Computer & Communications Industry Association
Tech Advocacy Since 1972

April 6, 2018

Ms. Lisa R. Barton
Secretary to the Commission
U.S. International Trade Commission
500 E Street S.W.
Washington, DC 20436

Re: Investigation No. 332-562 and Investigation No. 332-563

Dear Ms. Barton:

Pursuant to the request for comments published by the U.S. International Trade Commission (ITC) in the Federal Register at 83 Fed. Reg. 3,185 (Jan. 23, 2018), the Computer & Communications Industry Association (CCIA) submits this written submission regarding:

1. Investigation No. 332-562, Global Digital Trade 2: The Business-to-Business Market, Key Foreign Trade Restrictions, and U.S. Competitiveness; and

2. Investigation No. 332-563, Global Digital Trade 3: The Business-to-Consumer Market, Key Foreign Trade Restrictions, and U.S. Competitiveness.

CCIA has filed these comments electronically and will submit eight true paper copies to the ITC prior to the deadline listed in the Federal Register. Thank you for your consideration of these comments.

Respectfully submitted,

/s/ *Matthew Schruers*

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

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	Investigation No. 332-562
Global Digital Trade 3: The Business-to-Consumer Market, Key Foreign Trade Restrictions, and U.S. Competitiveness	Investigation No. 332-563

SUBMISSION 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 written submission regarding Investigation No. 332-562 and Investigation No. 332-563.

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. These written comments incorporate and expand on CCIA's prior submissions to the ITC, as well as comments provided in response to requests from the Office of the U.S. Trade Representative regarding barriers to digital trade.[2]

---

[1] A list of CCIA members is available at https://www.ccianet.org/members.

[2] Pre-Hearing Comments of CCIA, In Re Global Digital Trade Reports, Investigation Nos. 332-562, 332-563, filed Feb. 26, 2018, *available at* http://www.ccianet.org/wp-content/uploads/2018/03/PHB-to-USITC-2.2018.pdf [hereinafter "CCIA Pre-Hearing Brief"]; Post-Hearing Comments of CCIA, In Re Global Digital Trade Reports, Investigation No. 332-562, 332-563, filed Mar. 20, 2018, *available at* http://www.ccianet.org/wp-content/uploads/2018/03/CCIA-Post-Hearing-Comments-for-ITC-Global-Digital-Trade-Reports.pdf [hereinafter "CCIA Post-Hearing Comments"]; Comments of CCIA, In re Request for Public Comments for National Trade Estimate Report, USTR Dkt No. 2017-0013, *available at* http://www.ccianet.org/wp-content/uploads/2017/10/CCIA-Comments-for-2018-NTE-1.pdf; Comments of CCIA, In re Request for Public

The removal of foreign barriers to Internet-enabled commerce and export of digital goods and services is critical to the American economy.[3] In recent years U.S. trading partners adopted 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 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 and their impact on U.S. firms.

The ITC's *Global Digital Trade 1* report provided welcomed analysis on digital trade.[4] 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. This submission will expand on the following measures identified in CCIA's pre-hearing brief that affect Internet services and hardware: 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.

II. DISTINGUISHING BETWEEN B2B AND B2C

The ITC requested comments from the public on measures in key foreign markets that affect the ability of U.S. firms to develop and/or supply B2B and B2C digital products and services abroad. B2B and B2C services are critical to the U.S. economy. Projections suggest

---

Comment for 2018 Special 301 Review, USTR Dkt No. 2017-0024, filed Feb. 8, 2018, *available at* http://www.ccianet.org/wp-content/uploads/2018/02/CCIA_2018-Special_301_Review_Comments.pdf.

[3] One paper calculates that the Internet represents approximately 6% of the total U.S. economy, with mobile Internet and app services alone contributing to 3.11% of U.S. GDP. Christopher Hooton, *Refreshing Our Understanding of the Internet Economy*, INTERNET ASS'N (Jan. 2017), https://cdn1.internetassociation.org/wpcontent/uploads/2017/01/Refreshing-Our-Understanding-Economy-Internet-Association.pdf. In 2012, technology and Internet related industries represented 20% of the top 20 companies in the world, 40% of the top 5, while in 2017, technology and Internet-related industries represent 40% of the top 20 companies and 100% of the top 5. Mary Meeker, Internet Trends 2017, at 324-25 (2017), http://www.kpcb.com/internet-trends.

[4] U.S. INT'L TRADE COMM'N, Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions (Aug. 2017), Investigation No. 332-561, *available at* https://www.usitc.gov/publications/332/pub4716_0.pdf (hereinafter "Global Digital Trade 1").

that "B2B e-commerce services" in the United States will reach $1.1 trillion in 2020[5] and studies estimate that "B2C e-commerce" turnover in the United States in 2016 was $595.1 billion.[6] CCIA's comments discuss regulatory barriers and the impact of these barriers to U.S. firms operating in both the B2B and the B2C market. As CCIA noted in its pre-hearing statement, the distinction between B2B and B2C services and products 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. There are some issues that are more frequent in the context of each. However, these trade barriers are not strictly limited to either B2B or B2C and affect services and hardware in each market. For example, 21% of B2C e-commerce transactions are cross-border, and are projected to grow to 30% by 2020.[7] Likewise, the B2B cross-border e-commerce market had an estimated value of $1.8-$2 trillion in 2014.[8] Restrictions on cross-border data flows discussed on p. 17 of these comments would negatively impact both markets. The ITC should ensure that digital trade barriers identified below are reflected in both reports in order to adequately characterize threats faced by U.S. firms.

III. IMPACT OF IDENTIFIED BARRIERS TO DIGITAL TRADE

a. Regulatory and Policy Measures Relating to Intellectual Property Rights

Legislatures in Europe and EU Member States 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 raise concerns from a trade perspective.[9] These laws deter investment in online services and are a violation of international obligations.[10] Industry was pleased to see that the ITC highlighted ancillary rights in the *Global*

[5] Daniel S. Hamilton, The Transatlantic Digital Economy (2017) at 31 [hereinafter "The Transatlantic Digital Economy"].

[6] *Id*. at 33.

[7] *Id*. at 34.

[8] *Id*. at 31.

[9] The U.S. Trade Representative has also identified these laws as a trade barrier. Office of the U.S. Trade Rep. 2018 Digital Trade Barriers Fact Sheet (2018), https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital ("These measures impose financial and operational burdens on U.S. firms that help drive traffic to publishing sites."); Office of the U.S. Trade Rep., 2017 National Trade Estimate Report on Foreign Trade Barriers at 162 (2017), https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf.

[10] The imposition of a snippet tax conflicts with U.S. law and violates long-standing international law that prohibits nations from restricting quotation. These regulations not only undermine market access for U.S. online services and depart from established copyright law; they also contravene World Trade Organization (WTO)

Digital Trade 1 report, as they are significant barriers to trade for online services in the European market.[11]

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. This innovation is jeopardized by weak or nonexistent limitations and exceptions in the copyright laws of foreign countries. A 2017 study illustrated how U.S. firms operating abroad in regimes with balanced copyright law reported high incomes and increased total sales, encouraging foreign investment.[12] Another study showed 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 GDP.[13] 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.[14] 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 looking to export, while also deterring local innovation.

The upcoming ITC reports should identify ancillary rights and other failures to implement copyright polices that strike the correct balance as barriers in order to fully illustrate impediments to digital trade. The following regions discussed below have either adopted or are considering adopting ancillary rights regimes: the European Union, France, Germany, and Spain.

1. The European Union

In September 2016, the European Commission submitted a copyright reform proposal to the European Parliament and the European Council.[15] Article 11 of the EC's proposal creates a

---

commitments. By imposing a levy on quotations, these entitlements violate Berne Convention Article 10(1)'s mandate that "quotations from a work . . . lawfully made available to the public" "shall be" permissible. As TRIPS incorporates this Berne mandate, compliance with Article 10(1) is not optional for WTO Members; non-compliance is a TRIPS violation. Berne Convention for the Protection of Literary and Artistic Works, Sept. 28, 1979, art. 10(1), amended Oct. 2, 1979 (emphasis supplied).

[11] *Global Digital Trade 1*, *supra* note 4 at 291.

[12] Sean Flynn & Mike Palmedo, *The User Rights Database: Measuring the Impact of Copyright Balance*, PROGRAM ON INFORMATION JUSTICE & INTELLECTUAL PROPERTY (Oct. 30, 2017), http://infojustice.org/archives/38981.

[13] CCIA, *Fair Use in the U.S. Economy: Economic Contribution of Industries Relying on Fair Use* (2017), http://www.ccianet.org/wp-content/uploads/2017/06/Fair-Use-in-the-U.S.-Economy-2017.pdf, at 4.

[14] *Id*. at 6.

[15] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM (2016)593 {hereinafter "Copyright Proposal"].

new right for press publishers.[16] This proposal would limit access to news content and hamstring search and social media functionality in an attempt to compel principally U.S.-based online services to subsidize EU publishers.[17] If adopted, this new right will be detrimental to small press publishers, Internet users, and more generally to the free flow of information.

The EU's proposal is more expansive than previous efforts in Germany and Spain. Article 11 of the proposal empowers a new class of plaintiffs with a twenty-year, retroactive entitlement to control reproduction and making available of "press publications," independent of the journalist's underlying rights. Unlike the German law (p. 7), the new EU proposal lacks any exception for short snippets and is not limited only to search engines. Accordingly, it threatens to sweep in social networking and other services whose users rely on snippets when sharing content with friends.[18] Retroactivity means that these problems would extend to news content dating from the prior century.

Despite a study from the European Parliament criticizing the publisher's right,[19] the proposal continues to proceed.[20] As explained in CCIA's post-hearing comments,[21] a compromise is currently being discussed among EU Member States' permanent representatives.

---

[16] *Id*. at art. 11.

[17] This proposal does not have the support of the entire publishing industry, as some proponents of these new rights have claimed. Press publishers including the Spanish Association of Periodical Publications, the Italian Online Publishers Association, El Diario, Golem.de, the European, and Les Echos sent a letter opposing the introduction of an European ancillary copyright. See Statement on the Digital Single Market, Dec. 4, 2015, http://www.aeepp.com/pdf/151204_Statement_on_Digital_Single_Market_FINAL.pdf.

[18] This is also true for search services - a widely profitable industry whose estimated value was at least $780 billion worldwide in 2011. Jacques Bughin et al., *The Impact of Internet Technologies: Search*, MCKINSEY GLOBAL INSTITUTE (2011), *available at* http://www.mckinsey.com/insights/marketing_sales/measuring_the_value_of_search.

[19] L. Bently, Strengthening the Position of Press Publishers and Authors and Performs in the Copyright Directive, Legal Affairs Committee of the European Parliament (2017), available at http://www.europarl.europa.eu/RegData/etudes/STUD/2017/596810/IPOL_STU(2017)596810_EN.pdf (expressing doubts that "proposed right will do much to secure a sustainable press" and that the "implications of article 11 for the re-use of snippets are [...] extremely serious", that there is "no concrete need to extend" this provision to cover print as well as digital uses, cautioning the EU Parliament strongly against this extension, and stating that extending the scope of this provision to cover academic journals would strongly undermine open access policies). See also Draft Opinion, Committee on the Internet Market and Consumer Protection (2017), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE599.682+02+DOC+WORD+V0//EN&language=EN ("The Rapporteur believes that the introduction of a press publishers right under Article 11 lacks sufficient justification.").

[20] Recently, it was made public that the EC also requested a study on the publisher's right, its draft version made available through a public information request. The draft report concludes that "The available empirical evidence shows that newspapers actually benefit from news aggregation platforms in terms of increased traffic to newspaper websites and more advertising revenue." *See* Study: The Economics of Online News Aggregation and Neighbouring Rights for News Publishers, ASK THE EU.ORG (last visited Apr. 6, 2018), https://www.asktheeu.org/en/request/study_the_economics_of_online_ne.

[21] *CCIA Post-Hearing Comments*, *supra* note 2 at 2.

One compromise creates a relatively more reasonable solution, replacing the new right in the proposed Directive with a "presumption of entitlement to license and enforce the rights in their press publications."[22] The other compromise goes further than the EU's proposed Article 11 towards an explicit neighboring right for extracts of press publications. This compromise option would provide "that the uses of extracts of press publications should be subject to the authorisation of the press publisher."[23] This option would be a clear violation of international commitments as it restricts the quotation right for online publications.[24] CCIA continues to follow the developments closely and fears that the EU may be inclined to ignore the evidence provided by their own committees and pursue this option.

2. France

In addition to creating ancillary rights, other EU Member States are expanding the scope of existing exclusive rights of reproduction and communication to the public. In January 2017, a French regulation took effect that created a new royalty for indexing images on the Internet.[25] One provision of this legislation transfers rights in reproduction and communication to the public of pictures that are automatically indexed by search and ranking services to a French collecting society. While not a snippet tax *per se*, this law reflects the same intent as the German and Spanish taxes, insofar as it creates a regulatory structure intended to be exploited against U.S. exporters — a "right to be indexed."

By vesting the ability to monetize this entitlement in a domestic collecting society, the law directly targets an industry that consists largely of U.S. exporters. CCIA is among several industry and civil society organizations that have highlighted how the law will impact online

---

[22] The legal presumption does raise some questions. See Maud Sacquet, *The EU Copyright Reform: Will the EU Parliament Fix the EU Commission's Disastrous Proposal?*, THE DISRUPTIVE COMPETITION PROJECT (Mar. 29, 2017), http://www.project-disco.org/intellectualproperty/032917-eu-copyright-reform-will-eu-parliament-fix-eu-commissions-disastrous-proposal/#.WqLZfxPwZTa ("However, it needs to be looked at carefully, as it does not seem as if it would solve all issues raised by the 'publisher's right'. What impact, for instance, would this legal presumption have on the open access? What about journalists granting non-exclusive licenses for one article to two different publishers?")

[23] Discussion Paper on Article 11 and Article 13, Council of the European Union, Doc. No. 5902/18, Feb. 6, 2018, available at http://data.consilium.europa.eu/doc/document/ST-5902-2018-INIT/en/pdf.

[24] By imposing a tax on quotations, these entitlements violate Berne Convention Article 10(1)'s mandate that "quotations from a work . . . lawfully made available to be public" shall be permissible. As TRIPS incorporates this Berne mandate, compliance is not optional for WTO Members.

[25] French Act No. 2016-925, 7 July 2016, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032854341&categorieLien=id.

services and mobile applications.[26] The law creates a cloud of legal uncertainty, affecting everyday activities of online users, such as posting, linking, and embedding images online.[27]

3. Germany

Germany passed a law known as *Leistungsschutzrecht* in 2013 that targeted U.S.-based exporters of news aggregation services.[28] The law prohibits the making available to the public portions of "press products" in response to queries by users of search engines. As a result, a search engine's automated indexing of online content can result in legal liability, notwithstanding that such a process is necessary to the operation of modern search engines. The legal dispute about the interpretation of ancillary copyright has reached the German civil courts.[29] In 2017, the Court of Berlin referred questions to the Court of Justice for the European Union which will likely prolong legal uncertainty for years to come.[30]

4. Spain

Spain adopted a snippet tax in 2014, as part of its *ley de propriedad intelectual*. Article 32.2 created an unwaivable right for online content publishers which is independent of the author's copyright. Under the law, "electronic content aggregation service providers" are required to license "nonsignificant fragments of aggregated content which are disclosed in periodic publications or on websites which are regularly updated, for the purposes of informing, shaping public opinion or entertaining".[31] Thus, any quotation gives rise to an obligation of

---

[26] Open Letter to Minister Azoulay, Mar. 2016, *available at* http://www.ccianet.org/wpcontent/uploads/2016/03/OpenLetter-to-Minister-Azoulay-Image-Index-Bill-on-Creation-Eng.pdf ("While the alleged benefits of such initiatives have entirely failed to materialise, their negative implications are emerging fast and are well documented. From restrictions on competition, to litigation, reduced access to information and less innovation - as the closure of a number of starts ups [sic] can attest.").

[27] *Id*. *See also* Maud Sacquet*, An Unfortunately Typical French Initiative (Plus Ca Change, Plus C'est La Meme Chose)*; THE DISRUPTIVE COMPETITION PROJECT (Aug. 26, 2016), http://www.project-disco.org/intellectual-property/082616-unfortunately-typical-french-initiative-plus-ca-change-plus-cest-la-meme-chose/#.WsZdetPwZTY.

[28] Gesetz über Urheberrecht und verwandte Schutzrechte [Urheberrechtsgesetz] [UrhG] [Copyright Act], Sept. 9, 1965, BGBL. I at 1273, as amended Oct. 1, 2013, BGBL. I at 87f (Ger.).

[29] Colin Dwyer, *German Publishers' Lawsuit Against Google Threatens to Backfire*, NPR (May 10, 2017), https://www.npr.org/sections/thetwo-way/2017/05/10/527800498/german-publishers-lawsuit-against-googlethreatens-to-backfire.

[30] The Court of Berlin has asked for guidance on whether the German legislature should have notified the European Commission under Directive 98/34/EC upon enacting the Leistungsschutzrecht into local law in 2013. *German Court Refers Publishers' Case vs Google to European Court*, REUTERS (May 9, 2017 10:48 AM), https://www.reuters.com/article/google-media-germany/update-1-german-court-refers-publishers-case-vs-google-toeuropean-court-idUSL8N1IB4LX.

[31] Law No. 21/2014, amending the Consolidated Text of the Law on Intellectual Property and Law No. 1/2000 on Civil Procedure, art. 32.2 (B.O.E. 2014, 268) (Spain).

equitable compensation, and where quoted fragments are "significant," an actual license is required.

Implementation of the new right was followed by services leaving the market. Google shut down Google News entirely in Spain.[32] The law has also allowed publishers to demand excessive license fees: one small company was asked in pay 7,000 euros a day (2.5 million euros a year) for links or snippets posted by its users.[33] It has also not achieved its alleged purpose of increasing revenues for publishers. 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.[34]

b. Imbalanced Intermediary Liability Regimes

Intermediary liability protections are essential to digital trade in the context of both intellectual property and online speech. U.S. Internet companies face challenges when trying to export to new markets due to legal uncertainty and inconsistent liability rules for the conduct of their users. Today, U.S. firms face increasing hostility in many international markets that have imposed regulatory burdens and penalties on U.S. Internet services for the conduct of third parties. This affects not only Internet companies, but also denies local small and medium-sized enterprises Internet-enabled access to the global marketplace, discouraging investment and the growth of startups.[35]

While large technology companies may have the resources to invest in human review and algorithms, not all online services can take similar actions. If digital trade is to be encouraged around the world, intermediary liability rules must be clear, consistent, and strike the correct balance. These comments expand on the following countries' practices and proposed regulations that fail to strike the correct balance: Australia, Colombia, the EU, Germany, Greece, Italy, Ukraine, and Russia.

---

[32] Google Support, Google Noticias en España, https://support.google.com/news/answer/6140047#English (last visited Apr. 6, 2018).

[33] *Nuevo Intento de Imponer el Canon AED: Piden a Meneame 2,5 Millones de Euros al Ano*, EL CONFIDENCIAL (July 2, 2017), https://www.elconfidencial.com/tecnologia/2017-02-07/canon-aede-meneameinternet-facebook-agregadores_1327333/.

[34] Asociacion Espnaola de Editoriales de Publicaciones Periodicas, Informe económico del impacto del Nuevo Artículo 32.2 de la LPI (July 2015), http://www.aeepp.com/noticia/2272/actividades/informeeconomico-del-impacto-del-nuevo-articulo-32.2-de-la-lpi-nera-para-la-aeepp.html.

[35] Matthew Le Merle et al., The Impact of U.S. Internet Copyright Regulations on Early-Stage Investment: A Quantitative Study, BOOZ & CO. (2011), http://static1.squarespace.com/static/5481bc79e4b01c4bf3ceed80/t/54877560e4b0716e0e088c54/1418163552585/Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf.

1. Australia

Australia has long been out of compliance with obligations under the U.S.-Australia Free Trade Agreement (AUSFTA) regarding its intermediary liability regime. AUSFTA contains an obligation to provide liability limitations for service providers, analogous to protections under the Digital Millennium Copyright Act.[36] However, Australia has failed to fully implement these obligations. Current protections are far narrower than what is required. Australia's current statute limits protection to what it refers to as "carriage" service providers, not service providers generally.[37] Article 17.11.29 of AUSFTA makes clear that the protections envisioned should be available to all online service providers, not merely "carriage" service providers.[38] The consequence of this limitation is that intermediary protection is largely limited to Australia's domestic broadband providers. Online service providers exporting information services into the Australian market remain in a precarious legal situation.[39]

In December of 2017, legislation was introduced in the Australian Senate to amend the Copyright Act's provisions on safe harbors. The bill would expand the intermediary protections to some service providers including organizations assisting persons with a disability, public libraries, archives, educational institutions and key cultural institutions — effectively acknowledging that the scope of the current safe harbor is too narrow.[40] However, the bill pointedly leaves out commercial service providers including online platforms. The "fix" does not put Australian copyright law into compliance with AUSFTA. The bill should make sure that limitations on liability for service providers are extended to all functions provided for under Article 17.11.29(b)(i)(A-D). Under current Australian law, protection is only extended to functions described in Article 17.11.29(b)(i)(A) through the narrow inclusion of only "carriage"

---

[36] 17 U.S.C. § 512.

[37] Copyright Act 1968 (Cth) ss 116AA-116AJ (Austl.).

[38] U.S.-Austl. Free Trade Agreement, May 18, 2004, 43 I.L.M. 1248 ("Consistent with Article 41 of the TRIPS Agreement, for the purposes of providing enforcement procedures that permit effective action against any act of copyright infringement covered under this Chapter, including expeditious remedies to prevent infringements and criminal and civil remedies, each Party shall provide, consistent with the framework specified in this Article . . . limitations in its law regarding the scope of remedies available against service providers for copyright infringements that they do not control, initiate, or direct, and that take place through systems or networks controlled or operated by them or on their behalf, as set forth in this sub-paragraph.").

[39] Australian imports from the United States of telecommunications, computer, and information services – many of which rely on intermediary protections – amounts to $1.046 billion AUD, or over $806 million USD in 2016. Australian Government Department of Foreign Affairs and Trade, Trade in Services Australia 2016, *available at* http://dfat.gov.au/about-us/publications/Documents/trade-in-services-australia-2016.pdf at 71.

[40] Draft Copyright Amendment (Service Providers) Bill 2017, http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1115_firstsenate/toc_pdf/1728220.pdf;fileType=application%2Fpdf.

service providers. The failure to include online services such as search engines and commercial content distribution services disadvantages U.S. digital services in Australia and serves as a deterrent for investment in the Australian market.

A Senate report was released in March that indicated the Government will move forward with this proposal.[41] The Senate report confirms that Australia acknowledges it is out of compliance, and intentionally failed to extend intermediary liability protections to all services covered under the FTA. If the United States does not pressure its trading partners to honor commitments, especially on commitments that are essential to a large sector of American exports, industry can expect more countries to follow Australia's example.

2. Colombia

Like Australia, Colombia has also yet to comply with obligations under a free trade agreement with the U.S. to implement an intermediary liability framework.[42] Without a safe harbor that meets the requirements of the FTA, intermediaries exporting services to Colombia remain exposed to potential civil liability for services and functionality that is lawful in the United States and elsewhere.

3. The European Union

In September 2016, the European Commission (EC) submitted a copyright reform proposal to the European Parliament and the European Council.[43] Article 13 of the proposal would require proactive monitoring and filtering content uploaded, or possibly even linked to, on their platform.

The proposal would upend nearly two decades of established law in the EU under the E-Commerce Directive by eliminating longstanding liability protections, and suggests that most modern service providers may be carved out from its limited liability protections. Consistent with U.S. law, EU law explicitly provides that online services have no obligation to surveil users, or monitor or filter online content.[44] Since its implementation, online services have invested

---

[41] Senate Report, Copyright Amendment (Service Providers) Bill 2017, Standing Committee on Environment and Communications, *available at* https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/CopyrightSPBill/Report.

[42] U.S. Trade Representative Lighthizer was correct to cite Colombia's failure to comply with commitments under the FTA regarding copyright as a basis for concern regarding Colombia accession to the Organization for Economic Cooperation & Development (OECD). Letter to Colombia Minister of Trade, Feb. 14, 2018, *available at* https://insidetrade.com/sites/insidetrade.com/files/documents/2018/feb/wto2018_0091a.pdf.

[43] *Copyright Proposal*, *supra* note 15.

[44] Compare 17 U.S.C. § 512(m)(1) (2012) with Directive 2000/31/EC art. 15(1).

heavily in European operations. These protections have also enabled the startup community in the EU to develop, attracting investment from the United States.

Article 13 of the draft proposal implies that online services must develop or procure content recognition technology, and affirmatively filter all Internet content including audiovisual works, images, and text. The EC proposal does not specify what type of filtering a provider must implement, effectively empowering foreign rightsholders to dictate U.S. services technology inconsistently across the EU. In short, a provider will never know when it has done "enough" short of litigating in every EU Member State. This is in direct conflict with what the EU Commission sought to do under the Digital Single Market initiatives — provide clarity and uniformity of rules for the digital economy across the EU.[45] It will not be until the Court of Justice of the EU eventually addresses the question, and affected hosting providers can expect inconsistent rulings and injunctions from lower courts in different countries.

The draft proposal is currently under consideration and compromises are being discussed. Unfortunately, the "compromise" texts are not encouraging. At the European Parliament, recent proposals appear to go further to remove critical protections than the EC proposal does and suggests imposing direct liability on online intermediaries.

While some Internet companies have been able to invest the resources to voluntarily create similar technologies, they were able to do so under the long-standing limited liability framework for intermediaries. Further, mandatory adoption of the technologies vaguely contemplated in the proposal would effectively shut out smaller companies from market entry. The vagueness of the language in the EU's proposals, and the likelihood of inconsistent rules in different countries, threatens to grant control of U.S. innovation to the EU. U.S. platforms, especially small business and startups, will be deterred from exporting. For example, surveys of venture capitalists show that 88% of investors are less likely to invest in user-generated content platforms in regions that have similarly ambiguous legal framework for intermediaries.[46]

---

[45] European Commission Communication, May 5, 2017, *available at* http://ec.europa.eu/newsroom/document.cfm?doc_id=44527 ("The completion of the EU Single Digital Market also needs a clear and stable legal environment to stimulate innovation, tackle market fragmentation and allow all players to tap into the new market dynamics under fair and balanced conditions. This will provide the bedrock of trust that is essential for business and consumer confidence.").

[46] Matthew LeMerle, *The Impact of Internet Regulation on Early Stage Investment*, at 20 (Fifth Era 2014), http://static1.squarespace.com/static/5481bc79e4b01c4bf3ceed80/t/55200d9be4b0661088148c53/1428163995696/Fifth+Era+report+lr.pdf.

4. Germany

Germany adopted the Act to Improve the Enforcement of Rights on Social Networks (the "Network Enforcement Law" or "NetzDG") in June 2017.[47] 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 unlawful propaganda.[48] The large fines and broad considerations of "manifestly unlawful content" have led to companies removing lawful content, erring on the side of caution in attempts to comply. Since coming into force in January of 2018, the law has already led to high profile cases of content removal and wrongful account suspensions,[49] groups have expressed concerned about its threats to free expression,[50] and the German government has already indicated that changes are needed to protect lawful speech online.[51] Further concerning is that countries including Russia, Singapore, and the Philippines have cited this law as a positive example they intend to copy in the future.[52]

---

[47] LIBRARY OF CONGRESS, *Germany: Social Media Platforms to Be Held Accountable for Hosted Content Under "Facebook Act"* (June 30, 2017), http://www.loc.gov/law/foreign-news/article/germany-social-media-platforms-to-be-held-accountable-for-hosted-content-under-facebook-act/.

[48] Referencing the German Criminal Code making illegal the following speech-related activities: dissemination of propaganda material or use of symbols in unconstitutional organizations, defamation of the state, preparation or encouraging the commission of a seriously violent offense endangering the state, treasonous forgery, public incitement to crime, breach of the peace, forming criminal and terrorist organizations, incitement to hatred, dissemination of depictions of violence, defamation of religious associations, distribution of child pornography, insult, intentional and nonintentional defamation, violation of intimate privacy by taking photographs, threatening the commission of a felony, and forgery of data).

[49] *German Satire Magazine Titanic Back on Twitter Following 'Hate Speech' Ban*, DW (Jan. 6, 2018), http://www.dw.com/en/german-satire-magazine-titanic-back-on-twitter-following-hate-speech-ban/a-42046485; Scott Roxborough, *Why Ambitious New Online Anti-Hate Speech Law is Backfiring in Germany,* THE HOLLYWOOD REPORTER (Jan. 15, 2018), https://www.hollywoodreporter.com/news/why-an-ambitious-new-online-anti-hate-speech-law-is-backfiring-germany-1074232; Bernhard Rohleder, *Germany Set Out To Delete Hate Speech Online. Instead, It Made Things Worse*, WASH. POST (Feb. 20, 2018), https://www.washingtonpost.com/news/theworldpost/wp/2018/02/20/netzdg/?utm_term=.4162c324420e.

[50] *Germany: Flawed Social Media Law*, HUMAN RIGHTS WATCH (Feb. 14, 2018), https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law ("[T]he law places the burden on companies that host third-party content to make difficult determinations of when user speech violates the law, under conditions that encourage suppression of arguably lawful speech. Even courts can find these determinations challenging, as they require a nuanced understanding of context, culture, and law. Faced with short review periods and the risk of steep fines, companies have little incentive to err on the side of free expression.").

[51] Emma Thomasson, *Germany Looks to Revise Social Media Law As Europe Watches*, REUTERS (Mar. 8, 2018), https://www.reuters.com/article/us-germany-hatespeech/germany-looks-to-revise-social-media-law-as-europe-watches-idUSKCN1GK1BN.

[52] *See supra* note 50.

5. Greece

Greece is set to establish an administrative committee that can issue injunctions to remove or block potentially infringing content. A rightsholder can now apply to the committee for the removal of content for a fee. This is a significant divergence from the U.S. framework.

6. Italy

In 2013, the Italian government adopted regulations that further empowers the Italian Communications Authority (AGCOM) to mandate removal and monitoring. The amendments "require information providers to immediately terminate infringements of copyright and related rights, if the violations are evident, on the basis of a rough assessment of facts."[53] This law further empowers AGCOM to identify appropriate measures to prevent repeat infringements, amounting to a copyright "staydown" requirement that conflicts with both Section 512 of the Digital Millennium Copyright Act and the E-Commerce Directive. Departures from established law serve as a market access barrier for U.S. services in Italy. Despite legal challenges and public outcry from different stakeholders, these regulations have been implemented resulting in over 277 disabled websites.[54]

7. Ukraine

Ukraine adopted an intermediary liability law "On state support of cinematography" (3081-D) in March 2017. The legislation revises Article 52 of Ukrainian copyright law to impose twenty-four and forty-eight hour "shot clocks" for online intermediaries to act on demands to remove content. These deadlines may be feasible at times for some larger platforms who can hire multiple employees devoted to takedown compliance, but effectively deny market access to smaller firms and startups. The law also contains affirmative obligations to monitor content and engage in site-blocking, by revoking protection for intermediaries if the same content reappears on a site twice within two months, even despite full compliance with the notice and takedown system.

---

[53] Proposta emendativa pubblicata nell'Allegato A della seduta del 19/07/2017. 1.022, available at http://documenti.camera.it/apps/emendamenti/getPropostaEmendativa.aspx?contenitorePortante=leg.17.eme.ac.4505&tipoSeduta=0&sedeEsame=null&urnTestoRiferimento=urn:leg:17:4505:null:A:ass:null:null&dataSeduta=null&idPropostaEmendativa=1.022.&position=20170719.

[54] *Italian Regulation Against Online Copyright Piracy Is Valid*, LEXOLOGY (Apr. 12, 2017), https://www.lexology.com/library/detail.aspx?g=dffbee3b-b0a1-4a37-886d-8ab886062c19.

8. Russia

The recently enacted "Mirrors Law" extends Russia's copyright strict enforcement rules[55] into new domains by requiring search providers to delist website links within twenty-four hours of a removal request, including for so-called "mirrors" or websites that are "confusingly similar" to a previously blocked website. This law, which came into effect on October 1, 2017, conflicts with principles in Section 512 of the Digital Millennium Copyright Act and U.S. copyright jurisprudence.

c. Restrictions on Foreign Investment

1. China

China has long been hostile to foreign competitors. In recent years, however, focus on U.S. Internet and technology firms has intensified as China moves to fulfill goals under its 2025 plan to achieve global dominance in designated industries. An increase of discriminatory laws directed at information infrastructure and cloud services, combined with an uptick in Internet shutdowns and censorship, increases hesitancy of businesses to enter the Chinese market. To illustrate, AmCham China's 2017 survey of its members showed that 81% of its member companies felt less welcome in China, up from 77% in 2015.[56] The survey also showed that 31% of its members said the investment environment was deteriorating — the most dire response AmCham China has received since it started asking the question in 2011.[57] CCIA remains concerned about Chinese anti-competitive governance on digital services and technology.[58]

The current U.S. Administration recognizes the concerns of the U.S. Internet and technology community with respect to China, and is taking steps to address this concern through the Section 301 investigation to determine whether the policies of the Chinese government relating to technology transfer, intellectual property, and innovation are actionable under the

---

[55] Under Russian copyright law, a copyright owner may seek a preliminary injunction to block the site hosting infringing content prior to a judgement. A website may be permanently blocked if it receives two preliminary injunctions. Federal Law No. 187-FZ, on Amending Legislative Acts of the Russian Federation Concerning Questions of Protection of Intellectual Rights in Information and Telecommunications Networks, July 2, 2013.

[56] AMCHAM CHINA, *China Business Climate Survey Report 2017*, https://www.amchamchina.org/policyadvocacy/business-climate-survey/ (also reporting that 32% of companies cited inconsistent regulatory interpretation and unclear laws as the primary challenge to doing business in China).

[57] Sui-Lee Wee, *As Zeal for China Dims, Global Companies Complain More Boldly*, N.Y. TIMES (Apr. 19, 2017), https://www.nytimes.com/2017/04/19/business/china-companies-complain.html.

[58] See Samm Sacks, *China's Emerging Cyber Governance System*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES, https://www.csis.org/chinas-emerging-cyber-governance-system (last visited Apr. 6, 2018).

Trade Act.[59] However, industry cautions against the Administration's proposed imposition of tariffs on a broad array of technologies that would raise costs for consumers and have a significant impact on the U.S. economy.[60]

CCIA expanded on concerning provisions regarding cloud service providers in its post-hearing submission.[61] U.S. cloud service providers have been at the forefront of the movement to the cloud worldwide[62] and are strong American exporters.[63] The International Trade Administration estimated that there was a surplus of cloud computing services of approximately $18 billion in 2015.[64] China has adopted discriminatory practices against U.S. cloud service providers with increasing frequency in recent years. Draft regulations in conjunction with existing Chinese laws threaten to further disadvantage U.S. companies. There are two draft regulations that threaten to significantly disadvantage U.S. providers issued by the Ministry of Industry and Information Technology (MIIT): *Regulating Business Operation in Cloud Services Market* (2016) and *Cleaning Up and Regulating the Internet Access Service Market* (2017).[65] These proposals, together with existing licensing and foreign direct investment restrictions on foreign exporters in China, would require foreign cloud service providers to turn over essentially all ownership and operations to a Chinese company – including valuable U.S. intellectual property and know-how to China.[66] These measures are fundamentally protectionist and anti-competitive, and threaten to further discourage foreign investment.[67]

---

[59] OFFICE OF THE U.S. TRADE REP., Initiation of Section 301 Investigation: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation, Docket No. USTR-201700016, Aug. 18, 2017.

[60] Joint Industry Letter to President Trump on Section 301 Investigation on China, Mar. 18, 2018, *available at* http://www.ccianet.org/wp-content/uploads/2018/03/Letter-to-President-Trump-on-301-Investigation-and-China-March-18-2018.pdf.

[61] *CCIA Post-Hearing Submission*, *supra* note 2, at 3.

[62] SYNERGY RESEARCH GROUP, *Amazon Dominates Public IaaS and Ahead in PaaS; IBM Leads in Private Cloud* (Oct. 30, 2016), https://www.srgresearch.com/articles/amazon-dominates-public-iaas-paas-ibm-leads-managedprivate-cloud.

[63] CCIA has discussed these restrictions in submissions to the United States Trade Representative. *See* Comments of the Computer & Commc'ns Indus. Ass'n, In re Request for Public Comment for 2018 Special 301 Review, Dkt No. 2017-0024, filed Feb. 8, 2018, *available at* http://www.ccianet.org/wp-content/uploads/2018/02/CCIA_2018-Special_301_Review_Comments.pdf.

[64] U.S. DEPT. OF COMM., 2017 Top Markets Report Cloud Computing, *available at* https://www.trade.gov/topmarkets/pdf/Sector%20Snapshot%20Cloud%20Computing%202017.pdf.

[65] The *Cleaning Up and Regulating the Internet Access Service Market* proposal is also aimed at restricting operations of virtual private networks (VPNs).

[66] Specifically, these measures do the following: prohibit licensing foreign CSPs for operations; actively restrict direct foreign equity participation of foreign CSPs in Chinese companies; prohibit foreign CSPs from signing contracts directly with Chinese customers; prohibit foreign CSPs from independently using their brands and logos to market their services; prohibit foreign CSPs from contracting with Chinese telecommunication carriers for Internet

China has also taken several steps to crack down on tools used to evade its broad Internet firewall through restrictions on foreign investment in virtual private network (VPN) services and prohibitions on VPNs by domestic operators.[68] A VPN allows users to access a private network securely and share data remotely, rather than over a public network, enabling them to bypass content filters and government firewalls. An estimated 90 million people in China use VPNs regularly to conduct international business and access better search engines.[69] 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.

The *Cleaning Up and Regulating the Internet Access Service Market* proposal is also aimed at restricting operations of VPNs. The United States recently raised concerns at the World Trade Organization about the proposal's impact to U.S. services, and its ability to "add to the burdens and restrictions that China's Cybersecurity Law would place on cross-border transfers of information."[70]

2. Indonesia

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*

---

connectivity; restrict foreign CSPs from broadcasting IP addresses within China; prohibit foreign CSPs from providing customer support to Chinese customers; and require any cooperation between foreign CSPs and Chinese companies to be disclosed in detail to regulators.

[67] AmCham China's survey of its members showed that 81% of its companies felt less welcome in China, up from 77% in 2015 with 32% of companies citing inconsistent regulatory interpretation and unclear laws as the primary challenge to doing business in China. The survey also showed that 31% of its members said the investment environment was deteriorating — the most dire response AmCham has received since it started asking the question in 2011. *See China Business Climate Survey Report 2017*, AMCHAM CHINA, https://www.amchamchina.org/policy-advocacy/business-climate-survey/; Sui-Lee Wee, *As Zeal for China Dims, Global Companies Complain More Boldly*, N.Y. TIMES (Apr. 19, 2017), https://www.nytimes.com/2017/04/19/business/china-companies-complain.html.

[68] For example, Apple removed all VPNs from the China App Store at the direction of the government in the summer of 2017. Laurel Wamsley, *Apple Accused of Removing Apps Used to Evade Censorship From its China Store*, NPR (July 29, 2017), http://www.npr.org/sections/thetwo-way/2017/07/29/540280448/apple-accused-of-removing-appsused-to-evade-censorship-from-its-china-store.

[69] James Palmer, *China is Trying to Give the Internet a Death Blow*, FOREIGN POLICY (Aug. 25, 2017), http://foreignpolicy.com/2017/08/25/china-is-trying-to-give-the-internet-a-death-blow-vpn-technology/.

[70] Communications from the United States, Measures Adopted and Under Development by China Relating to Its Cybersecurity Law, Feb. 23, 2018, *available at* https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=243365,243385,243363&CurrentCatalogueIdIndex=0&FullTextHash=371857150&HasEnglishRecord=True&HasFrenchRecord=False&HasSpanishRecord=False.

report with respect to Indonesia's OTT proposals.[71] 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.[72] 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 is seeing similar regulatory proposals out of the International Telecommunications Union. International organizations' attempts to regulate the Internet and Internet transmissions present a threat to U.S. Internet firms' ability to operate in the global market.

3. Republic of Korea

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 Internet, a computer, or 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. A 2016 McKinsey Institute report observed the following:

> Global flows of all types support growth by raising productivity, and data flows are amplifying this effect by broadening participation and creating more efficient markets. MGI's analysis finds that over a decade, all types of flows acting together have raised world GDP by 10.1 percent over what would have resulted in

[71] *Global Digital Trade 1*, *supra* note 4 at 308.

[72] WIK, The Socio Economic Value of Rich Interaction Applications (RIAs) (2017), http://www.wik.org/index.php?id=879&L=1.

a world without any cross-border flows. This value amounted to some $7.8 trillion in 2014 alone, and data flows account for $2.8 trillion of this impact.[73]

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.[74] 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.[75] Data localization rules often centralize information in hotbeds for digital criminal activity, including Indonesia,[76] Brazil, Vietnam,[77] and Russia,[78] working against data security best practices that emphasize decentralization over single points of failure.[79] 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

---

[73] McKinsey Global Institute, Digital Globalization: The New Era of Global Flows (2016), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

[74] *Transatlantic Digital Economy*, *supra* note 5 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[.].").

[75] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677, 718-19 (2015), http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.

[76] Since 2012, service providers providing a "public service" have been required to localize data servers within the country. USTR has noted that these requirements "could prevent service suppliers from leveraging economies of scale from existing data centers and inhibit cross-border data flows" and that while larger companies may be able to comply, "such requirements could potentially impede access for small- and medium-sized businesses." The Ministry of Communication has also recently sought to require domestic data centers for purposes of disaster recovery, extending the mandate to all information technology providers. The Indonesian government requires that the equipment used for certain wireless broadband services contain certain levels of local content, and that telecommunication providers use half of their capital expenditures on network development of locally sourced components and services. Additionally, Indonesia has issued a regulation that requires 4G enabled devices to contain 30% local content.

[77] The Decree on Management, Provision, and Use of Internet Service and Information Content Online imposes a mandate on Internet service providers to maintain a copy of all data they hold within Vietnam for purposes of access by the Vietnamese authorities. This law has been accompanied by numerous burdensome regulations for service providers, including local storage of user registration information and complete histories of posting activities on "general information websites" and social networks. These "general information websites" and social networks must also have a high-level representative of the company be a Vietnamese national and local resident.

[78] Russia signed localization measures into law in July of 2014, which went into effect on September 1, 2015. See p. 23.

[79] Rohin Dharmakumar, *India's Internet Privacy Woes*, Forbes India (Aug. 23, 2013), http://forbesindia.com/article/checkin/indias-internet-privacy-woes/35971/1. *See generally* Patrick S. Ryan *et al.*, *When the Cloud Goes Local: The Global Problem with Data Localization*, IEEE Computer, vol. 46, no. 12, at 54-59 (Dec. 2013), http://www.computer.org/csdl/mags/co/2013/12/mco2013120054-abs.html.

enforcement access.[80] 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.[81]

As CCIA's pre-hearing brief detailed, data localization policies tend to have detrimental effects to the domestic economy that introduces these mandates, decreasing growth while increasing security vulnerability. Studies have shown that data localization regimes also reduce economic growth in countries that have adopted such policies.[82] This is due to prohibitively high compliance costs. A 2014 report found that "for many countries that are considering or have considered forced data localization laws, local companies would be required to pay 30-60% more for their computing needs than if they could go outside the country's borders."[83]

These costs are felt even more by startups and SMEs who wish to compete in the international market for both B2B and B2C contexts. Complying with multiple localization regimes, many who require local presence, becomes prohibitive for these companies. 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.[84] Data localization policies

---

[80] Vivek Krishnamurthy, *Cloudy with a Conflict of Laws*, BERKMAN CTR. FOR INTERNET & SOC'Y, Research Publication No. 2016-3 (Feb. 16, 2016), https://ssrn.com/abstract=2733350.

[81] 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 XIV - XIV bis of the General Agreement on Trade in Services provides these exceptions. General Agreement on Trade in Services Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994).

[82] Matthias Bauer, et al, *Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization*, GLOBAL COMMISSION ON INTERNET GOVERNANCE (May 2016), *available at* https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf; 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%).").

[83] LEVIATHAN SECURITY GROUP, *Quantifying the Cost of Forced Localization* (2014), *available at* https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.

[84] EBAY, *2015 U.S. Small Business Global Growth* Report (2015), *available at* https://www.ebaymainstreet.com/sites/default/files/2015-us-small-biz-global-growth-report_0.pdf.

have a significant adverse impact on these SMEs that do not have the resources to localize data around the world.

This is why agreements governing cross-border transfers such as the U.S.-EU Privacy Shield Framework and the APEC cross-border data rules[85] are critical to facilitating digital trade. 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.[86]

Below CCIA expands on the threats to cross-border data flows by the following countries identified in *Global Digital Trade 1*: China, the EU, India, and Russia.

1. China

China's Cybersecurity Law went into effect on June 1, 2017 after being adopted by the National People's Congress in November 2016 following a year of legislative hearings and close international scrutiny.[87] CCIA was disappointed to see that, despite universal concerns expressed by the technology industry around the world, most objectionable provisions from the drafts remained in the final piece of legislation.[88] Of particular concern is Section II of the law which mandates operations security obligations for "critical information infrastructure." Article 37 provides that "personal information and other important data" gathered or produced in China by "critical information infrastructure" must be stored on servers physically located within China, with extremely limited exceptions.[89] Further, it is not clear what constitutes "critical information infrastructure," possibly sweeping companies outside traditional information and communication technologies into these obligations.[90] Subsequent draft notices from Chinese

---

[85] APEC's cross-border privacy rules (CBPRs) are designed to facilitate international data flows between implementing nations. The APEC approach provides a flexible framework that recognizes the complexity of data transfers, while also protecting privacy and country autonomy to set standards.

[86] 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-flowsmeltzer/internettransatlantic-data-flows-version-2.pdf.

[87] 2016 Cybersecurity Law (unofficial translation), http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en.

[88] *Overview of China's Cybersecurity Law*, KPMG CHINA (Feb. 2017), https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.

[89] Article 37 (providing that if a business can show that it is "truly necessary" to store information outside Chinese mainland borders, they must negotiate with the State Council to agree on specific monitoring procedures).

[90] Chris Mirasola, *Understanding China's Cybersecurity Law*, LAWFARE (Nov. 8, 2016) ("Article 31 suggests that it could include any services needed for public communication or information, power, transportation, water works, finance, public service, or digital governance, as well as any infrastructure that would endanger national

officials only signal further problems ahead. The Cyberspace Administration of China (CAC) issued a first draft on "Personal Information and Important Data Cross Border Transfer Security Evaluation Measures" in April 2017. Article 2 of the measure goes beyond what is in the Cybersecurity law to mandate that all personal information and "important data" must be localized in mainland China.[91]

2. The European Union

Within the European Union, many Member States have localization requirements that represent trade barriers. The think tank ECIPE has "identified 22 data localization measures where European Union Member States impose restrictions on the transfer of data . . . The most common restrictions target company records, accounting data, banking, telecommunications, gambling and government data. In addition, there are at least 35 restrictions on data usage that could indirectly localize data within a certain Member State."[92] While policymakers might reasonably impose certain security-related limits to some sets of secure data, centralization and streamlining efforts may effectively result in application of localization mandates to all government services. Like other data localization measures, this may discriminate against foreign suppliers and be a violation of WTO commitments.[93]

Recognizing the threat that numerous, conflicting national data localization laws such as those supported in France and Germany pose to the Digital Single Market, the Commission proposed a draft regulation on free flow of non-personal data within the EU.[94] The regulation aims to remove national mandated data localization laws within Member States. CCIA supports

---

security, national welfare, popular livelihood, or the public interest if destroyed or hacked. It is easy to imagine how this broad provision could be interpreted to include a huge range of foreign and domestic internet companies.").

[91] COVINGTON, *China Seeks Public Comments on Draft Regulation on Cross-Border Data Transfer* (Apr. 12, 2017), https://www.cov.com/media/files/corporate/publications/file_repository/china_seeks_public_comments_on_draft_regulation_on_cross_border_data_transfer.pdf; COVINGTON, *China Releases Near-final Draft of Regulation on CrossBorder Data Transfer*s (May 19, 2017), https://www.cov.com//media/files/corporate/publications/2017/05/china_releases_near_final_draft_of_regulation_on_cross_border_data_transfers.pdf.

[92] ECIPE*, Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localization Measures in the EU Member States* (2016), http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flowsin-the-EU.pdf. For example, Germany proposed a draft telecom bill in 2015 that would, among other things, require telecommunication service providers and Internet service providers to store data in Germany for a period of 10 weeks. Under the draft law, data needing to be stored includes phone numbers, times called, IP addresses, and the international identifiers of mobile users for both ends of a call. Furthermore, user location data in the context of mobile phone services would have to be retained for a period of four weeks.

[93] *See supra* note 81.

[94] European Commission, Digital Single Market, Free Flow of Non-Personal Data, https://ec.europa.eu/digitalsingle-market/en/free-flow-non-personal-data (last updated Oct. 5, 2017).

the proposal as it will limit forced data localizations in EU Member States and provide legal clarity for companies and users.

Other proposals that will affect data flows include the EU's General Data Protection Regulation (GDPR) that will go into effect on May 25, 2018.[95] The GDPR is intended to unify data protection methods for individuals within the EU and confront issues resulting from the export of personal data outside of the EU. There are remaining concerns about latent ambiguities in the text of the GDPR which suggests that the impact of the bill will be determined by how EU data protection authorities interpret the text. Companies are investing significantly in compliance operations ahead of the May implementation date, with an estimated $7.8 billion spent by Fortune's Global 500 companies to ensure compliance.[96] It is critical that companies are clear about what is required of them under the law and that the GDPR is applied in a consistent manner to all operators in the EU. With legal penalties for noncompliance of key provisions of up to 4% of global operating costs, the stakes for U.S. firms operating in the EU are high.[97]

3. India

Through amendments in 2011 to its Information Technology Act of 2000, India has restricted the transfer of data in cases only "if it is necessary for the performance of the lawful contract" or when the data subject consents to the transfer. However, the necessity requirement is not adequately explained, effectively limiting transfer of data only when consent is given. India has also taken steps to avoid U.S.-based service providers in internal government communications, relying on interpretations of their Public Records Act of 1993. Proposed policies seek to mandate that all employees only use government email services and that agencies host their websites on servers within India, and to restrict use of private services regardless of geographic origin. Indian authorities have contemplated extending localization policies to non-government communications as well, which would require all private data of Indian citizens to be stored on servers within the country and prevent the mirroring of data on

---

[95] Commission Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (l 119) [hereinafter "GDPR"].

[96] IAPP, *Global 500 Companies to Spend $7.8B on GDPR Compliance* (Nov. 20, 2017), https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/.

[97] *GDPR*, *supra* note 95 at art. 83.

servers abroad.[98] While India may be looking to boost domestic investment, reports estimate that India's data localization efforts will lead to a 1.4% decrease in domestic investment.[99]

India's Telecommunications Regulatory Authority of India (TRAI) concluded a consultation on cloud computing in 2017.[100] In their recommendations, they failed to adopt strong prohibitory language on mandated data localization. Rather, they observed that any final view on this subject will have to be taken by the Indian government based on comprehensive review and its impact on the cloud industry. They also suggest the government may soon address many issues in the cloud computing industry by enacting a comprehensive data protection law covering all sectors.

4. Russia

Russia signed localization measures into law in July of 2014, which went into effect on September 1, 2015.[101] The law requires all operators that process the personal data of Russian citizens to maintain databases located in Russia, and to disclose the address of these databases to the Russian telecommunications authority. In August 2015, the Ministry of Communications and Mass Media issued "clarifications" explaining the law's provisions, indicating that the localization requirements will apply to business activities that are "oriented towards" a Russian audience.[102] Despite these clarifications, experts are concerned about the broad language of the rule, which would indicate that all multinational companies with Russian customers must comply as well as the requirements to inform Russia's telecommunications authorities. Further, Russia has yet to issue implementing regulations, creating further uncertainty as to what the rules actually require. The impact on U.S. industry was illustrated when Russia blocked access to

---

[98] Thomas K. Thomas, *National Security Council Proposes 3-pronged Plan to Protect Internet Users*, THE HINDU BUSINESS LINE (Feb. 13, 2014), http://www.thehindubusinessline.com/info-tech/national-security-councilproposes-3pronged-plan-to-protect-internet-users/article5685794.ece.

[99] Matthias Bauer et al., *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, ECIPE Occasional Paper No. 3/2014, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

[100] TELECOM. REG. AUTH.. OF INDIA, Recommendations on Cloud Services at 28 (Aug. 16, 2017), *available at* http://trai.gov.in/sites/default/files/Recommendations_cloud_computing_16082017.pdf ("While on one hand it is often argued that localisation aids the protection of privacy and security of the data, on the other, there is the concern that localisation requirements may 'make it impossible for cloud service providers to take advantage of the Internet's distributed infrastructure').

[101] Paul Sonne, *Russia Steps Up New Law to Control Foreign Internet Companies*, WALL ST. J. (Sept. 24, 2014), http://online.wsj.com/articles/russia-steps-up-new-law-to-control-foreign-internet-companies-1411574920.

[102] Sergei Blagov, *Russia Clarifies Looming Data Localization Law*, BLOOMBERG BNA (Aug. 10, 2015), http://www.bna.com/russia-clarifies-looming-n17179934521/.

LinkedIn in 2016 over perceived violations of the law.[103] Russian authorities continue to make threats to block access to additional websites.[104]

e. Lack of Adequate Competition in Broadband

Inadequate competition in a market for devices or services deters foreign investment and provision of online services, especially in the broadband market. 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.[105]

However, it is also important to recognize that the United States still lacks the necessary 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",[106] the FCC decided to allow incumbent BDS providers, which already control access to these crucial broadband inputs, to indiscriminately hike their rates.

IV. CONCLUSION

Given the importance of Internet services to cross-border trade, CCIA welcomes further study by the ITC on key barriers to digital trade in the B2B and B2C markets.

Respectfully submitted,

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

April 6, 2018

---

[103] Christian Lowe, *U.S. Stays Concerned Over Russia Blocking Access to LinkedIn*, REUTERS (Nov. 18, 2016), http://www.reuters.com/article/us-russia-linkedin-diplomacy/u-s-says-concerned-over-russia-blocking-access-tolinkedin-idUSKBN13D0ST.

[104] *Russia Tells Facebook to Localize User Data or Be Blocked,* REUTERS (Sept. 26, 2017), https://www.reuters.com/article/us-russia-facebook/russia-tells-facebook-to-localize-user-data-or-be-blocked-idUSKCN1C11R5.

[105] *See also* Nitin Rao, *Bandwidth Costs Around the World*, CLOUDFLARE BLOG (Aug. 17, 2016), https://blog.cloudflare.com/bandwidth-costs-around-the-world/.

[106] In the matter of Business Data Services in an Internet Protocol Environment, WC Dkt. No. 16-143 (rel. May 2, 2016) at ¶ 181.