ITI Forced Localization Strategy Briefs

July 2016

Contents

1101 K Street, NW Suite 610
Washington, D.C. 20005
(202) 737 - 8888 | www.itic.org

ITI Forced Localization Strategy in Brazil

Background

The Brazilian government continues its effort to nurture its domestic ICT industry through local content and local development requirements in various laws, including a number of programs for tax waivers in case of local manufacture. Additionally, multiple regulations require or give preference to locally produced ICT goods and services in government procurement, including in the *CERTICS* certification program, which favors local software development. There are also concerns in the *Processo Productivo Basico,* which requires a minimum level of local content. This process is currently being challenged at the WTO and a decision is expected to be issued by year end.

Data localization concerns remain as the *Marco Civil* is implemented alongside Brazil's current data protection draft legislation. Current data protection and cybersecurity initiatives—including *Decree 8135* that sets cybersecurity standards for government procurement—have the potential to force companies to use local data centers in order to comply with actual or *de facto* requirements.

Current State-of-Play

ITI has submitted numerous comments on various cybersecurity and data protection initiatives in Brazil. Additionally, ITI traveled to Brazil three times in 2015 and once in 2016 (with at least one more trip planned for June 2016) to meet with key government agencies including the Ministry of Communications, Ministry of Justice, Ministry of Trade, and the Ministry of Planning.

ITI Forced Localization Strategy in China

Background

China's pursuit of forced localization measures has resulted in an increasingly difficult business environment for the tech industry. Recent years have seen security concerns give political weight to sections of the Chinese government that have long supported restrictive trade and investment policies as a way of developing domestic industry at the expense of foreign firms.

The combination of a rising cognizance of the importance of cybersecurity, a sense of vulnerability vis-à-vis foreign technology, traditional views of the political importance of controlling information, and a sense of leverage from the size of their market have led to wide ranging localization policies. There are data storage and transfer requirements in the health and finance sectors, multiple measures requiring the localization of data centers, highly restrictive investment regulations, and a growing informal push to buy domestic via the "secure and controllable" moniker.

Current State-of-Play

There are a number of laws and regulation that are already in force, and many that are still in draft form, including a major piece of legislation, China's draft *Cybersecurity Law*. Due to its broad repercussions for many other forms of localization policies (procurement restrictions, licensing difficulties, server localization, and data storage and transfer) this draft law is a focus on ITI advocacy in China. There is a growing cognizance of data privacy and concerns on vulnerability of data that is transferred to servers outside of China, particularly routed through the United States. As a result, Chinese ministries continue to include data localization requirements in their draft regulations. All-in-all, the Chinese government has maintained a consistent message in recent years that they will continue to move forward with data residency and localization requirements. ITI and members are working to show the economic damage that these measures will have on the Chinese economy long-term, both for domestic SMEs as well as growing Chinese multi-nationals across sectors. The Chinese government has shown a greater concern with cybersecurity and protection of citizen personal information from company use, and less concern with government access to citizen and corporate data.

ITI Forced Localization Strategy in India

Background

In December of 2013, the government of India published its revised *Preferential Market Access Policy for government procurement* (*PMA-G*). While the revised policy was an improvement over the original *PMA* requirements that did not exclude private sector procurements or managed service providers, there were still many areas of the policy that remained unclear or that were of concern to industry. The following March, together with DigitalEurope, JEITA, TIA, and the USIBC, ITI submitted joint industry comments to India's Department of Electronics and IT (DeitY) on the *PMA-G*. These comments focused on encouraging the GoI to clearly define the scope and processes of the requirements to better ensure their smooth implementation. However, since its publication the *PMA-G* policy continues to create confusion and barriers for industry. Following the publication of further *PMA-G* implementation guidelines in November 2015, ITI submitted addition comments to address many of the same unresolved issues concerning product scope, liability for product sourcing, notification of products, and analysis and certification for domestic content.

ITI is also tracking India's *National Data Sharing and Accessibility Policy* from 2012 (*NDSAP-2012*). In 2016, ITI member companies are facing issues related to the implementation of this four-year-old policy. Section 10 of the NDSAP that states that "[d]ata will remain the property of the agency/department/ministry/entity which collected them and reside in their IT enabled facility...." The policy covers "non-sensitive data available either in digital or analog forms but generated *using public funds*..."

Current State-of-Play

ITI has not yet received a reply from GoI to our latest comments on the November 2015 revision of the *PMA-G* implementation guidelines. Companies continue to navigate *PMA-G* on a case-by-case basis, approaching GoI when there are specific questions or issues of concern. In ITI's meeting with the Department of Telecom in June 2015, DoT officials expressed that they believe *PMA-G* guidelines are clear (and that companies can still come to them with specific issues). With industry input, DeitY is also drafting a PMA-G policy for software. While initial feedback from local industry reps indicate this draft will be favorable, we are still waiting for an official document and consultation to begin. ITI is also preparing a submission to the Telecom Regulatory Authority of India (TRAI) to respond to their ongoing public consultation on potential regulation for cloud computing services. In its public consultation questionnaire, TRAI alluded to data localization requirements as a possible means to create more data centers in India.

ITI Forced Localization Strategy in Indonesia

Background

Citing both a desire to improve data security and to develop its local ICT sector, Indonesia has enacted and has considered enacting several localization measures. Of greatest concern is the *Ministry of Communication and Informatics (MICT) Regulation 82/2012*. In effect since 2012, the regulation includes requirements for source code surrender as a condition for market access and a requirement for local storage of data. In mid-2015 MICT released additional draft implementation measures, which contain more detailed requirements for protecting personal data on electronic systems, including requirements to store personal data in primary and back-up data centers in Indonesia.

Parallel to this regulation is the *Ministry of Trade (MOT) Regulation 82/2012*, which contains strict rules for local manufacturing presence and import licenses for mobile devices; as well as *Kominfo Regulation No. 27*, passed in July 2015 with implementing regulation imposing strict, phased in local content requirements for Lte enabled devices. Finally, in March 2016, MICT issued *Circular Letter Number 3* on "Over-the-Top (OTT)" services, which replicates the data localization requirement in Regulation 82/2012. The letter notifies foreign OTT providers to prepare themselves while the Ministry formulates new regulations.

Current State-of-Play

ITI has submitted comments to the relevant Indonesian authorities on the following draft measures: *MICT Regulation 82/2012,* the implementation regulation for *MICT 82/2012,* and the Lte local content requirements. ITI submitted a multi-associational letter in collaboration with DIGITALEUROPE and JEITA commenting on *Circular Letter Number 3*.

In January 2016 Minister of Communication and Information Technology Rudiantara stated that some of the data localization requirements of *MICT Regulation 82* will be loosened due to their potential to damage the Indonesian economy – primarily because of poor Indonesian infrastructure which causes many Indonesian companies to store their data in foreign markets that raised reliability, safety, and cost concerns. We understand that Rudiantara has requested that the draft implementation regulation for *MICT 82/2012*, cited above, be converted into a law. We are working to verify this information with US-ABC but it is possible that this measure never becomes a reality.

On February 10, 2016 Indonesia notified the WTO Committee on Technical Barriers to Trade (TBT) of *Kominfo Regulation No.27*. Although it entered into force on July 7, 2015, ITI submitted comments on April 8th through the NIST National Enquiry Point that echoed prior submissions on the harmful effects of this law.

MOT recently introduced a new draft amendment for *MOT Regulation 82*, which removes some of the importation requirements present in the original rules. Acting DG of Foreign Trade Karyanto

Suprih stressed that this should not to be seen as a sign of the government's faltering commitment to encourage the development of local industry but instead the amendment is trying to soften the definition of local content to include more than just manufacturing. Media reporting indicates that local mobile phone manufacturers have had great difficulty implementing the local content requirement.

Lastly, Kominfo recently released a draft version of Circular Letter Number 3, which includes a data localization requirement and a requirement to cooperate with the national telecommunications provider for any services that could have similar functions. Foreign OTT firms must also register no later than 30 business days prior to providing services in Indonesia and establish a permanent office in the country, subjecting them to Indonesian tax, content, and law enforcement regulations.[1]

[1] Firms would also have to provide law enforcement agencies with access to servers upon request and to filter content according to Indonesian censorship guidelines. Several foreign multinationals have reportedly already complied in part.

ITI Forced Localization Strategy in Korea

Background

The Korean government has several forced localization policies. In January of 2016 the government of Korea pre-announced new standards for operators of cloud computing services for government agencies within Korea. Key concerns include strict data localization requirements, as the standards would require both the physical systems of public institutions, as well as the data they process to be located within the borders of Korea. In addition, the Ministry of the Interior is scheduled this month to release new guidelines that will classify data according to sensitivity, with certain confidential data being restricted from export. Lastly, the Korean government announced in 2015 a new regulation mandating government agencies to only procure certain types of servers from domestic SMEs, affecting multiple ITI members.

In addition, the Korean government has export restrictions on mapping data. This restriction on cross border data flows is a *de facto* data localization rule as information cannot leave the borders of Korea. The government cites maintaining security as the policy objective of this rule.

Current State-of-Play

Both the US government and industry have been engaging with Korea for several years on its restriction on the exportation of mapping data with little progress. USTR highlighted the law in the most recent National Trade Estimate (NTE) but cites the difficulty of market entry for foreign companies to be a continuing problem. ITI is promoting data protection policies and the economic benefits of data flows as a priority topic for discussion at the fall US-Korea ICT Dialogue, given the long term impact on both the Korean economy, as well as the policy environment in Asia with relation to data protection regulations.

ITI Forced Localization Strategy in Nigeria

Background

The deployment and use of information and communications technology have grown exponentially in Nigeria in the last decade. However, the Nigerian government believes that domestic Nigerian ICT firms have not contributed sufficiently to this growth. To address this perception, Nigeria's National Information Technology Development Agency (NITDA) created and developed the *Guidelines for Nigerian Content Development in ICT.* These measures effectively service as an industrial policy to promote the growth of local ICT firms at the expense of foreign competitors, partially through rigid forced localization requirements. These guidelines include requiring domestic storage of data concerning Nigerian citizens, ensuring up to 50% local content in products entering the market, and developing local software. The initial provisions of these guidelines came into effect December 3rd, 2013. The Office of Nigerian Content Development in ICT (ONC) issued a final notice of implementation in the fall of 2015.

Current State-of-Play

In meetings with stakeholders, NITDA agreed that enforcement of some of the guidelines will for now only cover realistic areas – not currently manufacturing plants for production. All multinational companies, however, are expected to have local content development plans which outline the number of indigenous engineering jobs they provide, a valuation of R&D activities in country, and local ICT skill development programs. The American Business Council of Nigeria is trying to engage more with the Head of Local Content and is working to sit down with relevant domestic Senators/Representatives to express its concerns. In 2014, ITI together with the US Chamber of Commerce sent a number of letters to relevant Nigerian officials, including the former Minister of ICT. DIGITALEUROPE sent similar letters. At the behest of ITI and other industry stakeholders, the House Foreign Affairs Committee sent a letter to the former Minister of ICT in advance of AGOA renewal in 2015.

ITI Forced Localization Strategy in Russia

Background

The Kremlin has pursued an increasingly broad strategy of forced localization in recent years. The cornerstone of this agenda is *Federal Law No. 242-FZ*, signed by President Vladimir Putin in July 2014. The law requires companies that store and process the personal data of Russian citizens to maintain servers on Russian soil and to notify the federal media regulator, Roskomnadzor, of all server locations. It empowers Roskomnadzor to block websites and to maintain a registry of data violators. The localization provisions were originally scheduled to take effect in September 2016. In December 2014, however, President Putin signed *Federal Law No. 526-FZ*, moving forward the date a year, to September 2015.

Russia's ostensible justification for its forced localization policy is rooted in the national security concerns surrounding the Snowden revelations. Nevertheless, the law fits within the context of the Kremlin's recent import-substitution policies, meant to develop the Russian economy in a manner that is less dependent on companies headquartered in the United States and the European Union. In January 2016, the Kremlin issued a 16-point plan for improving the competitiveness and security of the Russian ICT sector through import-substitution, increased surveillance capabilities, and increased education on issues related to cyber. The plan includes specific goals, deadlines, and ministerial responsibilities.

In July 2016, President Putin signed a package of amendments to the federal law *On Fighting Terrorism*. The amendments impose extensive data storage requirements on telecommunications providers and companies classified as Internet telecommunications services. Telecoms operators will have to store metadata for 3 years and Internet telecoms for 1 year, while both will have to retain the content for up to 6 months. Companies will have until July 1, 2018 to begin implementing these requirements. Moreover, if the stored messages and files are encrypted, companies will be required to provide Russian state security services with decryption keys upon request.

Current State of Play

The current state of play is characterized by uncertainty.[2] On the one hand, the legislation is unclear on scope and enforcement. Roskomnadzor, for example, has not interpreted *Law 242-FZ's* applicability to foreign data operators. In the past, Russian data protection legislation has applied only to Russia-based operators and foreign data operators with a legal presence in Russia. The Russian Ministry of Communications, under which Roskomnadzor falls, published in August 2015 a non-binding clarification suggesting that localization might apply to websites that include a built-in Russian-language option, transact in Russian rubles, or use a Russian top-level domain such as .ru.

[2] The Russian Federation has a history of uneven and unpredictable enforcement of the law. It should be noted that *de facto* interpretations of data localization requirements are likely not stable and are liable to change to reflect future political headwinds.

On the other hand, regulators have made several positive statements to members of the international business community. The standard of individual consent, for example, is expected too low and violations of the law will likely not have consequences on contracts between companies and clients. Russian officials have also said that there will be opportunities to update the law in the future and have suggested inviting global experts to consult on best practices for data protection.

In January, 2016, Roskomnadzor released a plan of scheduled audits and officials are aiming to audit of 1,500 companies by the end of the year. According to Roskomnadzor, out of 645 inspections it found only four violations of 242-FZ. Companies in violation have been given nominal fines and have been given a de facto transition time. Moreover, reports from the ground have found that inspectors have only reviewed documents (ex: contracts with local server providers) rather than examining companies' software and hardware to ensure compliance.

With regard to the 16-point plan put out by the Kremlin, we understand that there are two executive decrees have been updated to create a potentially discriminatory certification system for government ICT procurement. Still, implementation and follow-up to the decrees have been opaque and not well-coordinated, so there is little information on how the plan has progressed.

The amendments to *On Fighting Terrorism* have faced rare public criticism from Russian telecoms providers and Russian Internet companies, as well as human rights activists. Telecoms executives have warned that the upfront costs of implementation would reach 2.2 trillion rubles ($34bn). Other industry leaders have said that the requirement could bankrupt some operators or force customers to pay two or three times the current price for services. The actual impact, however, is uncertain. The Kremlin, perhaps in response to the vocal public concerns, has signaled that it may water down the law's provisions, likely in the implementation phase, in a similar fashion to 242-FZ.

ITI Forced Localization Strategy in Turkey

Background

The Turkish government has enacted or has considered enacting a number of forced localization measures. In December 2014, Turkey had notified the WTO Committee on Safeguards of its investigation into applying safeguard duties on imported electronic goods. Turkish manufacturer Vestel requested the safeguards just before its entry into the country's foreign-dominated mobile phone market. In March 2016, Turkey ended the investigation, after Vestel had withdrawn its request.

In early April 2016, Turkey's new *Data Protection Law* came into force. First introduced by the Ministry of Justice in 2005, the draft legislation had lingered, untended, until the 2016 Brussels-Ankara refugee and migrant agreement required large transfers of personal data across borders. The law places new obligations on data controllers and processors and requires firms to obtain expressed consent from individuals. The most burdensome of these provisions—many of which are retroactive—have a two-year compliance period. The law also creates a Data Protection Board that determines whether countries receiving the data of Turkish citizens have an adequate level of privacy protection in place.

The data protection legislation follows the *Law on Electronic Payments*, which entered force in June 2015 and mandates that all electronic and mobile payment operators store their documents in country for a minimum of ten years. These firms are also required to register with the Central Bank of Turkey and are subject to the Banking and Regulatory Supervisory Authority's jurisdiction.

Current State of Play

The current state of play can be characterized as cautiously optimistic. The withdrawal of the safeguards investigation was a welcome development. The *Data Protection Law*, however, represents a significant modernization of the Turkish data privacy regime and so there is a lack of defined precedent on how Turkish authorities will proceed. Noncompliance with the law could lead to a monetary fine of up to one million Turkish Liras and a custodial sentence of between 1 to 4 years.

While the *Data Protection Law* brings the Turkish legal framework closer to the European Union's there are important points of departure. During the drafting of the legislation, the EU Delegation to Turkey raised concerns that the Data Protection Board, whose board members would be appointed by the Turkish President and Prime Minister, would be liable to politicization. Moreover, the final text contains broadly defined national security exceptions to the enumerated protections. The *Law on Electronic Payments*, meanwhile, which has a data localization requirement, has coincided with the launching of the Turkish card payment system, TROY. Foreign firms that have chosen not to comply with the law are reported to be leaving the Turkish market.

ITI Forced Localization Strategy in Vietnam

Background

Vietnam is considering or has implemented a number of forced localization measures, often citing national security concerns as the basis for their action. The most harmful of these has been the *Decree on Information Technology Services (Decree no. 72)* from 2013. This law requires that companies must physically locate at least one server within Vietnam to operate most internet based services.

In addition to this law, the Vietnamese government released a new *Draft Circular* in the beginning of 2016 which aims to regulate "Over-the-Top (OTT)" services. It has many restrictive clauses, including new server localization requirements and the shifting of power to control OTT services to domestic telecommunications firms.

Lastly, the *Law on Network Information Security* (LONIS) contains many troubling provision including broad business licensing requirements and vague language on potential access to encryption passwords and source code. The *Decree Guiding Law on Cybersecurity*, an implementing regulation currently open for comments, contains a requirement for local business presence in order to provide cyber security services.

Current State-of-Play

After the release of a draft of Decree no. 72, ITI and the US-ASEAN Business Council (US-ABC) submitted comments to the Vietnamese that outlined specific concerns with the measure and highlighted how its provisions could in practice harm the Vietnamese economy. We understand that Vietnam has not moved forward with this draft; ITI continues to monitor whether Vietnam takes any action, paying particular attention to how the provisions of the TPP Agreement would apply to this case. ITI submitted joint industry comments with five other associations in regards to LONIS and is developing comments for several draft implementing decrees.