WITSA's Statement of Policy on Restrictions of the Free Flow of Information Across Nationality/Regional Borders – July 2016

Synopsis

Cross-border data flows can relate to a multitude of different transactions. For example, personal data that millions of people share on social networking sites like Facebook, Twitter, YouTube, LinkedIn, Qzone, VK, hi5, Weibo and others is used by companies to develop better marketing practices. Cloud computing allows customers and businesses to access digital data from powerful off-site servers. Digital shopping on sites like Amazon is more popular than ever. Physical objects—TVs, home appliances, and cars for example—are being connected to each other more frequently in what's termed the "Internet-of-Things." Far from being exclusive to high-tech firms, data flows are used by almost all businesses and customers. Countries are concerned about these free data flows, however, for a variety of reasons: revelations about the ability of governments to collect digital traffic; protectionist goals to favor local companies; and concerns about the security of personal data, to name just a few. In response, barriers are being imposed on the free flow of data across borders by various nations, both developed and developing.

These barriers to free data flows form considerable obstacles to global trade. Customers would find themselves unable to access valuable digital services. Small and medium-sized enterprises (SMEs), which could greatly benefit from digital trade, would be disproportionately affected by these barriers. They do not have the resources to bear these unnecessary costs, and are far more restricted in their global reach.

WITSA believes 'data' is an essential resource for healthy economic growth and that excessive restrictions on data will be a barrier to secure management and protection of data. WITSA advocates a principled policy approach which recognizes that data regulations must be simple, transparent and harmonized with other legislative requirements. WITSA also opposes forced localization of data requirements as these interrupt the free flow of data that underpins the complex online networks

connecting the globe in ways that threaten the cultural and economic growth potential of the Internet and Internet-based technologies.

Context

About WITSA

WITSA is a global consortium of leading ICT industry association members from over 80 countries/economies.

As the leading recognized voice of the global ICT industry, WITSA aims to drive transformation and grow the industry, given that ICT is the key driver of the global economy:

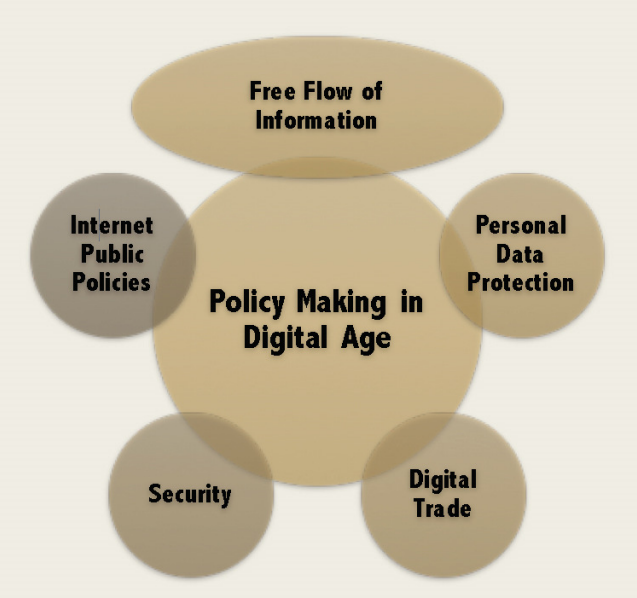
WITSA's members and stakeholders comprise national associations, multinational corporations, institutions and organizations, researchers, developers, manufacturers, software developers, telecommunication companies, suppliers, trainers and integrators of ICT goods and services. As such, they represent a large and obviously vital constituent group for whom the effective balancing of concerns and rights affecting the security, privacy and information capability provided by ICT products and services underpins business development and economic activity.

Why Do We Need Free Flow of Information?

In today's global economy, consumers, regulators, and businesses all benefit from a constant stream of data flowing seamlessly back and forth across national borders. Businesses use data to create valuable products and services, enhance productivity, reduce costs, improve efficiency, deter fraud, protect consumers, and foster economic growth and jobs. To secure these benefits, it is essential to have clear, consistent rules in place that allow for the unimpeded flow of data except as limited to legitimate public policy objectives.

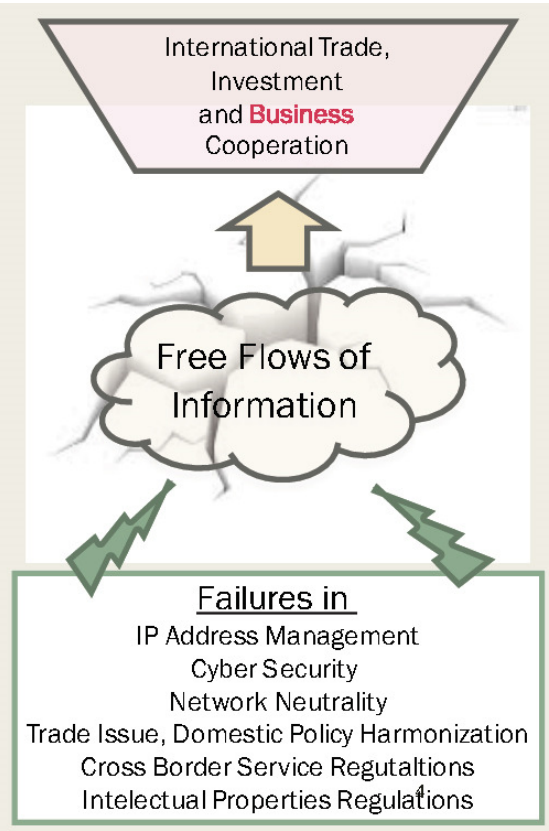
Despite these benefits, some countries have created rules that restrict the free flow of data across borders. While these rules ostensibly seek to protect national security or promote domestic innovation, such barriers to digital trade can stifle economic growth and job creation. Some of these negative impacts are inadvertent, while others are blatantly protectionist.

We live in an age which every aspect of modern society is being transformed by the application of data. The extent to which individuals, businesses of all sizes and governments benefit from data revolution depends on the creation and adoption of technologies that enable innovative use of data, the legal and policy environments that facilitate the free flow of data, and willing participation of all stakeholders in the global economy. A free, open and secure Internet is a global resource which should be managed in the public interest. We must ensure that the various stakeholders plan an active role in the ongoing discussions about its governance, management and security, and that those who do not yet have a voice in this debate are empowered to participate in these discussions – which will also shape their future.



It is important to note that the free flow of data issue is not independent from other public policy issues, but is an integral part of policy making in the digital age, including Internet public policies, personal data protection, digital trade and security. Unfortunately, many casual observers have conflated the issues of national security and the ability of business to move data cross borders. As a result, businesses and individuals often have to comply with a confusing set of requirements related to law enforcement where multiple governments may attempt to assert jurisdiction. Clear, concise rules should be developed for the transfer and processing of data for both private usage and in compliance with government requests. Establishing overly burdensome and prescriptive rules for business will do nothing to settle the current debate over government access to data.

Another area of policy that heavily affects the cross-border data flows is data privacy. Countries' domestic data privacy laws can vary quite substantially and often affect foreign companies seeking to provide any type of electronic service to consumers in that country. For example, the EU and the United States are often cited as having very different domestic approaches to privacy, with the United States following a self-regulatory approach (with sector-specific regulations for certain sensitive types of data), and the EU favoring a "baseline common level of privacy, protects the data privacy rights of Europeans regardless of where data are transferred and processed. Meanwhile, third countries have their own approaches, and data privacy laws in some of these countries are in flux, creating a challenge for cross-border cloud providers and an opportunity for greater international harmonization. Security policy measures also impact cross-border data flows and generally aims to ensure that unauthorized parties do not obtain access to sensitive data. In that sense, security is related to privacy. In some cases, governments themselves may present a threat to data security; e.g. instances where government authorities, such as police or intelligence agencies request access to personal data.



Political restrictions also impact the free flow of information across borders. In many ways, the Internet has become a tool for challenging political power. For example, popular uprisings in countries including Tunisia, Burma, Iran, Egypt and Ukraine were facilitated by social media. This has frequently resulted in politically motivated Internet restrictions including blocking access to media reporting on sensitive political issues or using the Internet as a site to express political views considered harmful by the government.

Morality based restrictions on flow of information is not uncommon. These include content on the Internet that countries find morally objectionable and attempt to block, such as pornography, sale of Nazi memorabilia gay rights, religious views and gambling.

Restrictions can also emerge due to intellectual property protection as well as commercial restrictions, such as routing traffic to domestically-owned companies or blocking particular non domestic sites

In the last few years, a growing number of countries have imposed what are called "localization barriers to trade" – forced localization measures designed to protect, favor, or stimulate domestic industries, service providers, and/or intellectual property (IP) at the expense of goods, services, or IP from other countries. Localization barriers are measures that can serve as disguised trade barriers when they unreasonably differentiate between domestic and foreign products, services, IP, or suppliers, and may or may not be consistent with WTO rules. Examples of localization barriers include:

- Local content requirements, i.e., requirements to purchase domestically-manufactured goods or domestically-supplied services
- Subsidies or other preferences that are only received if producers use local goods, locally-owned service providers, or domestically-owned or developed IP, or IP that is first registered in that country;
- Requirements to provide services using local facilities or infrastructure;
- Measures to force the transfer of technology or IP
- Requirements to comply with country- or region-specific or design-based standards that create unnecessary obstacles to trade
- Unjustified requirements to conduct or carry out duplicative conformity assessment procedures in-country.

When foreign goods, services, or IP are either disadvantaged in a market compared to domestic goods, services, or IP, or when they're kept out of the market altogether, that can distort trade, discourage foreign direct investment, and push other trading partners to impose similarly detrimental measures. And, consequently, often over the long term, these measures can actually stand in the way of the economic growth and competitiveness objectives that they were intended to achieve. For these reasons, WITSA strongly advocates against localization barriers and instead encourage governments to pursue policy approaches that help their economic growth and competitiveness without discriminating against imported goods or services.

The impact of recently proposed or enacted forced localization legislation has been shown to be quite substantial. According to the European Centre for International Political Economy (ECIPE), in a 2014 publication entitled "The Costs of Data Localization: Friendly Fire on Economic Recovery", studied[1] the effects of recently proposed or enacted forced localization legislation in seven jurisdictions, namely Brazil, China, the European Union (EU), India, Indonesia, South Korea and Vietnam.

- The impact of recently proposed or enacted legislation on GDP is substantial in all seven countries: Brazil (-0.2%), China (-1.1%), EU (-0.4%), India (-0.1%), Indonesia (-0.5%), Korea (-0.4%) and Vietnam (-1.7%). These changes significantly affect post-crisis economic recovery and can undo the productivity increases from major trade agreements, while economic growth is often instrumental to social stability.
- If these countries would also introduce economy-wide data localisation requirements that apply across all sectors of the economy, GDP losses would be even higher: Brazil (-0.8%), the EU (-1.1%), India (-0.8%), Indonesia (-0.7%), Korea (-1.1%).

[1] http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf

- The impact on overall domestic investments is also considerable: Brazil (-4.2%), China (-1.8%), the EU (-3.9%), India (-1.4%), Indonesia (-2.3%), Korea (-0.5%) and Vietnam (-3.1). Exports of China and Indonesia also decrease by -1.7% as a consequence of direct loss of competitiveness.
- Welfare losses (expressed as actual economic losses by the citizens) amount to up to $63 bn for China and $193 bn for the EU. For India, the loss per worker is equivalent to 11% of the average month salary, and almost 13 percent in China and around 20% in Korea and Brazil.

The findings show that the negative impact of disrupting cross-border data flows should not be ignored. The globalised economy has made unilateral trade restrictions a counterproductive strategy that puts the country at a relative loss to others, with no possibilities to mitigate the negative impact in the long run. Forced localisation is often the product of poor or one-sided economic analysis, with the surreptitious objective of keeping foreign competitors out. Any gains stemming from data localisation are too small to outweigh losses in terms of welfare and output in the general economy.

As demonstrated in a May 2016 report by the Global Commission on Internet Governance[2], data localization barriers consistently result in large industry productivity losses due to their high dependency on data inputs covered by data regulations. The production of data intensive manufacturing and services sectors shrink in all countries due to restrictions on the free flow of data. The study found that tight regulations on the free flow of data tend to cause an economy's production structure to become less innovative and competitive.

Other cases that are relevant include:

- (EU) data localization in name of privacy requires data to be hosted on EU geography unless some pre-determined special arrangement are provisioned for initiating cross border data flows. The new EU-US Privacy Shield is one such arrangement, enabling some US companies to comply with privacy laws[3] protecting European Union citizens.

- (US) While the proposed Trans-Pacific Partnership (TPP) would guarantee the cross-border data flows and prohibit computing facility localization requirements for all sectors, the e-commerce chapter excludes the financial services sector and government procurement[4]. Industry has voiced concern in particular on the financial services exclusion, arguing that the e-commerce chapter must include all types of data, include financial data. The U.S. Treasury has sought to maintain policy space for U.S. regulators to be able to implement such restrictions in the future, citing instances during the 2008-2009 financial crisis when U.S. regulators could not get needed data. Over the last few months, the U.S. Treasury and USTR have worked to develop a new approach for addressing concerns about the treatment of financial services under data localization obligations in trade and investment agreements[5].

- (Russia) data localization requirement law has been enacted and enforced with effect from September 1, 2015.

---

[2] "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization": https://www.cigionline.org/publications/tracing-economic-impact-of-regulations-free-flow-of-data-and-data-localization

[3] General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

[4] Congressional Research Service Reports: https://www.fas.org/sgp/crs/row/IN10498.pdf

[5] http://thehill.com/policy/finance/trade/281294-obama-administration-strikes-deal-on-data-storage-concerns-in-tpp

- (Brazil) "Marco Civil da Internet," a law to protect Internet users' rights, was formally signed by the Brazilian president in April 2014. The Clause requiring data localization was deleted, but Article 11 says this law should be respected wherever an Internet service is related to Brazilian citizens.

- (Thailand) A cabinet resolution unearthed by a Bangkok-based reported shows Thailand's intention to create a China-style Great Firewall - or a "single internet gateway". The gateway would be used "to control inappropriate websites and to control the flow of information into the country from overseas via the internet"

- (Vietnam) There is a notification that government procurement suppliers should deliver domestically produced IT products and services on the list.

- (China) The draft regulations, announced by the China Insurance Regulatory Commission (CIRC) last month, state that insurance companies, along with their holding companies and asset managers, should prioritize the purchase of "secure and controllable" products, including domestic encryption technologies and local hardware and software. "Secure and controllable" actually means products made in China.

- (Mexico) In the 1990s, Mexico government introduced local contents requirement of computer hardware which resulted in 150-300% increase in computer hardware price in Mexico

- (India) As an historic analysis of the impact of trade restrictions, in 1970s-1980s, the Indian Government imposed high custom duties on ICT products. According to the economists Kaushik and Singh, loss in other industries including productivity foregone by not using ICT products was USD 1.3 per USD 1 custom duties.

WITSA strongly supports its industry members and allies, including the October 2014 “Tokyo Resolution on Combatting Data Localization Requirements” by DIGITALEUROPE, the Information Technology Industry Council, Japan Electronics and Information Technology Industries Association (JEITA) and with the support the Japan Information Technology Services Industry Association (JISA):

The movement of data across borders is an imperative for today’s global economy;
Data localization requirements disrupt the free flow of data;
Data localization requirements are incompatible with the Internet’s distributed infrastructure that enables optimal system architecture;
The security of data does not hinge on the national boundaries of where such data resides; and
Data localization requirements create barriers to market access, particularly impacting small and medium sized enterprises (SMEs) which are eager to attract customers not only domestically, but also in foreign markets.
Any exceptions to these provisions, such as to protect personal data privacy, should be limited to legitimate public policy objectives and be in full compliance with the provisions of the GATS.

WITSA also supports the APEC Cross Border Privacy Rules (CBPR) system[6], which was developed by participating APEC economies in 2012 after seeking the views of industry and civil society, to build consumer, business and regulator trust in cross border flows of personal information. The APEC CBPR system establishes a voluntary certification system for complying with APEC's Privacy Framework. Countries that opt to participate must designate an accountability agent and a privacy enforcement authority. To date, participation rates in the CBPR system have been low at every level and WITSA encourages countries to participate in this important initiative.

Impact of Proposed WTO Trade in Services Agreement (TiSA)

Negotiations on a proposed Trade in Services Agreement (TiSA) were launched in April 2013, with the United States and Australia initially at the lead. TiSA participants account for about 70% of world The final structure and sectors to be covered in TiSA remain under negotiation, but some key issues have emerged. TiSA may expand market access beyond the current GATS commitments, building disciplines on transparency, setting common rules for cross-border data flows and digital trade, and ensuring fair competition with state-owned enterprises. TiSA participants have conducted 15 negotiating rounds through 2015, and aim to complete negotiations in 2016. The outlook and timeline for the ongoing TiSA negotiations remains uncertain, as participants are tackling difficult and complex issues such as regulatory processes and digital trade frameworks. Trade in services and include the European Union, in addition to the United States and Australia.

The ongoing TiSA negotiations allow an opportunity for these barriers to be neutralized and for the world's major trading nations to agree on an international framework which promotes free data flow. Potential solutions which should be added to these trade negotiations include:

- Explicit agreement among participating nations that data can flow freely across border, unless excepted for clearly defined and pre-accepted needs (such as national security). Explicit commitments will reduce uncertainty for businesses and ensure that governments form an adequate justification for any data flow restrictions they impose.
- Agreed upon harmonization of regulations involving the sharing of personal data. Such a rule would make compliance easier for businesses and provide security and essential information for consumers.

Statement of Policy Principles

Principles:

1. **Data as a Global Natural Resource Principle:** The movement of data across borders is an imperative for today's global economy. Like air, water and other natural resources, "Data" is an essential resource forming the basis for healthy economy growth in today's global economy. Industry needs to raise awareness of the importance of ensuring unrestricted access to data across border and collaborate with governments to keep these data flows "green".

2. **Data Protection Principle**: The regulatory focus should be on 'what' to protect instead of 'how' to protect. Detailing on the 'how' part undermines flexibility and takes away freedom from businesses to do things that are appropriate to their environment and context. Excessive

[6] http://www.cbprs.org/

restrictions on data transmissions may undermine the secure management and protection of data.

3. **Simple, Single, Transparent and Harmonized Data Legislation Principle**: Data regulations must be simple enough to be understood by anybody concerned, must have a Single administrative window to the public, must have Transparent criteria and no gradient, and must be harmonized with other legislative requirements in order to reduce barriers to market access, particularly impacting small and medium sized enterprises (SMEs) which are eager to attract customers not only domestically, but also in foreign markets.

4. **No Forced Localization Measures Principle**: Government mandated Data localization requirements create barriers to market access and must be minimized in order to promote inclusive growth regionally and globally. Data localization requirements are often the result of misguided attempts to protect local economies or for security or privacy reasons. Forced localization does not effectively strengthen privacy or security and are more often than not about data protectionism rather than data protection. Attempts to mandate localization of data can further escalate to internet balkanization.

5. **Legitimate Public Policy Objectives Principle:** While nations should be encouraged to adopt or maintain a domestic legal framework that ensures the protection of the personal data, they must not create unnecessary legal and administrative hurdles for data transfers in the name of privacy protection. Any restrictions on the free flow of data across borders, such as to protect personal data privacy, should be limited to legitimate public policy objectives and be in full compliance with the provisions of the General Agreement on Trade in Services (GATS). Industry advocates for the free flow of data across borders with minimum regulatory intervention and push back against countries that force data localization within their borders in name of privacy or security.

6. **Trade Agreements Principle:** As the current WTO laws on localization barriers to trade offer limited effectiveness in curbing forced localization of data centers or other barriers to data flows, government should consider a WTO plurilateral “Data Services Agreement” to protect cross-border data flows and prevent signatory countries from creating barriers to them. This agreement could augment other agreements currently being negotiated at the WTO, such as the TISA.