Before the
International Trade Commission
Washington, DC

In re

Global Digital Trade 2: The Business-to-Business Market, Key Foreign Trade Restrictions, and U.S. Competitiveness; and

Global Digital Trade 3: the Business-to-Consumer Market, Key Foreign Trade Restrictions, and U.S. Competitiveness; and

Scheduling of Hearing

Investigation No. 332-562
Investigation No. 332-563

PRE-HEARING BRIEF OF
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Pursuant to the request for comments published by the International Trade Commission (ITC) in the Federal Register at 83 Fed. Reg. 3,185 (Jan. 23, 2018), the Computer & Communications Industry Association (CCIA)1 submits the following pre-hearing brief.

I. INTRODUCTION

CCIA represents large, medium, and small companies in the high technology products and services sectors. CCIA members are either directly engaged in trade in digital goods and services, or facilitate it, in both the business-to-business (B2B) and business-to-consumer (B2C) context. CCIA appreciates the ITC’s continued efforts to quantify the opportunities and challenges facing this increasingly critical component of the global economy.

The Internet is now integral to international trade in services and goods. However, in recent years U.S. trading partners have begun adopting laws and regulations that hinder the further growth of cross-border delivery of Internet services and hardware. Restricted data flows, forced technology standards and localization requirements, and unbalanced intermediary liability regimes impose barriers to entry on economic sectors that may not traditionally be considered part of the technology industry, but which now rely on Internet-enabled services and hardware to reach new customers. As

1 A list of CCIA members is available at https://www.ccianet.org/members.
the Internet continues its exponential growth and becomes even more intertwined with international commerce, it is essential that policymakers have the data and evidence available to understand the nature of these barriers.

The ITC’s *Global Digital Trade 1* report provided welcomed analysis on digital trade. CCIA appreciates the opportunity to expand on how the measures identified in the report affect B2B and B2C services for the upcoming *Global Trade 2* and *Global Trade 3* reports — both of which are critical to the U.S. economy. Projections suggest that “B2B e-commerce services” in the United States will reach $1.1 trillion in 2020 and studies estimate that “B2C e-commerce” turnover in the United States in 2016 was $595.1 billion. However, it is important to recognize that the distinction between B2B and B2C may lead to an incomplete illustration of the digital market. There is not a clear separation between strictly enterprise services and products and other digital services and products used by both consumers and businesses. When a user registers to use a product or service, they do not always clearly identify themselves as a consumer or a business. The ITC should take this into consideration as they proceed with the *Global Digital Trade 2* and *Global Digital Trade 3* reports that will segregate the two markets in the analysis.

This pre-hearing brief will focus on the following measures that affect Internet services and Internet-connected devices: regulatory and policy measures relating to intellectual property rights; intermediary liability protections; restrictions on foreign investment; impediments to cross-border data flows; and lack of adequate competition in the broadband market.

---

4 Id. at 33.
II. BARRIERS TO TRADE IN THE BUSINESS-TO-BUSINESS AND BUSINESS-TO-
CONSUMER MARKETS


Industry was pleased to see that the ITC highlighted ancillary rights in the Global Digital
Trade 1 report, as they are significant barriers to trade for online services in the European market.5

Ancillary copyright laws remain a concern for CCIA members. Legislatures in Europe and
elsewhere have proposed or implemented new publisher subsidies styled as so-called “neighboring
rights” — related to copyright — that may be invoked against online news search and aggregation
services and, as USTR notes,6 raise concerns from a trade perspective. These laws deter investment
and are a violation of international obligations.7 Germany and Spain have implemented ancillary
rights legislation granting publisher subsidies. Implementation was followed by services leaving the
market. In Spain, Google shut down Google News entirely. A report by the Spanish Association of
Periodical Publications Publishers shows that, rather than helping domestic publishing, the law
actually harmed online publications that relied on new aggregators.8 Despite the problematic
implementation at the national level, the EU is nonetheless considering horizontal legislation creating
publishing rights in all Member States.9

These publisher subsidies have now been followed by a French law creating a new royalty
for indexing images on the Internet.10 While not a publisher subsidy per se, this law reflects the

5 Global Digital Trade 1, supra note 2, at 291.
NTE”).
7 CCIA, Understanding Ancillary Copyright in the Global Intellectual Property Environment (2015),
8 Asociacion Espaola de Editoriales de Publicaciones Periodicas, Informe econmico del impacto del
Nuevo Articulo 32.2 de la LPI (July 2015), http://www.aeepp.com/noticia/2272/actividades/informe-
economico-del-impacto-del-nuevo-articulo-32.2-de-la-lpi-para-la-aeepp.html.
10 French Act No. 2016-925, 7 July 2016, available at
same spirit as the German and Spanish taxes discussed above insofar as it creates a regulatory structure intended to be exploited against U.S. exporters – a “right to be indexed.” By vesting these “rights” in a domestic collecting society, the law targets an industry that consists largely of U.S. exporters.¹¹ As several industry and civil society organizations (including CCIA) have previously noted, the law will impact many online services and mobile apps.¹²

The creation of ancillary rights also conflicts with the growing universal approach to balanced copyright laws that provide relevant limitations and exceptions. Balanced copyright rules such as fair use have been critical to the growth of the U.S. technology and Internet economy. These innovations are jeopardized by weak or nonexistent limitations and exceptions in the copyright laws of other countries. A recent study illustrated how U.S. firms operating abroad in regimes with balanced copyright law and relevant limits and exceptions reported higher income and an increase in total sales, encouraging foreign investment.¹³ Further, studies show that in 2014, fair use industries accounted for 16% of the U.S. economy, employed 1 in 8 workers, and contributed $2.8 trillion to the GDP.¹⁴ U.S. exports of goods and services related to fair use increased by 21% from $304 billion in 2010 to $368 billion in 2014 driven by increases in service-sector exports.¹⁵ These economic benefits are lost when a country fails to uphold similar protections in their own copyright laws, impeding market access for U.S. companies while also deterring local innovation.

The upcoming ITC reports should identify ancillary rights and other failures to implement copyright policies that strike the correct balance as barriers in order to fully illustrate impediments to digital trade.

¹¹ In U.S. jurisprudence, image indexing has been held as lawful as fair use. See Perfect 10 Inc. v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007); Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003).
¹⁵ Id. at 6.
b. Intermediary Liability Protections

*Global Digital Trade 1* identified countries that have adopted unclear and burdensome obligations for online intermediaries. Intermediary protections are essential to digital trade in the context of both intellectual property and online speech. U.S. Internet companies continue to face challenges abroad when trying to enter new markets due to legal uncertainty and inconsistent liability rules for the conduct of their users.

Without consistent rules, digital services may choose to preemptively suppress content due to unclear obligations or strict timelines mandating removal. For example, Ukraine adopted legislation in March 2017 that established a notice and takedown system for copyright enforcement. However, the final law goes beyond what the notice and takedown system, under Section 512 of the Digital Millennium Copyright Act, requires in the United States. It appears that the legislation revises Article 52 of Ukrainian copyright law to impose 24- and 48-hour “shot clocks” for online intermediaries to act on demands to remove content in order for them to avoid liability. This deadline may be feasible at times for some larger platforms which can devote entire departments to takedown compliance, but it will effectively deny market access to smaller firms and startups. The law also effectively imposes an affirmative obligation to monitor content and engage in site-blocking, by revoking protections for intermediaries if the same content reappears on a site twice within three months, even despite full compliance with the notice and takedown system.

The *Global Digital Trade 1* report cites Russia’s copyright law that places the responsibility on ISPs to take down content. The law includes a 72-hour requirement to remove infringing content before being shut down. Since the *Global Digital Trade 1* report’s release, Russia has gone further and implemented the “Mirrors Law”, which came into effect in October 2017. This law

---

16 *Global Digital Trade 1, supra* note 2, at 291.
18 *Global Digital Trade 1, supra* note 2, at 299.
extends Russia’s strict copyright enforcement rules into new domains by requiring search providers to delist website links within 24 hours of a removal request, including for so-called “mirrors” or websites that are “confusingly similar” to a previously blocked website.19

In the context of non-IP liability, online services become unintentional arbiters of speech, left to discern whether or not the content falls within broad and unclear categories of “unlawful” content. For example, the Network Enforcement Act (“NetzDG”) law in Germany took effect in January 2018.20 The NetzDG law mandates removal of “manifestly unlawful” content within 24 hours, and provides for penalties of up to 50 million Euros. “Unlawful” content under the law includes a wide range of content from hate speech to propaganda. The law is designed to only apply to social media companies, but a wide variety of online services may also be implicated as the law is broadly written to include sites that host third-party content.21 This law is already facing scrutiny amid censorship concerns. Online services, in attempts to comply with the law, are being criticized for removing accounts for lawful speech such as satire.22

While large technology companies may have the resources to invest in human review and algorithms, not all online services can. If digital trade is to be encouraged around the world, intermediary liability rules must be clear and strike the correct balance.

---

21 Social media networks are defined as a tele-media service provider that operate online platforms (1) with the intent to make a profit and (2) on which users can share content with other users or make that content publicly available. See LIBRARY OF CONGRESS, Germany: Social Media Platforms to Be Held Accountable for Hosted Content Under Facebook Act (July 11, 2017), http://www.loc.gov/law/foreign-news/article/germany-social-media-platforms-to-be-held-accountable-for-hosted-content-under-facebook-act/.
c. Restrictions on Foreign Investment

The *Global Digital Trade 1* report outlined multiple measures relating to foreign investment.\(^{23}\) CCIA remains concerned about anti-competitive practices such as forced technology transfer and discriminatory licensing requirements, with a focus on China’s governance on digital services and technology.\(^{24}\)

Regulations threaten to compel U.S. companies to hand over operation and control of their business to domestic companies in order to operate in a foreign market. This is exemplified in China’s draft regulations on cloud services.\(^{25}\) U.S. cloud service providers are strong American exporters, supporting tens of thousands of high-paying American jobs.\(^{26}\) U.S. cloud service providers have been at the forefront of the movement to the cloud worldwide.\(^{27}\) The measures proposed in the draft are fundamentally protectionist and anti-competitive, and they threaten further growth in cloud services.

China also restricts foreign investment in virtual private networks (VPNs) as an effort to limit tools used to evade its broad Internet firewall.\(^{28}\) The ITC was correct to cite this restriction in the *Global Digital Trade 1* report.\(^{29}\) Last summer, Apple removed all VPNs from the Chinese App Store.

---

\(^{23}\) *Global Digital Trade 1, supra* note 2, at 307.


\(^{28}\) In order to offer telecommunications services in China, companies must obtain a business license, which is subject to stringent foreign ownership restrictions. VPNs and some other services are not open to foreign operators or investments. In order to offer domestic Internet Protocol VPN services, there is a 50% cap on foreign ownership of the company. Therefore, U.S. companies offering VPN services essentially may operate in China only through forced Chinese ownership.

\(^{29}\) *Global Digital Trade 1, supra* note 2, at 304.
at the direction of the government. Reports suggest that China may take further steps starting in March, subjecting “unauthorized” VPNs to more enforcement actions. U.S. VPN providers have expressed concern about the far-reaching effects for VPN providers, and for citizens and businesses operating in China.

China is also among the growing list of countries that restrict, or are looking to restrict, encryption technologies. Many countries, at the behest of their respective national security and law enforcement authorities, are considering or have implemented laws that mandate access to encrypted communications. Often the relevant provisions are not explicit, but they mandate facilitated access, technical assistance, or compliance with otherwise infeasible judicial orders. Countries considering anti-encryption laws include the Australia, Brazil, China, France, Germany, India, and the United Kingdom. These exceptional access regimes run contrary to the consensus assessments of security technologies because they are technically and economically infeasible to develop.

---


31 China to Block Overseas VPN Services from End of March, RADIO FREE ASIA (Jan. 31, 2018).

32 Liz Kintzele, VPN Ban Deadline Arrives - and Passes - and VPNs are Still Accessible in China, GOLDEN FROG BLOG (Feb. 5, 2018) (“VPNs provide an essential function of allowing people to access the information they need, as well as allowing businesses to access essential tools for operation (such as email clients). Without access to VPNs, everyone in China could truly lose access to the free and open Internet.”).

33 Global Digital Trade 1, supra note 2, at 290 (citing restrictions on cryptography in China, India, and the U.K.).


35 Harold Abelson, et al., Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications, MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE
technologists because they are technically and economically infeasible to develop and

Other restrictions on foreign investment include those directed at over-the-top services (OTT) or “rich interaction applications” (RIAs), which were cited by the *Global Digital Trade 1* report with respect to Indonesia’s OTT proposals. Online services help drive growth in some of the most profitable services offered by telecommunications providers. Indeed, a recent study found that rich interaction applications that enable immersive interaction and communication, such as photo/video sharing, payment, and chat between individuals, groups, and enterprises, contributed close to $6 trillion across 64 countries over a 16-year period. Foreign investment in these valuable services is discouraged when there are not clear distinctions between rules that apply to legacy services and emerging services.

Industry continues to express concerns over government attempts to regulate the Internet by asserting jurisdiction over transmissions. For example, one measure not cited in the *Global Digital Trade 1* report was interconnection pricing. Industry is becoming increasingly alarmed at foreign governments’ attempts to regulate Internet interconnections using outdated approaches more apt to apply to traditional telephony. This approach artificially inflates bandwidth costs and limits competition. The effects of these measures are illustrated in the Republic of Korea. Korean regulations favor three Korean ISPs at the expense of foreign ISPs and smaller domestic ISPs. U.S. company Cloudflare’s aggregate pricing per region jumped from $2.50 to $6.00 under new regulations that were introduced in 2016.

### d. Impediments to Cross-Border Data Flows

The Internet and the open flow of data across borders is key to enabling economic growth. Once small and medium-sized enterprises (SMEs) have the infrastructure necessary to access the

---

36 *Global Digital Trade 1*, supra note 2, at 308.
Internet, a computer, or a smartphone with broadband access, they can reach customers around the world and, for the first time, participate in the global supply chain for goods and services. Restrictions on cross-border data flows serve as an immediate threat to digital trade in goods and services. This is especially true in the business-to-business context.\textsuperscript{38} Despite this universal recognition, countries continue to pursue data localization policies, including mandated server localization and data storage.

Rather than ensuring user privacy or data security, forced localization creates a host of new targets of opportunity for hackers, criminals, and foreign intelligence agencies.\textsuperscript{39} Data localization rules often centralize information in hotbeds for digital criminal activity, including Indonesia, Brazil, Vietnam, and Russia, working against data security best practices that emphasize decentralization over single points of failure.\textsuperscript{40} Data localization measures also distract from the development of global efforts to counter criminal activity online, while undermining the international cooperation that is necessary to promote cross-border law enforcement access.\textsuperscript{41} Rather than promote domestic industry, data localization policies are likely to hinder economic development, restrict domestic economic activity, and impede global competitiveness. Data localization policies may also be in violation of international obligations.\textsuperscript{42}

\textsuperscript{38} Transatlantic Digital Economy, supra note 3, at 3 (“B2B e-commerce accounts for the dominant share of global e-commerce and is therefore also likely to be the most important component of cross-border sales online. . . . Official estimates put the value of global B2B e-commerce in 2013 at over $15 trillion[.]”).


\textsuperscript{42} To remain compliant with international trade rules, measures that restrict trade in services must be necessary to achieve specific legitimate national security or public policy objectives, and must not be applied in a discriminatory manner or in a way that amounts to a disguised restriction on trade in services. Data localization mandates almost invariably fail to meet this standard. In addition, these regulations are often vaguely construed, inadequately articulated and, therefore, nearly impossible to effectively implement. Article XI-XIV bis of the General Agreement on Trade in Services provides these exceptions.
Studies have shown that data localization regimes reduce economic growth in countries that have adopted such policies. Disruptions to the U.S.-EU Privacy Shield framework could affect cross-border data flows and the value provided to the over 2,400 companies that are now certified under the agreement. Localization policies also have a direct impact on SMEs that participate in B2B and B2C markets. For example, 95% of U.S. SMEs that sell products on eBay’s online platform exported to foreign markets, compared to fewer than 5% of brick and mortar businesses. Data localization policies have a significant adverse impact on these SMEs that do not have the resources to localize data around the world.

e. Lack of Adequate Competition in Broadband

In the context of broadband, inadequate competition in a market for devices or services deters foreign investment and provision of online services. This is true in countries such as Colombia where wholesale broadband access services have not been deemed to warrant ex-ante regulation in order to prevent abuse of dominance. However, it is also important to recognize that the United States still lacks the necessary


43 EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY, The Costs of Data Localisation: Friend Fire on Economic Recovery (2014), available at http://www.ecipe.org/app/uploads/2014/12/OCC32014_1.pdf at 2 (“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%).”).

44 In 2012, the Brookings Institute estimated that U.S. exports of digitally deliverable services to the EU were worth $140.6 billion, or 72% of services exports, and the EU’s share of digitally deliverable exports to the U.S. comprised 60% of services exports, amounting to $106.7 billion. See Joshua P. Meltzer, The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment, BROOKINGS INSTITUTE (2014), available at http://www.brookings.edu/-/media/research/files/papers/2014/10/internet-transatlanticdata-flows-meltzer/internettransatlantic-data-flows-version-2.pdf.


competition in the domestic market. The United States faces significant hurdles in the area of cross-border provision of B2B services – namely the lack of reasonably priced telecommunications access and the overall lack of competition in the U.S. market. For example, the FCC’s decision last year on business data service (BDS) is particularly harmful to competition and access. Despite the fact that the FCC noted that an estimated 73% of BDS locations are served by just one incumbent, and “almost all purchaser locations (97%) are served by only one or two suppliers”, the FCC decided to allow incumbent BDS providers, which already control access to these crucial broadband inputs, to arbitrarily hike their rates.

III. CONCLUSION

Given the importance of Internet services to cross-border trade, CCIA welcomes further study by the ITC on key barriers to digital trade.

Respectfully submitted,

Matthew Schruers
Vice President, Law & Policy
Computer & Communications Industry Association
655 15th Street NW, Suite 410
Washington, DC 20005

February 26, 2018

---

47 In the matter of Business Data Services in an Internet Protocol Environment, WC Dkt. No. 16-143 (rel. May 2, 2016) at ¶ 181.
48 See Price Change Notification, AT&T US Domestic Access Channels, (Apr. 14, 2017), http://serviceguidenew.att.com/apex/sg_landingpage?tgtPg=sg_nonArchivedFilePreviewer&testid=0681A000030EbnQAE (announcing AT&T’s plans to increase prices for intrastate private line DS3 services by 15%, which would take effect “on or after April 20, 2017”, which was the date of the FCC’s Open Meeting in which it ultimately approved of the final BDS Order that radically altered the FCC’s rules).