ALBRIGHT
STONEBRIDGE
GROUP

Data Localization

A Challenge To Global Commerce and the Free Flow of Information

September 2015

[THIS PAGE IS LEFT INTENTIONALLY BLANK]

EXECUTIVE SUMMARY

Data localization measures – regulations requiring companies to store and process data on servers physically located within national borders – are increasing around the world. These laws pose a growing threat to the information technology sector and beyond, with the potential to cause companies to withdraw operations from key markets, harm Internet users, and further fragment the global Internet. This paper explores data localization developments in the European Union, Russia and Brazil, and offers thoughts on the best routes to reverse current trends.

Five underlying issues are central to understanding the global growth of data localization measures. The first, and most fundamental, is a simple contradiction – the Internet is global but regulation is local. The past decade of developments in cyberspace has clearly shown that the vision of the Internet as a borderless medium, somehow beyond the reach of national authorities, is out of line with reality. In the midst of rapidly changing conceptions of national security, privacy and commerce in the digital age, governments have increased their efforts to exert control over information both inside and flowing across their borders.

Second, governing cyberspace—unlike other global challenges-- requires the constant cooperation of the private sector, a broad array of NGOs, and nation states. In particular, large firms holding vast quantities of data about consumers must first comprehend and then confront a mix of global and national regulations. Governments, meanwhile, struggle with how to induce cooperation from companies that control the data and means of access. In order to maintain the free flow of information that drives commerce, government and the private sector must at times act together.

Third, people around the world have awakened to the vulnerability of personal information in the digital age. Whether through cyberattacks from rogue actors, espionage from foreign governments, or the use of personal information by companies for commercial purposes, traditional definitions of private information no longer hold true. In some regions, citizens have pressured their governments to wrest information back under their control. Driven by these concerns, many countries are seeking to assert physical control over digital information – and data localization has become a means to achieve this goal.

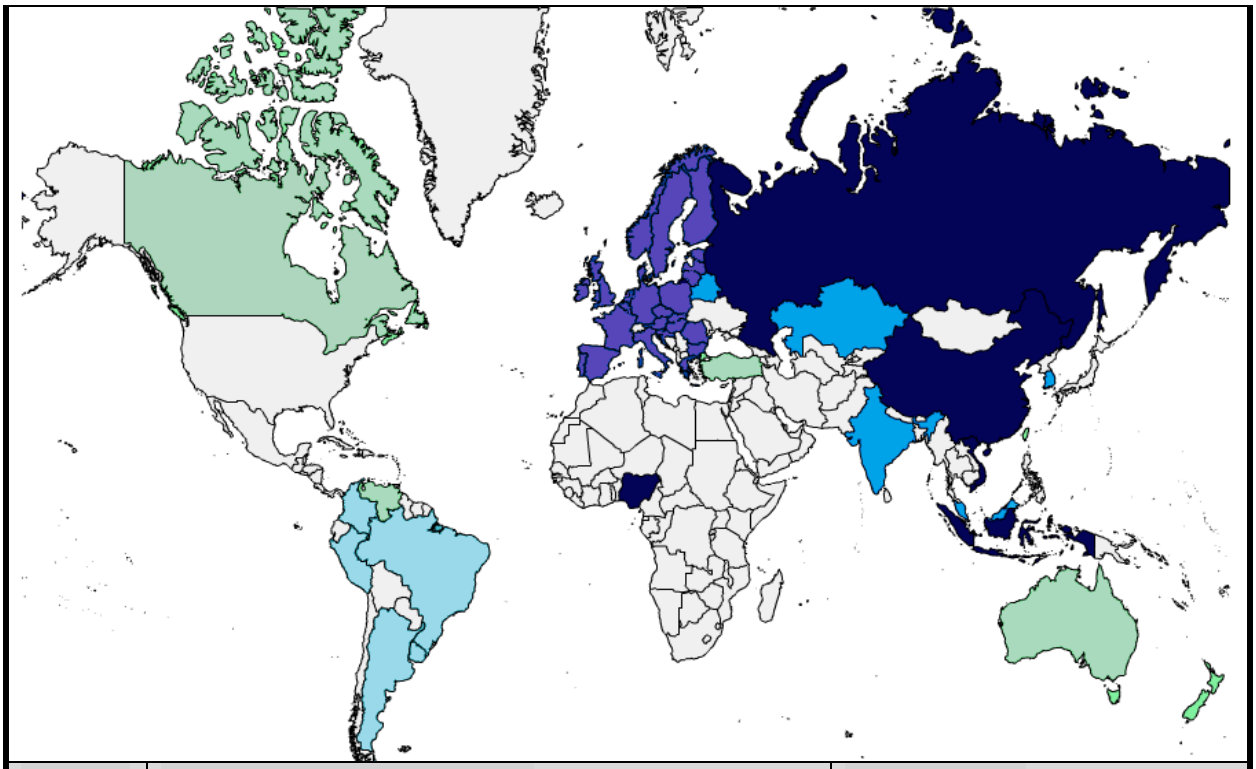
Fourth, data localization measures are a symptom of so-called “data protectionism,” a new twist on the traditional desire of governments to promote homegrown industry. But this trend – magnified by the vision of expanded benefits in the global economy – poses a practical contradiction. On the one hand, data localization is meant to promote short-term economic development through the construction of expensive data centers and the creation of a limited number of high-paying technical jobs. On the other hand, the disruption caused by requiring companies to store information within national borders can have a severe economic impact across sectors, leading to a reduction in foreign investment.

Finally, a lack of natural coalitions to combat data localization hinders efforts to roll back the regulatory tide in many countries. In autocratic nations, localization measures are used to control information, stifle the voices of advocates of free expression, and strangle political dissent. In other regions, including Europe and Latin America, concerns over foreign surveillance and privacy have united the left and right, giving a major boost to proponents of localization laws. Foreign firms have been strong opponents of data localization, but to date domestic firms have not stepped up in defense of their own self-interest. Those voices are perhaps the most critical to turn back the wave of data localization.

Failure to take action will place companies and NGOs in the unenviable position of being forced to choose between abandoning key markets or complying with regulations that will harm their customers and their economic interests. More important, companies and NGOs could become complicit in the activities of authoritarian regimes, and held responsible in the eyes of the public for the fates of individuals and groups whose data is seized, hijacked, or manipulated by regimes that value neither free expression nor privacy.

Halting this trend will not be easy as long as governments around the world continue to view the free flow of information as a political threat. A new path forward, based on a nuanced understanding of what is driving these measures, is necessary to slow the advance of data localization.

GLOBAL SPREAD OF DATA LOCALIZATION*



COLOR	STRENGH OF MEASURES	COUNTRIES
	Strong: Explicit requirements that data must be stored on servers within the country.	Brunei, China, Indonesia, Nigeria, Russia, Vietnam
	De Facto: Laws that create such large barriers to the transfer of data across borders that they effectively act as data localization requirements.	European Union
	Partial: Wide range of measures, including regulations applying only to certain domain names and regulations requiring the consent of an individual before data about them is transferred internationally.	Belarus, India, Kazakhstan, Malaysia, South Korea
	Mild: Restrictions on international data transfers under certain conditions.	Argentina, Brazil, Colombia, Peru, Uruguay
	Sector-specific: Tailored to specific sectors, including healthcare, telecom, finance, and national security.	Australia, Canada, New Zealand, Taiwan, Turkey, Venezuela
	None: No known data localization laws.	Remaining Countries

*Data localization laws, by their nature, are difficult to precisely categorize, and are constantly changing. This map is ASG's best assessment of current regulations at the time of publication.

REGIONAL ANALYSIS

Countries in nearly every region of the world (see map, page 5) have taken a growing number of steps to control information flowing across their borders. These measures vary widely in both scope and intensity, including strong and explicit requirements for all data to be stored within a country's boundaries; rules restricting the flow of data across borders that result in *de facto* localization; and more limited measures focusing on specific sectors.

Though the spread of data localization is a global trend, the details, motivations, and scope of these measures are unique to each country. The following case studies – the European Union (EU), Russia, and Brazil – illustrate how data localization laws are being used around the world: to expand national understandings of privacy and other Internet norms beyond a nation's boundaries; to exert political authority by controlling information; and to assert power in the face of technological dominance of U.S. companies.

EUROPEAN UNION

In Brussels, officials have justified data localization as part of broader efforts by the European Union and national governments to regain control of information owned by U.S. multinational companies and subject to the prying eyes of the U.S. government. Complex compliance requirements, driven by a web of recent court decisions and potential new regulations, may cause companies to believe they have no choice but to relocate server infrastructure in Europe. The key challenge in the near future for U.S. companies and others will be to make certain that the European framework stays within the continent and does not leak beyond the European Union.

Political momentum for data privacy grew in 2013 after Edward Snowden revealed U.S. National Security Administration (NSA) programs to monitor European citizens and political leaders, including taps on the phones of German Chancellor Angela Merkel and French President François Hollande. The disclosure of these programs shifted opinions in Europe about the protection of digital information, raised suspicions about U.S. companies and their possible cooperation with the U.S. government, and prodded European officials to act.

The post-Snowden EU Commission, led by Jean Claude Juncker, has elevated privacy issues to the top of its agenda and has created new positions and institutions focusing on issues surrounding data storage and ownership. The Commissioner for the Digital Economy, Günther Oettinger, has been particularly blunt about his desire to wrest control of information from foreign entities, saying in February that, "The Americans are in the lead, they've got the data, the business models and so the power."[1]

At the top of Commissioner Oettinger's agenda is to update the European Union's "data protection framework," created in 1995, which codified the protection of personal information as a right of European citizens. The updated regulations, which have been under negotiation since 2012, could expand the jurisdiction of all EU data protection requirements to include any company that offers services to EU citizens, regardless of whether the company has a physical presence in Europe. This new directive, which Commissioner Oettinger hopes to finalize by the end of the 2015 legislative session, could force international Internet and technology companies to work within Europe's conception of data privacy.

ECONOMIC CONSEQUENCES OF DATA LOCALIZATION

Data localization can have significant consequences in a global economy in which the Internet drives economic growth and enables commerce for industries far beyond the information technology sector. By adding restrictions on how and where data is stored or transferred, data localization poses a fundamental threat to the free flow of information across borders and the maintenance of global supply chains. Such regulations not only affect email communication, personal records, and social media services, but also limit access to information on which the manufacturing and the service economies depend.

The temptation to pursue data localization measures to stimulate local and national economies is understandable. Data centers, which often house more than 100,000 individual servers, cost an average of $43 million to construct in the United States.[2] Experts estimate that advances in cloud computing will more than triple worldwide data traffic over the next five years. Such predictions have created an expectation that hundreds of new data centers will need to be built, with thousands of high-paying jobs to support them.

But experience to date in both Europe and the United States indicates that while construction of data centers creates employment opportunities, they are relatively short-lived. For example, only 50 people are needed to support a $1 billion mega-data center built by Apple in the small town of Maiden, North Carolina.[3] Visions of years of enormous property tax benefits are outweighed by the incentives that local governments are required to pay to lure companies to locate in their jurisdiction and by the need to subsidize the large amount of electricity required to run a data center.

On a macro basis, studies indicate that data localization regulations can have damaging long-term consequences. Potential disruptions in information flows cause uncertainty among companies and leads to lower levels of foreign investment. In addition to its impact on businesses, localization tends to reduce services and increase prices for domestic consumers.

The European Centre for International Political Economy examined the overall impact of localization measures in seven countries – Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam – and found negative impacts on GDP and foreign investment. The study found that localization regulations cost EU citizens an estimated $193 billion per year, due in part to higher domestic prices, and that Vietnam's strict 2013 data localization requirement has reduced its GDP by 1.7 percent.[4]

This new data protection framework would be added to current restrictions limiting the flow of information out of the European Union. Under current rules, data on EU citizens can only be sent to national jurisdictions that the Commission has found have "adequate protections" for storing data, or to foreign companies who have contractually agreed to protections. The United States, for example, is not currently considered to have such protection; only through a separately negotiated "Safe Harbor" agreement can companies in the U.S. process data on EU citizens. These companies must also agree to a series of more strict data protections.

As a result of the Snowden revelations, there have been calls for Europe to drop the Safe Harbor agreement, or at least reform it to ensure greater protections for EU citizens. The European Court of Justice (ECJ) is currently considering the issue, and on September 23 the ECJ's advocate general found that the Safe Harbor agreement fails to adequately protect information on EU citizens when it is stored and processed in the United States.[5] While this opinion is nonbinding, it indicates that Safe Harbor as it currently exists is likely to be revisited – adding to the uncertainty for companies that rely on the agreement to transfer data across the Atlantic. Changes to Safe Harbor could result in effectively requiring data localization by prohibiting European citizen data from entering the U.S.

Implications of the "right to be forgotten"

This is not the first time the ECJ has taken a bold stance on data privacy. In 2014, the court ruled that citizens had a "right to be forgotten" – that is, the right to petition search engine providers to remove links to information about them that are found to be "inadequate, irrelevant or no longer relevant."[6] Following the decision, search engines worked with governments to develop standards for judging and removing search results according to these criteria. To date, Google has evaluated nearly one million links and removed more than 40 percent of them from its European domains (for example, .de for Germany and .fr for France).[7]

Now, the "right to be forgotten" has led to a new twist on data regulations and jurisdiction. French regulators have mandated that when Google removes materials under the "right to be forgotten" regime, it must do so not only in the European Union but throughout all its domains, including Google.com, the global service most frequently accessed by users in the United States and around the world. On September 21, Google lost its appeal to France's privacy administration, the Commission Nationale de l'Informatique et des Libertés (CNIL). It remains to be seen whether the authority will levy financial penalties against companies that do not abide by the regulations.

By attempting to extend the European standard, the French could give credence and credibility to data regimes – including harsh data localization measures – propounded by far less democratic governments. This could also create a dangerous precedent, where national governments each try to impose local laws in cyberspace, creating overlapping and contradictory mandates for Internet companies.

National regulations

The jurisdictional issues resulting from privacy regulations such as the right to be forgotten illustrate the challenge that the region faces when considering more strict data localization requirements. As the EU attempts to unify data protection measures, individual national regulations imposing data localization could take hold. The most stringent of these proposals have not yet gained significant traction in legislatures, but they reflect the growing desire of many Europeans for increased government action to protect information.

Individual governments have also begun to test data localization as a tool to protect information. In Germany, for example, Angela Merkel has publicly supported initiatives to create a "pan-European network," isolating email and telephone communications originating in Europe. This year Berlin also established a government cloud infrastructure (the "Bundes-cloud") as part of its plan to consolidate IT infrastructure and localize government data by 2022. The German Interior Ministry described the Bundes-cloud, which is scheduled to begin operating at the end of 2018, as a reaction to "more and

more IT companies processing and storing data in the Internet, outside of our networks and outside of Germany."[8]

Europe faces a crucial decision point as it considers new region-wide data protection directive. As the EU Commission reviews issues related to the updated privacy framework, it will be important to monitor for threats including explicit data localization requirements; regulations in specific nations that could spread across the region; and increased restrictions on data transfer outside of the European Union. These requirements could result in significant economic damage.

Economic consequences

The growing array of regulations and court decisions strengthening data protection and privacy across Europe could have significant long-term economic costs. An analysis by the European Centre for International Political Economy found if the EU were to implement proposed data protection measures, GDP and foreign investment would decline by nearly one-half of one percent and four percent, respectively.[9] Member nations that enact strict data localization requirements that go beyond the basic data protection directive could further wound their economies.

Localization measures will also prove costly to burgeoning start-ups and mid-sized companies, which rely on leasing or renting server space from larger enterprises to develop new technologies and sell services and products. In addition, measures that restrict data or increase the difficulty of navigating complicated privacy regulations could further dampen the prospects of the European technology industry. According to a study by the Business Roundtable, an association of U.S. CEOs, data localization measures will, "result in a slowing of technological innovation and prevent companies from offering certain products and services, consequently dampening economic growth."[10]

In addition, efforts to isolate European data could fundamentally alter the architecture of the Internet, which has long favored technical efficiency over political considerations. If increasing regulations drive the construction of additional data centers in Europe, the resulting inefficient patchwork system would restrict information flows across borders. This could facilitate the so-called "balkanization" of the Internet, increasing barriers to integration with the global digital economy.

RUSSIA

In Russia, the control of information – and strict data localization in particular – has been part and parcel of a comprehensive crackdown on political dissent and the perceived threat of foreign meddling in Russia's domestic politics. In his attempt to regulate U.S. firms and others, President Vladimir Putin has capitalized on a growing patriotic sentiment and sense that Russia is once again beset by foreign enemies in the wake of the crisis in Ukraine. In recent months, however, politics appears to be giving way to the practical economics of the situation.

Since Putin's return to the Kremlin in May 2012, Russian lawmakers have enacted a number of measures aimed at curbing outside influence over the country's economic and political life. Recent pressure to tighten data localization regulations arose in this context and fit within an overall campaign to curb domestic political activity, limit free expression, intimidate political opponents, restrict foreign NGOs and foundations, and impose foreign ownership caps on media enterprises.

DATA SEIZURE, HUMAN AND CORPORATE RISK

Data localization rules, because they often give authorities the ability to seize personal information, not only pose a threat to citizens but also to companies operating within those nations. Perhaps nothing better illustrates the possible impact of these laws than the 2005 jailing of the Chinese dissident, Shi Tao. The case resulted in a lengthy jail sentence for the accused and reputational damage to the American Internet giant Yahoo!.

In 2005, Chinese authorities demanded that Yahoo! – which was operating in China with a local partner, as required – turn over personally identifiable information about a dissident lawyer, Shi Tao. Shi had reportedly distributed a Communist party document, which directed journalists not to report on certain aspects of the anniversary of the 1989 Tiananmen Square protests. As a result of the investigation, Shi was sentenced to ten years in prison for divulging "state secrets."

Backlash against Yahoo! in the United States and elsewhere was swift and harsh. Media outlets closely covered the developments, the prisoner's family and anti-China groups filed a lawsuit against Yahoo!, and international NGOs called for an explanation of the company's involvement. Shi was deemed a political prisoner by many human rights organizations, and a Congressional investigation was launched. At one hearing Congressman Tom Lantos told Yahoo! co-founder Jerry Yang, "While technologically you are giants, morally you are pygmies." [11]

This case was one impetus for the creation of the Global Network Initiative, an alliance of companies, NGOs, and investors working to protect privacy and Internet freedom. In its wake, Yahoo! created a business and human rights program advocating for free expression and privacy, a human rights fund for the legal defense of dissidents, and an annual human rights and transparency report.

Ten years later, the Shi Tao case still casts a long shadow. By forcing data to be stored within a country's border, new laws allow local police and public security personnel to physically seize machines on which data is stored. In a worst-case scenario, authorities could force a foreign company to turn over records that could implicate individuals who had participated in protests or other acts of civil defiance. Western human rights groups, in turn, would no doubt accuse companies of complicity with these acts of authoritarian regimes.

Since 2007, Russia has imposed data protection measures similar to those found in other parts of Europe. Those requirements ensure that users must consent before companies transfer their personal information, and that consumers be notified in the case of a data breach. In addition, foreign companies operating in Russia have struggled with a heavy bias shown toward firms founded in the country, which follow the rules without question. Russia has also passed "right to be forgotten" legislation, which comes into effect on January 1, 2016. Each of these measures reflects the growing number of attempts by the Russian government to assert political authority over the rapidly growing Internet sector.

Current legislation

The latest legislation – the 242-FZ law, which went into effect September 1, 2015 – adds a specific data localization requirement to this existing data protection framework. The new regulation requires

"personal data operators" to collect, store, and process any data about Russian users in databases inside the country and to inform Russian authorities of the location of their data centers. In addition, the law provides authorities easier access to information and imposes harsh penalties on non-compliant companies. Finally, it restricts Russian users' access to any website that violates the nation's data protection laws.

In the six months leading up to the law's implementation, which included a meeting between Western business leaders and President Putin, the government suggested that it was receptive to complaints raised by companies operating in Russia. Uncertainty over the definition of personal data and the scope of the law dominated the talks between Russian authorities and foreign Internet companies. Foreign companies also questioned whether the new law would apply to businesses that do not maintain a physical presence in the country. A great many Russian firms also raised concerns about the potential disruption that the measures might cause average citizens, for example, who travel overseas. Adding to the confusion, authorities appeared to give some social media companies an exemption, saying the information they store would not qualify as "personal information."

Nevertheless, Russia's media regulator and telecom oversight agency, Roskomnadzor, decided to move forward without significant changes to the law. In September Roskomnadzor confirmed the move, but suggested it was beyond the agency's capabilities to monitor compliance effectively. As of this writing, the latest indication is that even companies with no physical presence in the country will be held to the requirements of the new legislation. Authorities have pledged to check the compliance record of any company processing personal data in Russia.

Well-connected interests, including many longtime associates of President Putin, support the law. Among them are the law enforcement and national security communities, who see the law as a tool to reduce Russia's vulnerability to Western pressure and economic sanctions. In addition, some oligarchs and large Russian IT firms have invested heavily in building server farms, creating a de facto commercial lobby that supports full implementation of the law. Other players in the Kremlin's political operations see the new requirements as a potential tool that can limit the reach of social media platforms, civil society, and foreign NGOs in the run-up to next year's parliamentary elections.

Russian Internet ombudsman Dmitry Marinichev indicated that a new round of talks between the government and IT businesses may occur at the end of 2015. If these talks take place, they could be an important dialogue for international companies struggling to maintain operations in the country.

Going forward

There are two possible paths that Russia will take moving forward. In one scenario, hard-liners prevail, the law takes full effect, and over time companies will either try to navigate its strict requirements or decide to leave the market. How far the government will go in trying to enforce this regulation remains to be seen, although it is unlikely that Moscow will try to enforce the requirements strictly within the next year. In a worst-case scenario, authorities would invoke the law, use data to identify activists, and detain or jail them.

A second possibility is that pragmatic voices will prevail and compliance with the law will remain half-hearted yet highly arbitrary. The rationale behind this would likely be economic, as a strict interpretation of the legislation would be damaging to the Russian economy and the burgeoning IT sector, which has begun to demonstrate its value to an economy dominated by the energy and raw

materials sectors. This would allow Russian authorities to maintain a hardline public stance, play to their citizens' chauvinism, continue to scapegoat Western firms, and claim that they are protecting their citizens' data – all without harming foreign investment or economic growth.

BRAZIL

One of the major obstacles facing opponents of data localization has been the lack of committed allies to back up the arguments of U.S. companies. Most recently in Brazil, an unusual alliance of outside governments and companies joined forces with a group of Brazilian firms to turn back an effort by some officials to impose one of the world's most restrictive data localization regulations. The regulation stood out among an otherwise progressive and innovative approach to regulation of cyberspace.

Although data localization efforts in Brazil date back to 2009, regulation only gained traction after Edward Snowden's 2013 disclosure revealed that American spy agencies had eavesdropped on President Dilma Rousseff's personal communications. The revelations caused an uproar in Brazil; President Rousseff called the revelations "incompatible" with a relationship among allies, and postponed a state visit to Washington in protest.[12] Michael Shifter, President of the American think tank Inter-American Dialogue, said the revelations, "touched a real nerve in Brazil, a country that prizes its sovereignty and is understandably sensitive about such abuses."[13]

Internet Bill of Rights

In 2013, the Brazilian National Congress began to consider a sweeping bill known as Marco Civil da Internet legislation, or the "Internet Bill of Rights." Among other provisions, initial drafts of the legislation guaranteed so-called net neutrality (guidelines promoting equal access to the Internet) and stronger data privacy rights. The draft also included a strict data localization regulation, Article XII.

Many Brazilian lawmakers supported localization because it enabled them to appear to be standing up the United States, which played well domestically in the wake of the NSA revelations. Others justified Article XII by arguing that it would help to better protect information from foreign surveillance and give Brazilian courts better access to documents stored by multinational technology companies. Under the current international system, judges and lawyers must make requests through cumbersome Mutual Legal Assistance Treaties (MLATs), which have not been updated for the Internet age.[14]

Recognizing the threat posed by Article XII, nearly 50 organizations from 18 countries engaged in a letter-writing campaign to individual members of the Brazilian Congress, urging them to reject the data localization provision. The coalition was composed of Internet and telecommunications industry organizations, as well as international chambers of commerce from Latin America, North America, Europe, and Asia.

Advocates argued that forced localization that would harm the country's long-term interests for three reasons. First, coalition members said that increasing the number of data centers – as required under the law – would actually reduce security by increasing the number of facilities requiring physical protection and maintenance. Second, the coalition generated evidence that users and companies relying on computational capacity and bandwidth would face higher costs. Finally, the coalition warned that Brazil would be unable to benefit from many innovative cloud services and its competitiveness would be reduced across a range of industries.

These efforts and arguments proved effective. In the buildup to the 2014 NetMundial global Internet conference in São Paolo, the U.S. government – fearing that Brazilian data localization could set a bad precedent – added its voice to the chorus of concern. Ultimately the Brazilian Congress stripped Article XII from the Marco Civil, clearing the way for the legislation to be signed into law.

Lessons from successful collective action

In the case of Brazil, the collective action of multinational companies and industry groups helped persuade authorities that data localization would hurt the nation's long-term political and economic interests. Gathering the right allies took place in tandem with a highly targeted campaign aimed at a very specific provision in a broad piece of legislation. Brazil has to date been the exception in the global fight against data localization, demonstrating an ability to put long-term economic interests ahead of short-term political gain.

Data privacy and protection remain at the forefront of debate in Brasilia, which, like many capitals, continues to grapple with how to best adapt to the development of disruptive technologies and the transition to a digital economy. The Brazilian government is now considering public comments on the implementing regulations for the Marco Civil, which officials in Brasília hope will serve as a global model. A broad array of stakeholders continue to provide input and advocacy to help shape more targeted and effective data protection regulations, but it now seems unlikely that Brazil will take steps as extreme as full data localization.

NEXT STEPS

As the movement for data localization has gained momentum, companies and other institutions are realizing the economic and institutional dangers that localization presents – but actions taken thus far have done little to reverse the trend.

In part, the failure to adequately address the problem stems from the fact that no one-size-fits-all solution is available, and the most effective path forward will be different in every market and for each company. Firms will have to take stock of their method of hosting data, the extent of their multinational footprint, and the volume and type of data they control. Crafting a strategy to fit separate nations will require the ability to look beyond the regulations to understand the underlying political, economic, and cultural elements driving governments to adopt these measures.

To succeed, companies must also think like the governments that find themselves under increasing pressure from internal and external sources– including from their own agencies and citizens. Judicial and national security personnel struggle through the lengthy MLAT process to obtain information locked in servers abroad. Citizens are demanding protection from foreign surveillance, and assurances about how and when companies can use their personal data. There is also an eagerness to protect their own technology industries by increasing investment and employment in communications technology.

Any successful strategy to combat these measures must also incorporate an understanding of the key non-government stakeholders in each market. Technologists and NGOs that have built and guarded the Internet should be part of that conversation, however the most critical actors may well be local companies whose voices will better resonate with national decision makers. Understanding the political

priorities and interests of each stakeholder will be necessary to develop an engagement strategy that can stop, fix or launch rules, laws or regulations.

Many firms are beginning to address localization and other issues surrounding the storage and use of data. They are working to better encrypt and protect data; conducting human rights assessments before they enter new markets; avoiding locating data centers in countries that limit Internet freedom; embracing transparency about their operations; and attempting to multiply their power by joining with NGOs and others through organizations such as the Global Network Initiative.[15] Given the limited power of a single company – and increasing anti-Americanism around the world – this last step may prove to be the most crucial.

International trade negotiations are another potential venue for action. Companies should press their governments to formally list data localization measures as non-tariff trade barriers. The U.S. Trade Representative hopes to include provisions forbidding data localization in the Trans-Pacific Partnership, and organizations should clearly state their support for its inclusions in the TPP and other major trade agreements.[16]

Efforts to roll back the tide of data localization have done little to slow the advance of these measures to date. However, recent history reveals that it is possible to protect the privacy and security of citizens' data without resorting to data localization or other measures restricting the free flow of information. Coordinated and focused coalitions of multinational and local industries and NGOs that work together to expose the threat to national economies, local industry and consumers can be effective. Data protection without data protectionism is possible, but only if organizations come together to prevent governments from attempting to redraw the boundaries of the Internet.

ENDNOTES

[1] Fairless, Tom. "Europe's Digital Czar Slams Google, Facebook." Wall Street Journal. February 24, 2015. http://www.wsj.com/articles/europes-digital-czar-slams-google-facebook-over-selling-personal-data-1424789664
[2] Loretta Chao and Paulo Trevisani. "Brazil Legislators Bear Down on Internet Bill." Wall Street Journal. November 13, 2013. http://www.wsj.com/articles/SB10001424052702304868404579194290325348688
[3] Rosenwald, Michael. "Cloud centers bring high-tech flash but not many jobs to beaten-down towns." Washington Post. November 24, 2011. http://www.washingtonpost.com/business/economy/cloud-centers-bring-high-tech-flash-but-not-many-jobs-to-beaten-down-towns/2011/11/08/gIQAccTQtN_print.html
[4] "The Costs of Data Localization: Friendly Fire on Economic Recovery." European Centre for International Political Economy. No. 3. 2014.http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf
[5] Tung, Liam. "Safe Harbour: Data sharing rules are invalid, says European court expert." ZDNet. September 23, 2015. http://www.zdnet.com/article/safe-harbour-data-sharing-rules-are-invalid-say-european-court-expert/
[6] "Press Release: Google Spain SL, Google Inc. v Angencia Espanola de Proteccion de Datos." Court of Justice of the European Union. May 13, 2014. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf
[7] Crovitz, Gordon. "Hiding on the Internet." Wall Street Journal. August 30, 2015. http://www.wsj.com/articles/hiding-on-the-internet-1440975213
[8] "Data Localization Requirements Through the Backdoor? Germany's "Federal Cloud", and New Criteria For the Use of Cloud Services by the German Federal Administration." National Law Review. September 16, 2015. http://www.natlawreview.com/article/data-localization-requirements-through-backdoor-germany-s-federal-cloud-and-new
[9] "The Costs of Data Localization: Friendly Fire on Economic Recovery." European Centre for International Political Economy. No. 3. 2014.http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf
[10] "Promoting Economic Growth through Smart Global Information Technology Policy. The Growing Threat of Local Data Server Requirements." Business Roundtable. June 2012. http://businessroundtable.org/sites/default/files/legacy/uploads/studies-reports/downloads/Global_IT_Policy_Paper_final.pdf
[11] "Yahoo Criticized in Case of Jailed Dissident." New York Times. November 7, 2007.http://www.nytimes.com/2007/11/07/technology/07yahoo.html?_r=0
[12] Forero, Juan. "NSA spying scandal spoils dinner at the White House for Brazil's president." Washington Post. September 17, 2013. https://www.washingtonpost.com/world/nsa-spying-scandal-spoils-dinner-at-the-white-house-for-brazils-president/2013/09/17/24f5acf6-1fc5-11e3-9ad0-96244100e647_story.html
[13] Forero, Juan. "Brazil TV to release NSA documents that show U.S. spied on Petrobras." Washington Post. September 8, 2013. https://www.washingtonpost.com/world/brazil-tv-to-release-nsa-documents-that-show-us-spied-on-petrobras/2013/09/08/8c4cdaf6-18d0-11e3-a628-7e6dde8f889d_story.html
[14] MLAT treaties are bilateral or multilateral agreements to provide information related to public safety, taxation, or national security investigations. Courts or governments must engage in a lengthy formal request process that is becoming increasingly common when digital information is stored abroad. In addition, MLATs are a patchwork of treaties, leaving some jurisdictions out of the reach of tax or law enforcement oversight.
[15] The Global Network Initiative. https://www.globalnetworkinitiative.org/
[16] "Trans-Pacific Partnership: Summary of U.S. Objectives." Office of the United States Trade Representative. https://ustr.gov/tpp/Summary-of-US-objectives