

Written Testimony to the United States International Trade Commission

Investigation No. 332-531

Hearing: Digital Trade in the U.S. and Global Economies

Prepared by:

Stephen Ezell, Senior Analyst

Information Technology & Innovation Foundation (ITIF)

March 14, 2013

The Importance of the Digital Economy and Digital Trade

The Information Technology and Innovation Foundation appreciates the invitation to provide testimony regarding digital trade in the global economy. Digital trade based on information and communications technologies (ICTs) matters because ICTs are the global economy's strongest driver of productivity, innovation, and growth. For instance, the McKinsey Global Institute estimates that the Internet alone accounted for 21 percent of the aggregate GDP growth across thirteen of the world's largest economies from 2006 to 2011, while the World Bank estimates that ICTs accounted for one-quarter of GDP growth in many developing countries during the first decade of the 21st century. Going forward, a March 2013 study by Finland's Ministry of Employment and the Economy estimates that, by 2025, half of all value in the global economy will be created digitally. This growing digitalization of the global economy is reflected in the expected quintupling of global Internet traffic between 2011 and 2015 and the approximate 50 percent growth in cross-border trade in data annually. Therefore, ensuring the uninhibited flow of information, data, and ICT products and services across borders has become vital both to realizing a robust global economy and healthy national economies.

Anti-Competitive Foreign Practices in Digital Trade

Unfortunately, an increasing number of countries are introducing anti-competitive practices in digital trade, including restrictions on the free flow of both data and ICT products and services and in some cases outright digital content theft. Many of these practices take the form of localization barriers to trade (or LBTs)—measures designed to protect, favor, or stimulate one country's domestic industries, service providers, or intellectual property (IP) at the expense of other countries' goods and services. LBTs include an array of practices such as local content requirements; restrictions on government procurement; requirements that enterprises provide services using local facilities or infrastructure, like mandated local data storage or processing of financial transaction requirements; or unjustified requirements to conduct duplicative conformity assessment procedures in-country. The World Trade Organization (WTO) finds

that these types of LBTs and other non-tariff barriers are twice as trade restrictive as traditional tariff barriers and account for the majority of trade barriers in place among countries today.

Regarding the digital data trade, almost two dozen countries, developed and developing alike—including Australia, Brunei, Canada, China, France, Greece, India, Indonesia, Kazakhstan, Malaysia, New Zealand, South Korea, Taiwan, Turkey, and Vietnam, among others—have already introduced or are actively considering local data storage requirements or onerous data security and data privacy regulations that create geographic restrictions on where corporations or ICT service providers (such as cloud computing service providers) can store and process data.

For example, Brunei, Greece, China, India, and Malaysia have all passed laws which require that data generated within the country be stored on servers within the country. Vietnam's Draft Decree on Information Technology Services would require companies' Web search portals, data centers, and cloud computing services be located in Vietnam. Likewise, Indonesia's draft Local Data Center Law would require all data carriers, including mobile phone providers and foreign banks operating in Indonesia, to have a local data server/center in the country.

Elsewhere, both the Norwegian and Danish Data Protection Authorities have issued rulings to prevent the use of cloud computing services when servers are not located domestically. Russia, Venezuela, and Nigeria have all passed regulations requiring that IT infrastructure for payment processing be located domestically. And South Korea's Financial Services Commission is considering regulations that would require insurers and other financial institutions to maintain servers for housing company financial data in-country and restricting transfers of such data outside of South Korea's borders.

These restrictions on the cross-border flow of information disadvantage a wide range of U.S. enterprises from financial and health care services to cloud computing server providers such as Amazon, Rackspace, and Google. They diminish the ability of service providers to distribute data over a diverse geographic region to ensure redundancy and increase reliability, while also raising the cost to compete since it may not be economically viable for a foreign competitor to build a new data center in-country.

But LBTs don't just impact trade in digital data; they are becoming increasingly prevalent with regard to trade in digital goods, and nowhere more so than in India. In February 2012, the Indian Ministry of Communications and Information Technology announced a Preferential Market Access mandate for electronic goods (the PMA Mandate) which imposes local content requirements on procurement of electronic products by government and private sector entities with "security implications for the country."

A specified share of each product's market—anywhere from 30 to possibly even 100 percent—would have to be filled by India-based manufacturers, with the local content share for each product rising over time. The policy's coverage is so broad that it could easily capture half of India's ICT marketplace. One of the goals of India's PMA Mandate is to have at least 80 percent of the computers and electronics sold in India be manufactured domestically by 2020.

Beyond the PMA, India appears poised to exclude foreign ICT vendors from participating in the country's recently announced \$4 billion national fiber optic network project to bring high-speed Internet to rural areas of the country. It has also announced a new compulsory registration scheme (which goes into effect in April 2013) that requires duplicative, in-country certification testing on a range of computer and electronics equipment. Likewise, China's Multi-Level Protection Scheme (MLPS) requires onerous local IP and testing requirements for ICT in certain critical infrastructures.

Elsewhere, Brazil has imposed restrictions on foreign enterprises' participation in the development of a 4G wireless telecommunications network, requiring that at least 60 percent of the equipment used be sourced locally. Likewise, Indonesia's wireless broadband decree requires that at least 40 percent of the equipment used in wireless network deployment today and 50 percent by 2017 be sourced locally. And Nigeria has gone a step further, implementing an act banning procurement and use of foreign computers and technological products in public institutions in Nigeria (when locally made products are available for use).

One reason the digital trade linkage between products and services is so important is that the increasing phenomenon of "servicization" means that products are increasingly being sold as services. For example, General Electric (GE) no longer sells individual radiological equipment (e.g., MRI or X-Ray machines) to hospitals; rather it sells radiological services, whereby GE takes over for example a hospital's entire suite of radiological assets, installing the devices with remote-monitoring capabilities that allow GE to know if they are operating and functioning properly or to diagnose various failure models. In other words, GE is selling its products as a package of bundled services, with the quality of GE's service offering being dependent on the digital data stream produced by its devices. (In a like manner, GE's Aircraft Engines division no longer sells airlines individual jet engines; it sells them "guaranteed thrust." And Johnson Controls no longer sells individual heating or air conditioning units; it sells to customers a service—"chilled air.") The point is that these "servicized" business models account for an increasingly large share of the economy—and digital trade—and they depend upon the free flow of unfettered data across borders;

any trade restrictions that impede the free flow of such information imperil these digital-data-predicated business models.

Beyond policies that impose localization barriers to digital trade or that restrict cross-border data flows, it's also important to note that global digital trade continues to be impaired by rampant outright digital content theft in a number of countries. For example, the Business Software Alliance's *2011 Global Piracy Study* estimated the commercial value of PC software theft in 2011 to equal \$63.4 billion. Software piracy rates reached an astounding 88 percent in Venezuela, 86 percent in Indonesia, 81 percent in Vietnam, and 77 percent in China. And while it would be bad enough if these were only private sector infringements, despite a ten-year-old government order, at least 80 percent of Chinese government computers run versions of Microsoft Windows operating systems that were illegally copied or otherwise not purchased. Music piracy is also a challenge. For example, the International Federation of the Phonographic Industry (IFPI) estimates that more than half of internet users (54 percent) access unlicensed services on a monthly basis in India. Such rampant digital piracy distorts global trade, threatens the production of digital content in the future, and costs jobs in the United States.

Also an issue is countries' manipulation of technology standards in order to benefit domestic enterprises at the expense of foreign ones. China has perhaps been the most aggressive country in manipulating technology standards. For example, China has attempted to give its wireless telecommunications equipment manufacturers and operators a competitive advantage by developing a domestic standard and then forcing foreign companies to adopt it for their Chinese products and operations. In addition to mandating standards, the Chinese government dominates the process and runs it without international consensus. It drafts most standards without foreign, or even public, input.

As Figure 1 illustrates, there are a growing number of international ICT standards that most countries have adopted through a regular, open, industry-led standards-setting process for which China is currently trying to establish its own domestic standards, several of which the country is seeking to make compulsory in products sold in China.

Figure 1: Chinese ICT Standardization

Technology—Product Category	International Standard	Chinese Standard
Wireless—Home Networking	WiFi	WAPI
Wireless—Mobile TV	3G; WiMAX	TD-SCDMA;McWii
Wireless—Storage	RFID	China RFID
Security—Personal Computers	TPM (Trusted Protocol Manager)	TCM (Trusted Cryptographic Manager)
Consumer Electronics—Terrestrial TV	DVB-T	DTMB (Compulsory)
Consumer Electronics—Satellite DTV	DVB-S	ABS-S
Consumer Electronics—IPTV	Open IPTV	CCSA
Video Codec	Various MPEG formats	AVS
DRM (Digital Rights Management)	Marlin, OMA DRM, or DTCP-IP	China DRM

One of the primary reasons why China seeks to manipulate technology standards is so that its firms won't have to pay royalties on embedded foreign intellectual property, while by creating indigenous technology standards that are required to go into Chinese products, it can force foreign firms to pay royalties to Chinese firms. Because the Chinese government knows that it has considerable "market power" over foreign companies due to its sheer size, it knows that unless challenged by other governments or the WTO it has considerable leeway in unilaterally setting standards to favor domestic firms and force foreign firms to pay licensing fees. Such was the Chinese government's motivation when it announced that by June 2004 the Wireless Local Area Network Authentication and Privacy Infrastructure (WAPI) standard would be mandatory for both domestic and foreign companies to use for Wi-Fi technology going into computers, even though an international standard had existed since 1997. While the government claimed WAPI was justified because it was more secure than the existing standard, there was no evidence of this; its true motivation was to force foreign companies to pay license fees to Chinese companies and to surrender U.S. technology.

Another example of technology standards manipulation is that both the Chinese and Korean governments have supported the development of mandated domestic radio frequency identification (RFID) standards,

without international participation or consensus, despite the fact that global standards for RFID have long-existed.

Conclusion

In conclusion, an increasing number of countries erroneously believe that they can boost domestic jobs and economic growth through modernized import substitution industrialization policies that erect barriers to trade in digital goods and services. Unfortunately, these countries are likely to only end up hurting themselves and the global economy. Barriers to digital trade damage the competitiveness of domestic producers and consumers by raising the cost of general purpose technologies like ICTs that are a foundational input to companies operating in virtually all manufacturing and services industries. Moreover, global trade raises the level of local competition within economies and actually enhances domestic production in the long run.

Nowhere have the effects of countries shielding themselves from trade in digital goods been more apparent than in new OECD data measuring trade in value added. The OECD compared countries' participation in global ICT value chains based on whether or not countries are members of the Information Technology Agreement (ITA) or not. They found that countries not participating in the ITA saw their participation in global ICT value chains decline by over 60 percent from 1995 (when the ITA was chartered) to 2009. This leaves a clear message: countries that don't participate in open cross-border flows of digital information and ICT products only end up excising themselves from global production networks.

Going forward, strong leadership from U.S. trade policymakers will be necessary both to combat unfair digital trade practices that other nations are using to block foreign competitors in the rapidly growing cloud computing industry, and to demonstrate to these countries such practices are neither in the interest of their own or the global economy.