. 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.
25. European Banking Authority (EBA), "EBA Final Draft Regulatory Technical Standards on the Content of Resolution Plans and the Assessment of Resolvability" (London: EBA, December, 2014), http://www.eba.europa.eu/documents/10180/933992/EBA-RTS-2014-15+%28Final+draft+RTS+on+Resolution+Plan+Contents%29.pdf.

26. 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.
27. Ibid., 26.
28. Ibid., 26.
29. *Hearings on the financial services chapter of the North American Free Trade Agreement*, *Before the Committee on Banking, Finance, and Urban Affairs*, 103rd Cong. (September 28, 1993) (statement by the Hon. John. P LaWare, member of the Board of Governors of the Federal Reserve System), http://www.archive.org/stream/financialservice00unit/financialservice00unit_djvu.txt.
30. Inu Barbee and Simon Lester, "Financial Services in the TTIP: Making the Prudential Exception Work," *Georgetown Journal of International Law,* 45 (2013): 953, http://object.cato.org/sites/cato.org/files/articles/barbee-lester-gjil.pdf.
31. Laura Puccio, "TTIP and Regulation of Financial Markets: Regulatory Autonomy versus Fragmentation" (Brussels: European Parliamentary Research Service, June 2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/559494/EPRS_IDA(2015)559494_EN.pdf.
32. Ibid., 30.
33. World Trade Organization Secretariat, "'Necessity Tests' in the WTO" (note, working document S/WPDR/W/27 presented to the Working Party on Domestic Regulation, December 2, 2003), http://www.ictsd.org/downloads/2008/04/nectest.pdf.
34. Chris Daniels, "First Step to Wider Free Trade," *The New Zealand Herald,* February 10, 2008, http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=10491556.
35. World Trade Organization Secretariat, "Report on the Meeting held on 27 June 2012" (meetings note report S/FIN/M/73 from the Committee on Trade in Financial Services, July, 2012), https://docs.wto.org/dol2fe/Pages/FE_Search/DDFDocuments/42814/Q/S/FIN/M73.pdf.
36. NAFTA (article 14.10(1) added a further description of a legitimate objective that prudential measures may pursue: "the maintenance of the safety, soundness, integrity, or financial responsibility of financial service suppliers."
37. U.S. Department of State, "2012 U.S. Model Bilateral Investment Treaty" (Washington, DC: U.S. Department of State, 2012), http://www.state.gov/documents/organization/188371.pdf.
38. Article 13.10 of the Korea-United States Free Trade Agreement: Exceptions: Notwithstanding any other provision of this Chapter or Chapter Eleven (Investment), Fourteen (Telecommunications), including specifically Article 14.23 (Relation to Other Chapters), or Fifteen (Electronic Commerce), and, in addition, Article 12.1.3 (Scope and Coverage) with respect to the supply of financial services in the territory of a Party by a covered investment, a Party shall not be prevented from adopting or maintaining measures for prudential reasons, including for the protection of investors, depositors, policy holders, or persons to whom a fiduciary duty is owed by a financial institution or cross-border financial service supplier, or to ensure the integrity and stability of the financial system. Where such measures do not conform with the provisions of this Agreement referred to in this paragraph, they shall not be used as a means of avoiding the Party's commitments or obligations under such provisions. It is understood that the term "prudential reasons" includes the maintenance of the safety, soundness, integrity, or financial responsibility of individual financial institutions or cross-border financial service suppliers. "Korea-United States Free Trade Agreement," Office of the U.S. Trade Representative, accessed April 4, 2016, https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file35_12712.pdf.
39. Bipartisan Congressional Trade Priorities and Accountability Act of 2015, S. 995, 114th Cong. (2015), http://www.finance.senate.gov/imo/media/doc/Bipartisan%20Congressional%20Trade%20Priorities%20and%20Accountability%20Act%20of%202015.pdf.
40. "Lew Floats Possibility of Side Deal to Address TPP Data Localization," *Inside U.S. Trade's World Trade Online,* March 16, 2016, http://insidetrade.com/daily-news/lew-floats-possibility-side-deal-address-tpp-data-localization.
41. European Commission, *Questions and Answers on the EU-US Data Protection "Umbrella Agreement,"* (press release, European Commission, Brussels, September 2015), http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm/.
42. This committee was established to, among other things, supervise the implementation of the broader financial services chapter and consider financial services issues referred to it by a member of the TPP.
43. 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.

44. 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.
45. 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.
46. 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.
47. 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.
48. FSB, "Second Thematic Review."
49. Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries (Information Technology and Innovation Foundation, February 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf.
50. Victoria Guida, "Lew Defends Financial Services Data Carveout," *Politico Morning Trade,* February 11, 2016, http://www.politico.com/tipsheets/morning-trade/2016/02/lew-defends-financial-services-data-carveout-senate-to-vote-on-customs-bill-democrats-weigh-in-on-tpp-212657#ixzz43AY2qpUa.
51. "Lew Says EU Open to Excluding Financial Services Regs from TTIP," *Inside U.S. Trade,* March 23, 2016, http://insidetrade.com/daily-news/lew-says-eu-open-excluding-financial-services-regs-ttip.

ACKNOWLEDGMENTS

The authors wish to thank the following individuals for providing input to this report: Randolph Court and Stephen Ezell. Any errors or omissions are the authors' alone.

ABOUT THE AUTHORS

Nigel Cory is a trade policy analyst at ITIF. He previously worked as a researcher at the Sumitro Chair for Southeast Asia Studies at the Center for Strategic and International Studies. Prior to that, he worked for eight years in Australia's Department of Foreign Affairs and Trade and also had diplomatic postings to Malaysia and Afghanistan. Cory holds a master's degree in public policy from Georgetown University and a bachelor's degree in international business and commerce from Griffith University in Brisbane, Australia.

Robert D. Atkinson is the founder and president of ITIF. Atkinson's books include *Innovation Economics: The Race for Global Advantage* (Yale, 2012), *Supply-Side Follies: Why Conservative Economics Fails, Liberal Economics Falters, and Innovation Economics is the Answer* (Rowman & Littlefield, 2006), and *The Past And Future Of America's Economy: Long Waves Of Innovation That Power Cycles Of Growth* (Edward Elgar, 2005). Atkinson holds a Ph.D. in city and regional planning from the University of North Carolina, Chapel Hill, and a master's degree in urban and regional planning from the University of Oregon.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as one of the world's leading science and technology think tanks, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

FOR MORE INFORMATION, VISIT US AT WWW.ITIF.ORG.