Computer & Communications Industry Association
1972-2012: 40 YEARS OF TECH ADVOCACY

Primer: Issues in International Digital Trade

With the growing impact of the Internet on global productivity and commerce has come policies that hinder its potential and impede digital trade: blocking and filtering actions; forced localization mandates; onerous intermediary liability rules; and investment restrictions. Inadequate copyright limitations and low *de minimis* customs values have also been a source of concern. These policies have emerged in different forms across different geographies, but they generally result in tipping the balance of digital trade in favor of domestic industries through national laws or regulations, or overall impeding digital trade. Such policies harm the economic potential of U.S. companies and restrict the choices available to domestic consumers. This memo provides a brief overview of such policies.

Blocking/Filtering: Perhaps the most apparent barriers to digital trade are the outright filtering and blocking of U.S. Internet platforms and online content.[1] Methods can vary from legal or regulatory obligations imposed upon intermediary services, or network-level actions achieved through state control of communications, to technology mandates that hobble user privacy and security or that force product manufacturers to include intrusive monitoring technology. These practices have trade-distorting effects well beyond the services directly involved, and they likely violate WTO obligations. As CCIA noted, in submitted testimony last year[2], GATS (as well as GATT) requires reasonable publication and impartial administration of trade-related regulatory measures. When U.S. services encounter arbitrary restrictions, often at odds with what domestic competitors are subjected to, it likely constitutes a GATS violation. The market access commitments contained in GATS Article XVI also apply in this context.

- *China:* For many years U.S. sites, platforms, and services have been intermittently or persistently blocked at the network level, often over relatively trivial content. High-profile examples of targeted blocking of whole services in China include Facebook, Picasa, Twitter, Tumblr, Google Search, Foursquare, Hulu, YouTube, Dropbox, LinkedIn, and Slideshare. Chinese authorities have also been known to redirect traffic from U.S.-based search engines to Baidu, their China-based competitor.

- *Turkey:* Social media accounts are frequently subject to censorship in Turkey, which adopted laws in February 2014 allowing it to 'preventively' block websites for vague reasons, such as 'insulting' content. The recent unrest in Syria has led to further government censorship with Turkish authorities censoring websites and Twitter accounts accused of spreading Kurdish propaganda, including journalism sites.

- *Russia:* Russia's 2012 Internet blacklist law, depending how expansively it is used, has the potential to block numerous American owned websites and services. According to a 2013 Freedom House report,

[1] *See, e.g.*, Office of the U.S. Trade Representative, *The 2016 National Trade Estimate Report*, at 91, 213, 336, 429, 456 https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf.

[2] Matthew Schruers, Testimony before the U.S.-China Economic and Security Review Commission, *Commercial Espionage and Barriers to Digital Trade in China* (June 15, 2015), http://www.uscc.gov/sites/default/files/Schruers%20Testimony.pdf.

"[b]locking access to information on entire websites, IP addresses, and particular webpages has become the most common means in Russia to restrict user activity on the Internet."[3]

Forced Localization: Various countries have implemented data localization policies, such as mandated server localization or local storage of domestic citizens' data.[4] While such policies are ostensibly aimed at ensuring domestic privacy or promoting local economic development, studies have cast doubt on the effectiveness of these policies to achieve either goal.

- *Russia:* In September 2015, Russia's Federal Law No. 242-FZ entered into effect. The law requires all operators processing the personal data of Russian citizens, including groups like online retailers with no actual presence in Russia, but who target its market, to use databases located in Russia. Data controllers with a Russian presence must also disclose the location of the databases to the Russian Data Protection Authority.

- *China:* China enforces a variety of regulations relating to data location. National security regulations prevent the transfer of data abroad if it contains a state secret, which is defined broadly to include all communication of "matters that have a vital bearing on state security and national interests." A 2011 law also prohibits financial institutions from analyzing, processing, or storing offshore personal financial information of Chinese citizens. Such policies continue to be frequently considered, as shown by a recently enacted cybersecurity law that had initially contained onerous language on data localization.[5]

- *Germany:* In late 2015, the German Parliament approved a national Data Retention Act, stipulating that telecom providers and ISPs must store certain traffic data for 10 week periods. Crucially, this data must be located on a server in Germany. The federal government has also been developing a plan for a federal cloud (called "Bundes-Cloud"), which, while ostensibly about streamlining government IT processes, has created concerns about data localization mandates. For example, a measure on procuring cloud services called Resolution 2015/5 requires that "sensitive" information be localized on servers inside Germany and that cloud suppliers guarantee that information not be subject to any disclosure obligations in foreign jurisdictions.

- *Indonesia:* Since 2012, service providers that offer a "public service" are required to maintain data servers within the country. The Ministry of Communication has also recently sought to compel that data centers be maintained domestically for purposes of disaster recovery, extending this mandate to all information technology providers.

[3] 2013 Report, *Freedom on the Net: Russia,* FREEDOM HOUSE 5 (2013), *available at* https://freedomhouse.org/sites/default/files/resources/FOTN%202013_Russia.pdf.

[4] *See, e.g.*, Office of the U.S. Trade Representative, *2016 National Trade Estimate Report*, at 85-90, 213, 231, 376, 429, 456 https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf

[5] Chris Buckley, *China Passes Antiterrorism Law That Critics Fear May Overreach*, NYT.COM (Dec. 27, 2015), http://www.nytimes.com/2015/12/28/world/asia/china-passes-antiterrorism-law-that-critics-fear-may-overreach.html (While U.S. pressure helped get that language removed, the law still requires telecoms and Internet companies to provide technical assistance to law enforcement in probes meant "to avert and investigate terrorist activities.").

Intermediary Liability Protections: The safe harbors provided in U.S. law to online intermediaries have been key to the growth of Internet commerce in the United States. Some countries, however, lack similarly modern safe harbors and instead enforce a "shoot-the-messenger" rule against intermediaries.[6] Given the scale of the Internet and the importance of user-generated content, holding intermediaries liable for content posted by users short-circuits the economic engine that allows these Internet services to thrive, and places private companies in the awkward position of deciding what speech to censor prior to receiving a court order. Although laws that impose liability on internet platforms are difficult and burdensome for large companies like Google, Facebook, and Twitter, they often prove fatal to the business models of new companies and small and medium enterprises (SMEs), who can't shoulder the liability risk or hire the staff necessary to monitor all user-generated content on their platforms. As a result, onerous intermediary liability rules deter investment and market entry, especially for SMEs (both domestic and foreign).

Current examples include:

- *Estonia*: In 2015, the European Court on Human Rights upheld an Estonian court's decision that the local news portal Delfi could be liable for comments posted under news articles on its site after a ferry operator targeted by commenters took the portal to court. This decision conflicts with the existence of safe harbors in the EU's E-Commerce Directive, and the decision will likely have important consequences in Europe.

- *Vietnam:* The 2013 Decree No. 72, concerning "Management, Provision, and Use of Internet Services and Online Information", contains articles describing the obligations of social networks or information aggregators to not provide 'prohibited acts', including such vaguely defined behaviors as "Opposing the State of...Vietnam" or "Providing information...offending the...honor and dignity of individuals."

- *Thailand:* The 2007 Computer Crime Act, while slightly amended in 2015 to exempt service providers from liability if they destroy offending data, nevertheless still contains onerous provisions under which ISPs may be found liable for users' speech even without a prior court order.

Copyright Balance: Balanced copyright rules such as fair use and related limitations and exceptions have been critical to the growth of the U.S. technology and Internet economy. However, digital platforms have been harmed in countries that lack such limitations. In fact, other countries have considered developing imbalanced copyright regulations, which contradict established multilateral obligations (such as the Berne Convention):

- *Europe*: Germany and Spain have implemented policies variously called 'neighboring rights' or 'link taxes,' which compel news aggregators and other Internet services to pay publishers if they display text quotations from publications in search results.[7] The Spanish version does not allow publishers to waive these rights, and forces them to receive payment through a government-designated entity. The policy forced Google to suspend its News service in the country, and studies have revealed the harmful

[6] *See* OFFICE OF THE U.S. TRADE REPRESENTATIVE, *supra* note 4, at 178, 213.

[7] *See* OFFICE OF THE U.S. TRADE REPRESENTATIVE, *supra* note 4, at 179. These rules appear to violate the Berne Convention and other international obligations. *See* CCIA, *Understanding "Ancillary Copyright" in the Global Intellectual Property Environment* (2015), http://cdn.ccianet.org/wp-content/uploads/2015/02/CCIA-Understanding-Ancillary-Copyright.pdf

impact on smaller publishers. There are ongoing concerns that such policies may be implemented across the EU.

***De Minimis* Customs Thresholds:** Recently enacted U.S. law raised the *de minimis* value threshold for imports from $200 to $800. When its value is below this level, an import is generally free from duties and taxes. This measure will strengthen the trading environment for importers specializing in lower-value goods and SMEs using the Internet. Raising this value also allows smaller importers to avoid the time-consuming burden of customs administrative costs. Several other countries have extremely low *de minimis* customs levels, which, if raised, would benefit SMEs and Internet commerce:

- *Canada*: Canada's *de minimis* threshold is one of the lowest in the world; it has been set at $20 Canadian (roughly $16 USD at current exchange rates) since 1985.

- *European Union:* Goods with a total value no higher than 150 euros (≈$170) are exempt from import duties. Member states also impose a *de minimis* level for exemption from VAT of between 10 and 22 euros. Most Member States apply the 22 euro limit ($25).

- *China:* The Global Express Association describes China's *de minimis* value as "shipments with duty and VAT liability less than RMB 50." (≈$8)

Investment Restrictions: Several countries have implemented restrictive policies relating to foreign investment. Such bans are usually designed to protect domestic incumbents with far-reaching impacts on market entry and consumption choices for domestic citizens.

- *India:* India has long been noted for its restrictions on foreign direct investment, particularly in ecommerce. India does not allow foreign firms to participate in B2C ecommerce, meaning foreign firms cannot own inventory and sell directly to Indian consumers online. Such a restriction inhibits the growth of India's digital economy and limits competition for consumers. India did recently clarify that it allows for 100 percent FDI in B2B 'marketplace' e-commerce (i.e. e-commerce used as a platform for third party sellers to reach Indian consumers), but there are even stipulations there. First, no single vendor in a marketplace is allowed to account for more than 25 percent of sales. Second, the e-commerce provider is prevented from offering marketplace sales or discounts.

- *China:* China implements many policies designed to restrict foreign investment, or allows investment only with mandated local participation. For example, foreign companies operating in cloud computing are forced to enter into joint partnerships with Chinese firms to conduct business. According to the State Department's Investment Climate Statement: "China's investment approval regime appears designed to foster economic growth but may also shield inefficient or monopolistic Chinese enterprises from competition, particularly those China is trying to cultivate as market leaders. Foreign investors cite rising costs...market access limitations, and unclear and inconsistent enforcement of laws and regulations as significant challenges to establishing and operating businesses in China."[8]

[8] U.S. Department of State, *2015 Investment Climate Statement – China,* STATE.GOV (May 2015), http://www.state.gov/e/eb/rls/othr/ics/2015/241518.htm