TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org
Tel: +1.703.907.7700
Fax: +1.703.907.7727

Pre-Hearing Statement of K.C. Swanson
Director, Global Policy
Telecommunications Industry Association (TIA)

Before the
U.S. International Trade Commission
Hearing on Global Digital Trade I. Market Opportunities and Key Foreign Trade Restrictions
Investigation # 332-561

March 28, 2017

The Telecommunications Industry Association (TIA) appreciates the opportunity to provide testimony to the US International Trade Commission on "Global Digital Trade I. Market Opportunities and Key Foreign Trade Restrictions."

TIA represents over 200 manufacturers and suppliers of high-tech telecommunications networks and services here in the United States and around the world. TIA is also an ANSI-accredited standards development organization. Our members' products and services empower communications in many industries and markets, including healthcare, education, security, public safety, transportation, government, the military, the environment, and entertainment.

The positive effects of digital trade for the U.S. economy are well documented. As the USITC itself has noted, digital trade was found to increase U.S. GDP by up to 4.8 percent in a given year (2011) by increasing productivity and lowering costs. The same factors contributed to an increase in average American real wages of 4.5-5.0 percent[1]. In short, more digital trade benefits the U.S. economy.

Below, we outline some of the principles of digital trade that we consider essential to combating market access barriers. Some of these basic principles are not only important to information and communications technology (ICT) firms, but also support the growth of U.S. exporters in a range of different industries. They include:

- Free cross-border data flows
- Open markets for cloud computing
- Security measures that align with international norms

[1] *U.S. International Trade Commission, Digital Trade in the U.S. and Global Economies, Part 2*, Publication No: 4485, Investigation No: 332-540, p. 17

- Standards-setting process that is transparent, open, impartial, and consensus-based
- Compliance with Information Technology Agreement commitments
- Testing requirements that are not trade-restrictive

Free cross-border data flows. Global data transfers have been dramatically rising: according to an estimate from McKinsey, worldwide data and communications flows jumped nearly seven times between 2008 and 2013[2].

Cross-border data flows are essential for enabling new communications technologies that benefit the broader U.S. economy.

One example of a communications technology that benefits a broad swath of U.S. exporters is the Internet of Things (IoT). The growing use of IoT services by American companies has introduced transformative new efficiencies in areas such as manufacturing, agriculture and logistics. For example, using IoT services, American manufacturers can outfit machinery with tiny data analytics that reduce idle time and improve energy efficiency, while providing early warnings of possible malfunctions. Better access to information lets them operate faster, more responsive global distribution chains and customer service. In agriculture, IoT devices help farmers monitor soil and temperature to optimize planting conditions, resulting in higher crop yields. Automakers selling into overseas markets can keep better tabs on their inventory, reducing theft and getting product to market more quickly, through the use of sophisticated sensors. For companies that have a global presence, communication with devices across borders and access to data wherever it is located is essential for coordinating work and output.

These are only some of the early use cases for IoT, which is expected to see global spending of $1.3 trillion by 2019[3]. Yet the successful deployment of global services will require that governments allow free flows of data across international borders. And in a worrying trend, some countries have begun adopting regulations that force service providers to store data in-country.

Most notably, in the name of security, China has been especially aggressive in enacting and proposing rules requiring local storage of data for a wide host of economic sectors. While China is positioning their regulations as seeking to protect user-related data, the impacts are extremely wide ranging and will limit data flows across many sectors. These include civil aviation, health information management, banking, online publishing, insurance, and connected vehicles, among others. Russia, Vietnam, and a number of other countries have also implemented some form of data localization requirements.

Nations that adopt such rules often try to cast them as a way to improve privacy and security. Yet the location of a piece of data has no bearing on whether it is secure. The data of foreign citizens is no more likely to be compromised if it is located overseas than if it is located in their home country. As should be clear by now from multiple well-publicized cases of international hacking, cyber bad actors do not respect national boundaries. In fact localization rules actually undermine network security, because restrictions on data transfers make it harder to aggregate information in order to holistically analyze cyber threats and fraud.

---

[2] James Manyika, Jacques Bughin, and Susan Lund, et al., *Global Flows in a Digital Age: How Trade, Finance, People, and Data Connect*, McKinsey Global Institute, April 2014

[3] "Internet of Things Spending Forecast to Reach Nearly $1.3 Trillion in 2019 Led by Widespread Initiatives and Outlays Across Asia/Pacific," IDC website, December 2015

Given that network risks are constantly changing, a far more effective approach in promoting security is to pay attention to *how* the data is handled rather than *where* it is handled. This approach requires more work – an ongoing effort to stay abreast of evolving best practices – but yields much better results than a tick-the-box localization requirement. In addition, the close communication channels between government and the private sector in the U.S. offer a positive model of a framework for formulating rapid cyber responses.

Meanwhile, from a business standpoint, the most immediate cost of data localization in other countries is lost sales opportunities for U.S. ICT firms. But in the bigger picture, the resulting information bottlenecks also handicap the American manufacturers, farmers and service providers that are among the early adopters of IoT and big data services. Restrictions on data transfer deprive decision makers of full access to a global portfolio of business information. They make it harder to leverage the value of big data – to identify larger-scale patterns that could tip companies off early to inventory problems or emerging customer needs.

Data localization also requires companies to needlessly replicate their communications networks in countries with data transfer restrictions, which increases infrastructure costs. It complicates the ongoing internal transfers of company and human resource data across borders that are necessary to carry out daily business.

For this reason, we believe it is especially important that the U.S. government works with our trading partners, both within and outside of formal agreements, to ensure robust cross-border flows of data. A system that allows information to travel freely creates a foundation where a broad base of U.S. business – not just ICT companies – can prosper.

Open markets for cloud computing. In a similar vein, the negative effects of Chinese restrictions on cloud computing extend beyond ICT firms to affect a wider range of U.S. companies operating in that market.

In the U.S., which established an early global lead in cloud computing, use of the cloud has become a well-established means of lowering infrastructure costs for a broad range of companies, both large and small. Worldwide, the use of cloud computing services is experiencing massive growth. According to a 2015 study[4] by Cisco, by 2020, 92 percent of workloads will be processed by cloud data centers (with only 8 percent processed by traditional data centers).

However, U.S. service providers that offer or use cloud computing facilities have run into substantial market access barriers in China. Under new Chinese restrictions that took effect in March 2016 (when Beijing revised its catalog regulating telecom services), foreign providers can offer cloud-based storage or other services only through a joint venture with a Chinese partner, with ownership capped at 50%. In late 2016 China went a step further with proposed rules on what foreign firms are permitted to do within joint ventures. For example, it would regulate such details as which party can sign contracts, how the two partners use trademarks and brands and the degree to which they may share data.

These restrictions serve as a major limitation for ICT companies. In January 2017, the CEO of Alibaba

[4] Cisco Global Cloud Index: Forecast and Methodology, 2015–2020, 2016

Group, a publicly-traded Chinese conglomerate that offers cloud services, estimated the Chinese cloud market is worth some $30 billion – a considerable portion of China's estimated total IT spend of $200 billion a year[5].

The companies that provide cloud services and their suppliers are most directly impacted by China's rules. But the restrictions also stand to affect any U.S. businesses operating in China. If they want to use cloud services, they must establish a separate relationship with a China-based provider, which may have implications for what kind of cloud-based applications they can use.

It's important to note that China imposed limits on foreign cloud providers at the same time it is actively seeking to build up its own cloud industry. Cloud computing was highlighted as a key strategic area for China in the 13th Five-Year Plan on National Scientific and Technological Innovation issued in 2016.

Security measures that align with international norms. China is pursuing another approach that would disadvantage foreign technology used in cloud services and IoT, along with a growing number of other commercial markets. Over the past year, Beijing has announced plans to expand a security ranking system that mandates only products with Chinese IP can be used for sensitive networks. Besides cloud and IoT, Beijing has either proposed to apply or already applied that system to insurance, mobile internet, industrial controls, big data, and most recently, civil aviation.

Taken together, these moves represent the vast expansion of an approach that is premised on excluding foreign ICT equipment from many Chinese information networks. Measures purporting to improve security would be broadly disruptive to U.S. firms that provide services in the targeted markets. It is likely no coincidence that those markets are almost exactly the same sectors China has targeted for development as part of its industrial policy– a list that includes cloud computing, mobile Internet, the Internet of Things and big data[6].

The government has also invoked national security in seeking access to proprietary IP. Most recently in February 2017, Beijing issued cybersecurity draft standards that demand that suppliers of IoT services and mobile Internet provide access to source code. No other country, even countries with a strong emphasis on privacy and security, requires such access, so we find it unpersuasive that the motivation is enhancement of cybersecurity.

In short, it is clear that a number of policies China has pursued in the name of security are being used to justify protectionist actions in the service of domestic industry. Such measures do not only handicap ICT firms from outside China. They also disadvantage U.S. companies in a number of other service industries, undermining their competitive ability to export to China.

Standards-setting process that is transparent, open, impartial, and consensus-based. China is also revising a major law that governs standards, raising concerns that some of the changes under discussion may create de facto market access barriers. For example, draft text of the revised law would require mandatory standards to be made available free of charge, which could infringe on copyright or patent rights.

---

[5] Alibaba Group Holding (BABA) Q3 2017 Results - Earnings Call Transcript, January 24, 2017

[6] *National Informatization Development Strategy*, Ministry of Industry and Information Technology, People's Republic of China, July 2016

The legislation outlines an important role for "enterprise standards" – a construct unique to China, in which companies would be required to disclose product details that might reveal proprietary information.

The revised standardization law would also create a new type of standards body that would operate through consortia such as associations or technical alliances. While we recognize the important role that voluntary associations can have in promoting best practices and standards, our members are concerned that these standards bodies may operate in a way that disadvantages U.S. and other foreign companies. We seek to ensure that they comply with the principles of the World Trade Organization's (WTO) Agreement on Technical Barriers to Trade (TBT).

Compliance with Information Technology Agreement commitments. Another aspect of building a strong digital ecosystem is upholding commitments to the Information Technology Agreement. Our members have been disappointed in recent years to witness India imposing a number of duties on ICT products covered by the ITA. This contravenes India's obligations as a member of the ITA to maintain duties of zero on covered goods.

It is critical to the continued health of the global ICT industry that signatories to the ITA comply with their obligations. This will in turn further the goal of making connectivity more accessible and affordable.

Contrary to a global trend of lowering tariffs, New Delhi has also increased duties on non-ITA ICT components.

Testing requirements that are not trade-restrictive. Over the past few years, India has steadily expanded the list of imported ICT products required to undergo in-country safety testing, including set top boxes and cell phones. The requirements for local testing to Indian standards, many of which are identical to international standards, represent a needless expense, since companies already have established systems for testing products to international standards. Moreover, the expansion of testing scope to cover new products has often been poorly publicized and announced with little forewarning, leaving companies with inadequate time to comply with regulations.

New Delhi has also repeatedly postponed requirements (as yet undefined) for in-country security testing of telecommunications equipment. However, the government is currently building labs it intends to use for this purpose, and in the fall of 2016 announced plans to add more ICT products (routers and soft switches) to the list of products required to undergo testing. Such tests would be unnecessary and potentially intrusive without providing genuine security benefits.

China requires testing for a safety certification mark used for many ICT products, but has virtually closed off the testing market to American and other foreign firms. This restriction serves as a market access restriction for U.S. testing companies and reduces testing options for American ICT vendors. A mutual recognition agreement with China on telecommunications products could help open the testing market and facilitate trade in digital goods.

Conclusion. We appreciate the work of the U.S. government to promote digital trade principles that will further open markets and support the growth of communications technologies. With the increasing adoption of innovative technologies by many U.S. companies, a strong digital ecosystem stands to benefit not only providers of ICT products but also American exporters across a range of industries.