Before the
Office of the United States Trade Representative
Washington, D.C.

In re Request for Public Comments to Compile the National Trade Estimate Report on Foreign Trade Barriers	Docket No. 2017-0013

COMMENTS OF THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION REGARDING FOREIGN TRADE BARRIERS TO U.S. EXPORTS FOR 2018 REPORTING

October 25, 2017

Executive Summary

Pursuant to the request for comments issued by the Office of the United States Trade Representative (USTR) and published in the Federal Register at 82 Fed. Reg. 36,069 (Aug. 2, 2017), the Computer & Communications Industry Association (CCIA) submits the following comments for consideration as USTR composes its annual National Trade Estimate Report on Foreign Trade Barriers (NTE).

CCIA welcomes USTR's deepened focus and renewed commitment to reducing unjustified barriers to digital trade. The Internet is now an integral component to international trade in both services and goods. According to the U.S. International Trade Commission, digital trade added $517.10-$710 billion to U.S. GDP in 2011 alone. However, in recent years countries have begun adopting laws and regulations that hinder the further growth of cross-border delivery of Internet services. Under the guise of promoting domestic innovation, national security, and privacy protections, countries are increasingly adopting discriminatory policies that disadvantage U.S. technology companies in particular and pose significant barriers to cross-border delivery of Internet services. As the Internet continues its exponential growth and becomes even more intertwined with international commerce, it is essential that such barriers are identified and quelled.

CCIA's comments first recommend a strategy forward for U.S. trade policy, including a recommendation to use the ongoing renegotiation of the North American Free Trade Agreement (NAFTA) as an opportunity to create the global model for modern trade agreements. Second, the comments provide a general overview of six key barriers to digital trade: (a) data and infrastructure localization mandates, (b) filtering and blocking, (c) legal liability for online intermediaries, (d) imbalanced copyright and *sui generis* content/link taxes, (e) "backdoor" access to secure technologies, and (f) undue restrictions on "rich interaction applications." Finally, CCIA highlights countries whose current and proposed regimes pose a threat to digital trade and negatively affect foreign investment by U.S. technology companies.

Table of Contents

I. INTRODUCTION

CCIA represents technology products and services providers of all sizes, including computer hardware and software, electronic commerce, telecommunications and Internet products and services. CCIA members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.[1]

CCIA thanks USTR for highlighting digital trade as a key priority for the Administration in the 2017 NTE, and encourages USTR to build upon this work in years to come, given the increasing centrality of digital and Internet technologies to U.S. trade.[2] The United States is a world leader in high-tech innovation and Internet technology — a central component of cross-border trade in both goods and services.[3] The removal of foreign obstacles to Internet-enabled, international commerce and export of Internet-enabled products and services is thus increasingly critical to the growth of the American economy.[4] As the U.S. International Trade Commission (USITC) noted in a 2013 report, "[s]tudies that have quantified the economic contributions of the Internet have generally found that it has made significant contributions to U.S. output,

---

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

[2] *See* Office of the U.S. Trade Rep., *Key Barriers to Digital Trade*, (last modified Mar. 2017), https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade ("In this year's National Trade Estimate (NTE), USTR maintains and deepens its focus on barriers to digital trade.") [hereinafter "*2017 Key Barriers to Digital Trade*"].

[3] In the cloud computing industry alone, 4 U.S.-based companies (Amazon Web Services, Microsoft, IBM, and Google) control more than half of the worldwide cloud computing market. This dominance is projected to grow. For example, Amazon Web Services' third quarter revenue in 2016 jumped from $2.56B to $3.66B during the same period in 2017 - representing a 43% growth. Katherine Noyes, *Four U.S. Companies Rule the World's Cloud Infrastructure*, COMPUTER WORLD (Aug. 1, 2016); Louis Columbus, *Roundup of Cloud Computing Forecasts 2017*, FORBES (Apr. 29, 2017), https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#27db189331e8.

[4] 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/wp-content/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. 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.

employment, consumer welfare, trade, innovation, productivity, and corporate financial performance."[5]

International markets continue to present the most significant growth opportunities for major U.S. companies, even as international competition has grown. In 2014, nine out of the top ten "global Internet properties" were made in the United States, but 79% of their users came from outside the United States.[6] Today, only six of those leading brands are U.S.-based,[7] vying for some 3.7 billion Internet users across the world.[8] Last year, China overtook the United States as the largest market in the world for the iOS App Store revenue, earning 15% more than the United States over the third quarter of 2016.[9]

These changing dynamics are not only driven by competitive market forces. Countries recognize the immense value that a strong digital industry contributes to the national economy, and with the predominance of U.S. companies in this sector, governments are increasingly adopting policies designed to favor domestic innovation and specifically target U.S. companies ushering in a new form of discrimination.[10]

---

[5] U.S. Int'l Trade Comm'n, *Digital Trade in the U.S. and Global Economies, Part 1* (July 2013), http://www.usitc.gov/publications/332/pub4415.pdf.

[6] Mary Meeker, *Internet Trends 2014*, at 130 (2014), http://www.kpcb.com/blog/2014-internet-trends. By way of specific example, Google's total international revenue was 39% of its overall sales in 2005, whereas in 2017 52% of its revenue comes from outside the United States. *Compare* Press Release, Google, *Google Announces Fourth Quarter and Fiscal Year 2005 Results* (Jan. 31, 2006), https://investor.google.com/earnings/2005/Q4_google_earnings.html *with* Press Release, Alphabet, *Alphabet Announces Second Quarter 2017 Results* (July 24, 2017), https://abc.xyz/investor/news/earnings/2017/Q2_alphabet_earnings/. Similarly, 86.3% of Facebook's daily active users lie outside of the U.S. and Canada, while fewer than 50% of Facebook users were international in 2008. *Compare* Facebook Q2 2017 Results, https://s21.q4cdn.com/399680738/files/doc_presentations/FB-Q2'17-Earnings-Presentation.pdf *with* Miguel Helft, *Facebook Makes Headway Around the World*, N.Y. TIMES (July 7, 2010), http://www.nytimes.com/2010/07/08/technology/companies/08facebook.html.

[7] Mary Meeker, *Internet Trends 2016*, at 187 (2016), http://www.kpcb.com/blog/2016-internet-trends-report.

[8] *Internet Live Stats*, http://www.internetlivestats.com/internet-users/ (last visited Oct. 3, 2017).

[9] Sarah Perez, *China Overtakes the U.S. in App Store Revenue*, TECHCRUNCH (Oct. 20, 2016), https://techcrunch.com/2016/10/20/china-overtakes-the-u-s-in-ios-app-store-revenue/ (referencing Lexi Snow, *Q3 2016 Index: China Hits an iOS App Store Milestone*, APP ANNIE (Oct. 20, 2016), https://www.appannie.com/insights/market-data/q3-2016-index-china-hits-ios-app-store-milestone/).

[10] WORLD ECONOMIC FORUM, *Internet Fragmentation: An Overview* at 35-36 (2016), http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf [hereinafter *"Internet Fragmentation"*] ("[G]overnments are often tempted to play for time and pursue approaches that preference national/regional players and digital spaces, including by restraining first-moving companies from abroad. In this

The United States must retain its global dominance in technology products and services and continue to drive innovation at home and abroad. The Administration has committed itself to revitalizing American trade and prioritizing U.S. industries, the vast majority of which create, provide, or rely on Internet technologies. To fully realize this goal, the United States must develop a trade agenda and craft agreements that will reflect our global digital economy and set the stage for all future trade agreements.

U.S. trade policies and priorities have not sufficiently adapted to reflect the importance of Internet-enabled trade to the U.S. economy. While trade policy has dramatically reduced barriers to trade in goods, the United States is gradually becoming a services economy, with service industries employing a large majority of U.S. private-sector workers, and digital services increasingly integrated into manufacturing, agriculture, and other traditional U.S. sectors.[11] Meanwhile, the United States is the largest global exporter of services, exporting $733 billion in 2016.[12] The Internet has been the single biggest component of the cross-border trade in services, with many of those services facilitating the international goods trade as well. The U.S. trade agenda should recognize these trends and commit to removing barriers in the delivery of such services.

The renegotiation of the North American Free Trade Agreement (NAFTA) — first negotiated in the infancy of the commercial Internet — is a key opportunity to incorporate provisions focused on liberalizing digital trade and enabling innovation in the agreement. While NAFTA has been a net economic success for the United States,[13] a modern overhaul is much

---

context, the predominance of US technology companies in key market segments has led some governments to consider or adopt laws and regulatory practices that hinder certain kinds of operations and transactions or block the use of particular tools, be it social networking platforms or cross-border delivery via 3D printing.").

[11] BUREAU OF LABOR STATISTICS, Current Employment Statistics, Employees on Nonfarm Payrolls by Industry Sector (last modified Oct. 6, 2017), http://www.bls.gov/web/empsit/ceseeb1a.htm.

[12] WORLD TRADE ORGANIZATION, *World Trade Statistical Review*, at 104 (2017), https://www.wto.org/english/res_e/statis_e/wts2017_e/wts2017_e.pdf. *Compare* WORLD TRADE ORGANIZATION, International Trade Statistics 2015, at 46 (2015), https://www.wto.org/english/res_e/statis_e/its2015_e/its2015_e.pdf (noting that the U.S. exported $688 billion in 2014).

[13] U.S. CHAMBER OF COMMERCE, *NAFTA Works for America*, https://www.uschamber.com/nafta-works (last visited Oct. 11, 2017) (noting that trade with Canada and Mexico supports 14 million American jobs and nearly 4 million of those jobs are supported by the increase in trade generated by NAFTA); Amanda Waldron, *NAFTA*

needed for the 23-year-old agreement to factor in the growth of the digital economy. As outlined in our comments below, this includes commitments from the three parties to (1) protect the free flow of data across borders and (2) maintain balanced copyright and protections for online intermediaries. CCIA applauds USTR for including cross-border data flows in the stated NAFTA objectives, calling for "rules to ensure that NAFTA countries do not impose measures that restrict cross-border data flows and do not require the use or installation of local computing facilities."[14] However, to fulfill its commitment to growing the Internet sector and remain compliant with international commitments, USTR must also commit to upholding and promoting U.S. rules on balanced copyright in NAFTA. Carefully tailored protections for intermediaries and balanced copyright law are equally as important as open data flows to the continued growth of the digital economy, building off a record of success since their first inclusion in free trade agreements nearly 15 years ago. Copyright balance is a critical aspect of digital trade and should be incorporated into the Administration's trade policy.

Modernizing U.S. trade policy also calls for maintaining and expanding the NTE Report's focus on digital trade barriers. CCIA commends USTR for doing so in the 2017 NTE Report[15] and hopes that USTR will continue to highlight digital trade barriers in the 2018 Report.

II. PROMINENT DIGITAL TRADE-RELATED BARRIERS

A. Data and Infrastructure Localization Mandates

As CCIA has noted in previous NTE filings,[16] a number of countries continue to pursue data localization policies, including mandated server localization and data storage.[17] In a 2017

Renegotiation: Separating Fact From Fiction, BROOKINGS (Aug. 17, 2017) ("NAFTA has allowed U.S. companies to access new markets for their exports, reduce their costs of production, and create even more jobs.").

[14] Office of the U.S. Trade Rep., Summary of Objectives for the NAFTA Renegotiation, at 8-9 (July 17, 2017), https://ustr.gov/sites/default/files/files/Press/Releases/NAFTAObjectives.pdf.

[15] *See 2017 Key Barriers to Digital Trade*, *supra* note 2 ("In this year's National Trade Estimate (NTE), USTR maintains and deepens its focus on barriers to digital trade.").

[16] Comments of the Computer & Commc'ns Indus. Ass'n, *In re Request for Public Comments To Compile the National Trade Estimate Report on Foreign Trade Barriers*, Dkt. No. 2016-0007, filed Oct. 26, 2016, *available at* http://www.ccianet.org/wp-content/uploads/2016/10/CCIA-Comments-for-2017-NTE.pdf [hereinafter "CCIA NTE Comments 2016"]; Comments of the Computer & Commc'ns Indus. Ass'n, *In re Request for Public Comments To Compile the National Trade Estimate Report on Foreign Trade Barriers*, Docket No. 2015-0014, filed Oct. 28, 2015, *available at* http://www.ccianet.org/wp-content/uploads/2015/10/CCIA-NTE-2016.pdf.

report, the ITC included estimates that such localization measures have doubled in the last six years.[18] Citing domestic privacy protections, defense against foreign espionage, law enforcement needs, and the promotion of local economic development, foreign governments are considering these policies at an increasing rate. While rarely the stated intention, in practice many of these policies effectively keep foreign competitors out of their markets.

Political motivations aside, data localization requirements in fact tend to undermine their stated goals. 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.[19] 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.[20] 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.[21] Rather than promote domestic industry, data localization policies are likely to hinder economic development,[22] restrict domestic economic activity,[23] and impede

---

[17] A recent study by the Information Technology & Innovation Foundation listed of most of the word's formal data localization policies identifying over 30 countries that have enacted such policies as of April 2017. *See* Nigel Cory, *Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?,* INFORMATION TECHNOLOGY & INNOVATION FOUNDATION at 20 (May 2017), http://www2.itif.org/2017-cross-border-data-flows.pdf. *See also* Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Information* at 6 (Sept. 2015), http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20%20September%202015.pdf.

[18] U.S. Int'l Trade Comm'n, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, at 16 (Aug. 2017), https://www.usitc.gov/publications/332/pub4716.pdf [hereinafter "*2017 Global Digital Trade 1"*].

[19] 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.

[20] 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.

[21] 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.

[22] *See* Leviathan Security Group, *Quantifying the Costs of Forced Localization* (2015), http://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/

global competitiveness.[24] Data localization policies may also be in violation of international obligations. 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.[25] 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.[26]

B. Filtering and Blocking

Perhaps the most apparent barriers to digital trade are the outright filtering and blocking of U.S. Internet platforms and online content, with one recent study finding that countries lose $23.6 million (per 10 million in population) for every day that the Internet is shut down.[27] Despite these costs, governments continue to filter and block Internet content, platforms, and

---

Quantifying+the+Cost+of+Forced+Localization.pdf (finding that "local companies would be required to pay 30-60% more for their computing needs than if they could go outside their country's borders).

[23] Matthias Bauer *et al*., *The Costs of Data Localization: Friendly Fire on Economic Recovery*, ECIPE (2014), http://www.ecipe.org/media/publication_pdfs/OCC32014__1.pdf.

[24] For example, foreign investment will likely decline. Given the high cost of constructing data centers, many companies will simply opt out of serving markets with onerous data localization requirements, especially small- and medium-sized businesses. In 2013, the average cost of data centers in Brazil and Chile were $60.3 million and $43 million, respectively. Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill Push for Data Localization*, WALL ST. J. (Nov. 13, 2013), http://online.wsj.com/articles/SB10001424052702304868404579194290325348688. *See also* U.N. Conference on Trade and Development, *Data Protection Regulations and International Data Flows* at 3, (2016), http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ("[I]f data protection regulations go 'too far' they may have a negative impact on trade, innovation and competition."); *ITIF supra* note 4 at 6-7 ("At the firm level, barriers to data flows make firms less competitive, as a company will be forced to spend more than necessary on IT services. Companies will likely have to pay more for data-storage services, especially those in smaller countries (which will not naturally be home to a data center). Such barriers also prevent companies from transferring data that's needed for day-to-day activities, such as for human resources, which means companies may have to pay for duplicative services.").

[25] 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).

[26] *See* Chander & Lê, *Data Nationalism*, *supra* note 19; U.S. Int'l Trade Comm'n, *Digital Trade in the U.S. and Global Economies, Part 2* (2014), http://www.usitc.gov/publications/332/pub4485.pdf [hereinafter "*2014 Digital Trade in the U.S. and Global Economies, Part 2"*].

[27] DELOITTE, *The Economic Impact of Disruptions to Internet Connectivity, A Report for Facebook,* at 6 (Oct. 2016), http://globalnetworkinitiative.org/sites/default/files/The-Economic-Impact-of-Disruptions-to-Internet-Connectivity-Deloitte.pdf.

services for various reasons. For example, as discussed further below, the services of many U.S. Internet platforms are either blocked or severely restricted in the world's largest online market: China. In its 2016 report, Freedom House assessed that global Internet freedom declined for the sixth consecutive year due to growing online censorship and monitoring practices.[28] It also reported that since June 2015, 34 out of the 65 countries assessed in the report have been on a negative trajectory,[29] increasing political censorship, prosecutions for speech, and surveillance. The same report observed a new key trend where governments are increasingly targeting messaging and voice communications apps, while others are cracking down on users expressing political views on social media.[30] Whether deliberate or not, these practices clearly have trade-distorting effects well beyond the services directly involved. When a social media or video platform is blocked, it is not only harmful to the service and users in question, but it also immediately affects content providers, advertisers, and small businesses using the service to find and interact with new and existing customers. A recent Brookings Institution estimate pegged the global loss of intermittent blackouts at no less than $2.4 billion in one year.[31] Such blocking is likely to violate international commitments, such as the World Trade Organization's rules on market access and national treatment.

Methods of filtering and blocking generally consist of (a) legal or regulatory obligations imposed upon intermediary services, (b) network-level blocking and/or filtering achieved through state control of or influence over communications infrastructure, or (c) technology mandates that either hobble user privacy and security, or that force product manufacturers to include intrusive monitoring technology.[32] Known offenders who use some or all of these

---

[28] FREEDOM HOUSE, *Freedom on the Net 2016: Silencing the Messenger: Communication Apps Under Pressure* (2016), https://freedomhouse.org/sites/default/files/FOTN_2016_BOOKLET_FINAL.pdf [hereinafter "*Freedom House 2016"*].

[29] *Id*. at 2.

[30] *Id*. at 1 ("Using in some countries were put behind bar for simply 'liking' offending material on Facebook, or for not denouncing critical messages sent to them by others. . .The number of countries where such arrests occur has increased by over 50 % since 2013.").

[31] Darrell M. West, *Global Economy Loses Billions from Internet Shutdowns*, BROOKINGS INSTITUTION (Oct. 6, 2016), https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf [hereinafter Darrell M. West, *Internet Shutdowns*].

[32] *Internet Fragmentation*, *supra* note 10.

practices include Afghanistan, Burma, China, Cuba, Egypt, Guatemala, Indonesia, Iran, Kazakhstan, North Korea, Pakistan, Saudi Arabia, Syria, Tunisia, Turkey, Turkmenistan, Uzbekistan, and Vietnam.[33] States are often disinclined to explain or justify blocking Internet content, and in many cases restrictions are not developed in a transparent manner. This lack of clarity is sometimes used against foreign firms to the advantage of domestic ones.[34]

A similar barrier to cross-border data flows is gateway filtering. When countries operate national firewalls, all foreign websites and services must pass through "gateways." Domestic Internet content, however, does not pass through the gateways to reach its own domestic market. This has the effect of systemically affecting the speed and quality of service of foreign websites and services vis-à-vis domestic Internet content.[35]

As CCIA has previously stated, U.S. trade policy should ensure that insofar as any filtering or blocking is conducted against online content, policies are applied equally to both domestic and foreign websites. Furthermore, such restrictions must comply with WTO principles of transparency, necessity, being as minimally restrictive as possible, and the provision of due process to affected parties.

C. Legal Liability for Online Intermediaries

Foreign countries have frequently imposed substantial penalties on U.S. Internet companies for conduct of third parties — something that is not permitted under U.S. law and that impedes the ability of U.S. online services to be a platform for trade.[36] U.S. firms operating as online intermediaries face an increasingly hostile environment in a variety of international markets which impedes U.S. Internet companies from expanding services abroad. This hurts not only Internet companies, but also denies local small and medium-sized enterprises Internet-enabled access to the global marketplace, similarly discouraging investment in and growth of

---

[33] Darrell M. West, *Internet Shutdowns*, *supra* note 31; *Freedom House 2016 supra* note 28.

[34] *2014 Digital Trade in the U.S. and Global Economies, Part 2*, *supra* note 26, at 98.

[35] *See* Paul Mozur & Carlos Tejada, *China's 'Wall' Hits Business*, WALL ST. J. (Feb. 13, 2013), http://online.wsj.com/articles/SB10001424127887323926104578277511385052752.

[36] *See generally* Ali Sternburg & Matt Schruers, *Modernizing Liability Rules to Promote Internet Trade*, CCIA (2013), http://cdn.ccianet.org/wp-content/uploads/2013/09/CCIA-Liability-Rules-Paper.pdf.

domestic startups.[37] While U.S. Internet businesses have thrived domestically under carefully crafted legal frameworks, international asymmetries in liability rules frequently favor domestic plaintiffs.[38]

The United States must utilize trade agreements in order to rectify the barriers these legal asymmetries create. Requiring U.S. trading partners to implement analogous intermediary protections has been a central U.S. trade policy for well over a decade, a policy aimed at enabling the export of U.S. online services by preventing other countries from imposing crippling liability on these services. However, a concerning trend among U.S. trading partners is a failure to fully implement carefully negotiated intermediary protections in the context of copyright liability, as discussed in the next section.[39]

D. Imbalanced Copyright and *Sui Generis* Context/Link Taxes

Balanced copyright rules such as fair use and related limitations and exceptions have been critical to the growth of the U.S. technology and Internet economy.[40] They are also a defining aspect of U.S. trade policy. Beginning with free trade agreements with Chile and Singapore in 2003, every modern U.S. trade agreement has ensured some measure of copyright balance, at least through the inclusion of intermediary protections.[41] USTR also stated this year

---

[37] 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.

[38] For a general overview of these issues, *see* Ignacio Garrote Fernández-Díez, *Comparative Analysis on National Approaches to the Liability of Internet Intermediaries for Infringement of Copyright and Related Rights*, http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries_garrote.pdf (comparative analysis on national approaches to the liability of Internet intermediaries for infringement of copyright and related rights).

[39] CCIA has further expanded on this issue in other forums. *See* Comments of CCIA, *In re* 2017 Special 301 Review, Dkt. No. USTR-2016-0026, filed Feb. 9, 2017 [hereinafter "*2017 CCIA Special 301 Comments*"].

[40] In 2014, fair use industries accounted for 16 % of the economy, employed 1 in 8 workers, and contributed $2.8 trillion to the GDP. Exports of goods and services related to fair use increased by 21 percent from $304 billion in 2010 to $368 billion in 2014 driven by increases in service-sector exports. COMPUTER & COMM'NS INDUS. ASS'N., *Fair Use in the U.S. Economy* (2017), *available at* http://www.ccianet.org/wp-content/uploads/2017/06/Fair-Use-in-the-U.S.-Economy-2017.pdf.

[41] *See* U.S-Austl. Free Trade Agreement, May 18, 2004, 43 I.L.M. 1248, art. 17.11, para. 29; U.S.-Bahr. Free Trade Agreement, Dec. 7, 2005, 44 I.L.M. 544, art. 14.10, para. 29; U.S.-Chile Free Trade Agreement, June 6, 2003, 42 I.L.M. 1026, art. 17.11, para. 23; U.S.-Colom. Free Trade Agreement, Nov. 22, 2006, art. 16.11, para. 29; U.S.-S. Kor. Free Trade Agreement, June. 30, 2007, art. 18.10, para. 30; U.S.-Morocco Free Trade Agreement, June 15,

its commitment to seek "the commitment of our free trade agreement partners to continuously seek to achieve an appropriate balance in their copyright systems, including through copyright exceptions and limitations."[42]

Within the last thirty years, such rules have enabled the development of innovative new products and services such as the VCR, DVR, iPod, cloud computing, search engines, social media services, and 3D printing. Similarly, users of copyrighted works — including consumers, libraries, museums, reporters, and creators — depend upon concepts like fair use and other limitations and exceptions to engage in research, reporting, parody, and political discourse.

These innovations are jeopardized by weak or nonexistent limitations and exceptions in the copyright laws of other countries.[43] While many of the countries outlined below and discussed in prior NTE Reports either have adopted or proposed strong copyright enforcement rules, few of these countries have implemented U.S.-style fair use or other flexible copyright limitations and exceptions. Such exceptions are necessary to enable U.S. innovation abroad.

Some countries are going further and creating new rights. For example, as the 2017 NTE described (discussed *infra* pp. 28), legislatures in Europe and elsewhere have increasingly 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, raise concerns from a trade perspective.[44] A recent USITC report also

---

2004, art. 15.11, para. 28; U.S.-Oman Free Trade Agreement, Jan. 19, 2006, art. 15.10, para. 29; U.S.-Pan. Trade Promotion Agreement, June 28, 2007, art. 15.11, para. 27; U.S.-Sing. Free Trade Agreement, May 6, 2003, 42 I.L.M. 1026, art. 16.9, para. 22.

[42] OFFICE OF U.S. TRADE REP., *The Digital 2 Dozen* (2017), *available at* https://ustr.gov/sites/default/files/Digital-2-Dozen-Updated.pdf.

[43] This is exacerbated when the U.S. trade agenda does not include commitments to upholding long-standing limitations and exceptions to copyright around the world. *See* Jonathan Band, *Keeping the DMCA's Grand Bargain in NAFTA*, DISRUPTIVE COMPETITION PROJECT (Oct. 2, 2017), http://www.project-disco.org/intellectual-property/100217-keeping-dmcas-grand-bargain-nafta/ ("The balanced structure of the DMCA has been reflected in our trade agreements for the purpose of benefitting the overseas operations of both the content industry and the service providers. Precisely because the free trade agreements embodied the DMCA's evenhanded approach, USTR negotiated the copyright sections of these agreements with relatively little domestic controversy. Now, however, the content providers seek to depart from this framework in NAFTA; they hope to achieve the DMCA's benefit—the TPM provisions—without the tradeoff they have agreed to repeatedly since 1998.").

[44] 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 [hereinafter "*2017 NTE"*].

observed that these laws tend to have "generated unintended consequences" to small online publishers.[45] Service providers of online search, news aggregation, and social media platforms are compelled to pay for the "privilege" of quoting from news publications. This proposal is often referred to as a "snippet tax." It is also at times formally described as "ancillary copyright" in that it is allegedly an "ancillary" IP right — yet it is in fact inconsistent with international IP law, violates international trade obligations, and constitutes a TRIPS-violating barrier to trade. While only the European Union is seriously contemplating ancillary/neighboring rights protection at the moment, other jurisdictions have at times considered such proposals. This issue is discussed in greater detail below, in the European Union section (discussed *infra* pp. 28).

As identified above, countries frequently impose penalties on U.S. Internet companies for the conduct of third parties. This is especially true in the context of copyright enforcement. Countries are increasingly using outdated Internet service liability laws that impose substantial penalties. These practices deter investment and market entry, impeding legitimate online services. Countries that have imposed copyright liability on online intermediaries contrary to the laws of the United States include France, Germany, India, Italy, and Vietnam.[46] Another concerning trend is the failure of current U.S. trading partners to fully implement carefully negotiated intermediary protections in free trade agreements. This is illustrated by Australia and Colombia's lack of compliance (discussed *infra* pp. 17 and pp. 27). USTR has highlighted failures to comply with trading obligations and inadequate intermediary liability protections in past Special 301 Reports, indicating the importance of such projections to trade relations.[47]

---

[45] *2017 Global Digital Trade I*, *supra* note 18, at 291-92 ("Small online publishers have been reluctant to demand fees from online platforms because they rely on traffic from those search engines, and industry experts have stated that ancillary copyright laws have not generated increased fees to publishers; rather, they have acted as a barrier to entry for news aggregators.").

[46] Rachel F. Fefer, et al, *Digital Trade and U.S. Trade Policy*, CONGRESSIONAL RESEARCH SERVICE, at 17 (Jun. 6, 2017), https://fas.org/sgp/crs/misc/R44565.pdf.

[47] OFFICE OF THE U.S. TRADE REP., 2009 Special 301 Report (2009) (watching Chile for failing to implement provisions of the FTA regarding Internet service provider liability); OFFICE OF THE U.S. TRADE REP., 2016 Special 301 Report, at 47 (2016) (watch listing Ukraine, which has no specific intermediary liability FTA commitment as being based in part upon the "lack of transparent and predictable provisions on intermediary liability").

E. "Backdoor" Access to Secure Technologies

Providers of digital devices and services have for many years sought to improve the security of their platforms through the deployment of technologies that safeguard the communications and commercial transactions that they enable. Strong encryption has been increasingly enabled on now-ubiquitous smartphones and deployed end-to-end on consumer-grade communications services and browsers. Encrypted devices and connections protect users' sensitive personal and financial information from bad actors who might attempt exploit that information.[48]

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 United Kingdom, France, Germany, Australia,[49] Brazil, India, and China.[50] Russia has already imposed this requirement on companies operating in its jurisdiction through its "Yarovaya" laws.[51]

These exceptional access regimes run contrary to the consensus assessments of security technologists because they are technically and economically infeasible to develop and

---

[48] Bijan Madhani, *Blast from the Past: Learning Lessons from Previous Panics Over Ubiquitous Strong Encryption*, DISRUPTIVE COMPETITION PROJECT (Sept. 10, 2015), http://www.project-disco.org/privacy/091015-blast-from-the-past-learning-lessons-from-previous-panics-over-ubiquitous-strong-encryption/.

[49] Australia also pushed this past summer for a joint measure to expand powers to weaken encryption at a meeting of ministers from the "Five Eyes" intelligence network of the U.S., U.K, Canada, Australia, and New Zealand. *Australia to Seek Greater Powers on Encrypted Messaging at 'Five Eyes' Meeting*, REUTERS (June 25, 2017), https://www.reuters.com/article/us-australia-security-messaging/australia-to-seek-greater-powers-on-encrypted-messaging-at-five-eyes-meeting-idUSKBN19G044.

[50] Kevin Collier, *The Countries That Are Considering Banning Encryption*, VOCATIV (Apr. 11, 2016), http://www.vocativ.com/307667/encryption-law-europe-asia/; Jeremy Malcom, *Australian PM Calls for End-to-End Encryption*, ELECTRONIC FRONTIER FOUNDATION (July 14, 2017), https://www.eff.org/deeplinks/2017/07/australian-pm-calls-end-end-encryption-ban-says-laws-mathematics-dont-apply-down.

[51] Alec Luhn, *Russia Passes 'Big Brother' Anti-terror Laws*, THE GUARDIAN (June 26, 2016), https://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother-anti-terror-laws.

implement.[52] Companies already operating in countries that have or are considering anti-encryption laws will be required to alter global platforms or design region-specific devices, or face fines and shutdowns for noncompliance. Companies that might have otherwise expanded to these markets will likely find the anti-encryption requirements to be barriers to entry. The United States should recognize these concerns and address them in future trade agreements, incorporating provisions that prevent countries from compelling manufacturers or suppliers to use a particular cryptographic algorithm or to provide access to a technology, private key, algorithm, or other cryptographic design details.[53]

F. Undue Restrictions on "Rich Interaction Applications"

Several countries have proposed or implemented undue or unreasonable regulatory restrictions on rich interaction applications (RIAs)[54] — a term that refers to applications that facilitate "rich interaction" such as photo/video sharing, money transferring, in-app gaming, location sharing, translation, and chat among individuals, groups and enterprises.[55] However, a recent study has shown the vast economic and societal benefits from RIAs.[56] Global GDP has increased $5.6 trillion for every 10% increase in the usage of RIAs across 164 countries over 16

---

[52] Harold Abelson, *et al.*, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY TECHNICAL REPORT (July 6, 2015), http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[53] Bijan Madhani, *Digital Issues in NAFTA: Cross-Border Data Flows and Cybersecurity*, DISRUPTIVE COMPETITION PROJECT (June 15, 2017), http://www.project-disco.org/21st-century-trade/061517-digital-issues-in-nafta-cross-border-data-flows-and-cybersecurity/.

[54] *See NTA Bans 'Viber Out' Service in Nepal*, THE HIMALAYAN TIMES (Sept. 26, 2017), https://thehimalayantimes.com/business/nepal-telecommunications-authority-bans-viber-out-service-nepal; *En 15 días estará la ley sobre las aplicaciones*, EL PAIS (Feb. 24, 2016), http://www.elpais.com.uy/informacion/dias-estara-ley-aplicaciones.html; Saad Guerraoui, Morocco Banned Skype, Viber, WhatsApp and Facebook Messenger. It Didn't Go Down Well, MIDDLE EAST EYE (Mar. 9, 2016), http://www.middleeasteye.net/columns/boycotts-appeals-petitions-restore-blocked-voip-calls-morocco-1520817507; Letter from Hans W. Vriens, Secretariat - Asia Internet Coalition to Ministry of Information & Communications (Jan. 6, 2015), *available at* https://www.aicasia.org/wp-content/uploads/2015/01/AIC-comments-on-OTT-Circular-2015-01-06_EN.pdf.

[55] The term RIA is distinguished from the commonly used phrase "over-the-top" services. The term OTT originates in the telecommunications industry and broadly describes *any* application or service traveling across telecommunications infrastructure.

[56] Dr. René Arnold et al., *The Economic and Societal Value of Rich Interaction Applications (RIAs)*, WIK WISSENSCHAFTLICHES INSTITUT FÜR INFRASTRUKTUR UND KOMMUNIKATIONSDIENSTE GMBH (May 2017), *available at* http://www.wik.org/index.php?id=879&L=1 [hereinafter "*RIA Study*"].

years (2000 to 2015).[57] USTR should encourage countries that may be considering imposing antiquated regulations on these emerging services to instead promote policies that encourage greater growth and competition in ICT services. For example, Kenya, in its draft national ICT policy, acknowledges the contribution of RIAs to the economy.[58] Instead of raising regulatory barriers, Kenya has attempted to promote RIAs and other Internet-enabled services and to encourage telecommunication operators to evolve their business models. Maintaining a clear, regulatory distinction between information services and telecommunication services has been critical to the development of Internet services and applications in the United States and elsewhere. Governments should recognize that RIAs can offer societal benefits to them and their citizens by ensuring closer links, so governments can be more responsive to the needs of the citizenry. RIAs help governments respond to emergencies and public health crises more quickly and accurately; they can also improve enterprise and government efficiency through Smart Cities initiatives.

Online services help drive growth in some of the most profitable services offered by telecommunication providers.[59] Indeed, RIA use has a substantial, positive impact on telecommunication providers' businesses, giving them more opportunities to earn revenue and finance new infrastructure because RIAs drive demand for connectivity. As RIAs develop and become more popular, consumers will want to spend more time online and subscribe to telecommunication services – increasingly mobile services but also fixed broadband.[60] For example, video and music streaming services require more bandwidth and better connections, so heavy users of such services and RIAs "are more likely to have upgraded their mobile and fixed [Interest access services] subscriptions within the last two years."[61] In addition, online services

---

[57] *Id.*

[58] *National Information & Communications Policy, 2016*, Ministry of Information & Communications Technology, para 18.5 p 44, http://icta.go.ke/pdf/National-ICT-Policy-20June2016.pdf.

[59] *See* OECD, *The Development of Fixed Broadband Networks* (Jan. 2015), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP%282013%298/FINAL&docLanguage=En (noting that "pricing mechanisms that do not excessively depress demand have the advantage of stimulating adoption").

[60] *RIA Study*, *supra* note 56, at 19.

[61] *Id*.

also present cost-saving and product-enhancement opportunities for telecommunication providers, such as the opportunity to substitute fully featured VoIP for circuit-switched voice.

III. COUNTRY-SPECIFIC CONSIDERATIONS

What follows is a non-exhaustive list highlighting a few examples of potentially trade-restrictive localization policies or policy proposals:

A. Australia

Legal Liability for Online Intermediaries

Failing to implement obligations under trade agreements represents a barrier to trade. The U.S.-Australia Free Trade Agreement[62] contains an obligation to provide liability limitations for service providers, analogous to 17 U.S.C. § 512. However, Australia has failed to fully implement such obligations and current implementations are far narrower than what is required. Australia's statute limits protection to what it refers to as "carriage" service providers, not service providers generally.[63] The consequence of this limitation is that intermediary protection is largely limited to Australia's domestic broadband providers. Online service providers engaged in the export of information services into the Australian market remain in a precarious legal situation. This unduly narrow construction violates Australia's trade obligations under Article 17.11.29 of the FTA. This article makes clear that the protections envisioned should be available to all online service providers, not merely carriage service providers. Although Australian authorities documented this implementation flaw years ago, no legislation has been enacted to remedy it.[64] This oversight was set to be addressed by passage of new amendments to Australia's Copyright Act, however, the intermediary liability protections were dropped from the final bill passed in June.[65]

---

[62] U.S.-Austl. Free Trade Agreement, May 18, 2004, 43 I.L.M. 1248.

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

[64] Australian Attorney-General's Department, Consultation Paper: Revising the Scope of the Copyright Safe Harbour Scheme (2011), https://www.ag.gov.au/Consultations/Documents/Revising+the+Scope+of+the+Copyright+Safe+Harbour+Scheme.pdf.

[65] Copyright Amendment (Disability Access and Other Measures) Bill 2017. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5832

B. Brazil

Over time, Brazilian policymakers have implemented policies which prevented innovation and technological progress. These policies place many restrictions on international trade, including, for example: (a) through government procurement preferences and preferable margins for local information and communications technology goods and equipment,[66] (b) Brazil's Presidential Decree 8135, which requires federal agencies to procure e-mail, file sharing, teleconferencing and VoIP services from Brazilian federal public entities,[67] or (c) the CERTICS Decree implemented to check whether software programs are the result of Brazilian innovation.[68] Brazil is also home to various local content requirements, filtering obligations, and tax incentives for locally-sourced ICT goods. These policies have prevented innovation and technological progress, and constitute unlawful barriers to trade. Urging Brazil to repeal these measures, in addition to addressing the issues outlined below, will help increase international trade of information and communications technology goods and equipment, allowing more U.S. tech companies to do business in Brazil.

Filtering & Blocking

In February 2015, municipal judge Luiz de Moura Correia in the state of Piauí ordered ISPs to block access to the Internet application WhatsApp in order to force WhatsApp to cooperate with local police in an investigation.[69] This order was issued in relation to the Brazilian "Marco Civil," which "authorizes a series of punishments that can be ordered against companies that do not comply with various regulations. . . Judge Correia's order selected the most severe of these sanctions, and interpreted it as authorizing censorship orders to ISPs."[70]

---

[66] LIBRARY OF CONGRESS, *Government Procurement Law and Policy: Brazil*, https://www.loc.gov/law/help/govt-procurement-law/brazil.php (last visited Oct. 10, 2017).

[67] Jefferson Ribeiro, *Bill Would Allow Brazil to Decree Local Internet Data Storage*, REUTERS (Nov. 5, 2013), http://www.reuters.com/article/net-us-brazil-internet-idUSBRE9A30SI20131105.

[68] *Certificate of Technology and Innovation in Brazil*, CERTICS, http://www.certics.cti.gov.br/?page_id=7&lang=en (last visited Oct. 10, 2017).

[69] Jonathan Watts, *Judge Lifts WhatsApp Ban in Brazil After Ruling Block Punished Users Unfairly,* THE GUARDIAN (Dec. 17, 2015), https://www.theguardian.com/world/2015/dec/17/brazil-whatsapp-ban-lifted-facebook.

[70] Danny O'Brien & Katitza Rodriguez, *You Can't Block Apps on the Free and Open Brazilian Internet*, ELECTRONIC FRONTIER FOUNDATION (Mar. 2, 2015), https://www.eff.org/deeplinks/2015/03/you-cant-block-apps-free-and-open-brazilian-internet.

Fortunately, the decision was reversed by an appellate court, citing the disproportionate impact caused by shutting down the whole service over a local investigation.[71] WhatsApp was blocked for the third time in eight months in July of 2016, but the ban was once again overturned for the same reasons listed above.[72] Nevertheless, the May 2016 WhatsApp ban cost the Brazilian economy an estimated $39 million in just one day.[73] The Supreme Court of Brazil held public hearings on June 2 of this year to further address the issue of banning secure communications technologies.[74] Because these interruptions impose corresponding costs on U.S. service exporters, the prospect of blocking content or services — as opposed to other legal avenues (such as MLATs) for securing compliance with court orders — should concern USTR.

De Minimis Threshold

Brazil's de minimis threshold for duty-free importation remains at USD $50, which is applicable only to consumer-to-consumer transactions, and does not apply to business-to-consumer or business-to-business transactions.[75] The differential treatment and low de minimis threshold for consumer-to-consumer transactions create barriers to international trade by increasing transaction costs for Brazilian businesses while limiting consumer choice and competition amongst Brazilian businesses. Extending the de minimis threshold to business-to-consumer and business-to-business transactions and raising the de minimis threshold would help Brazil conform with international consumer standards and shopping behaviors.

B. Canada

Data Localization

The Canadian federal government has endeavored to consolidate information and communications technology services across dozens of Canadian federal entities into a single

---

[71] Watts, *supra* note 69.

[72] *Id*.

[73] Darrell M. West, *Internet Shutdowns*, *supra* note 31, at 9.

[74] Javier Pallero, *Supreme Court of Brazil Holds Hearings on Blocking Apps*, ACCESS NOW (June 7, 2017), https://www.accessnow.org/supreme-court-brazil-holds-hearings-blocking-apps/; Angelica Mari, *WhatsApp Executives Come to Brazil to Avoid New Bans,* ZDNET (June 5, 2017), http://www.zdnet.com/article/whatsapp-executives-come-to-brazil-to-avoid-new-bans/.

[75] *Overview of De Minimis Value Regimes Open to Express Shipments World Wide*, GLOBAL EXPRESS ASSOCIATION (Apr. 2016), http://www.global-express.org/assets/files/Customs%20Committee/de-minimis/GEA-overview-on-de-minimis_April-2016.pdf.

central agency called "Shared Services Canada."[76] For reasons of privacy and national security, U.S. and foreign cloud computing suppliers are precluded from participating in government procurement processes for systems containing personal or sensitive information, unless the data will be stored on servers physically located in Canada.[77] As the public sector represents approximately one third of the Canadian economy and is a major consumer of U.S. services in the information and communications technology sector, this initiative should concern USTR.

De Minimis Threshold

Canada has one of the world's lowest de minimis thresholds for goods coming across the border at $20 CAD — a threshold that has not been adjusted since the 1980s.[78] This de minimis level — the lowest among major U.S. trading partners[79] — includes shipped goods, which has a huge effect on digital trade. Recent studies have shown that the small gains realized by collecting duties on these shipped goods are heavily outweighed by the costs of processing the large amount of shipments that fall below the de minimis level.[80] Encouraging Canada to raise the de minimis level on shipped goods and imports would result in a huge economic gain for both the U.S. and Canada by ensuring fairness for Canadian consumers, improving economic and government efficiency, and reducing the amount of hurdles small businesses operating internationally must jump over. As CCIA and others have observed, the renegotiation of the North American Free Trade Agreement provides a strategic opportunity to update the de minimis

---

[76] Comments of the Computer & Comm'ns Indus. Ass'n, Negotiating Objectives Regarding Modernization of the North American Free Trade Agreement with Canada and Mexico, Docket No. 2017-0006 (May 23, 2017), http://www.ccianet.org/wp-content/uploads/2017/06/CCIA-USTR-NAFTA-Comments.pdf [hereinafter "CCIA NAFTA Comments"].

[77] Not only is the restriction detrimental to U.S. services, but reports suggest that the strict requirements are ultimately financial unstainable as government services wish to move to cloud computing. *See* Jim Bagnal, *The Cloud Looms on Shared Services' Horizon*, THE OTTAWA SUN (Mar. 19, 2017), http://www.ottawasun.com/2017/03/19/bagnall-the-cloud-looms-on-shared-services-horizon.

[78] Andy Blatchford, *Feds Urged to Bump Up Duty-Free Limit For Canadian Shoppers*, THE HUFFINGTON POST (Mar. 16, 2016), http://www.huffingtonpost.ca/2016/03/16/ottawa-faces-renewed-calls-to-let-canadians-spend-more-without-paying-duty_n_9481262.html.

[79] *2017 Global Digital Trade Part I*, *supra* note 18, at 310.

[80] *See generally* Christine McDaniel, Simon Schropp, & Omin Latipov, *Rites of Passage: The Economic Effects of Raising the de minimis Threshold in Canada*, C.D. HOWE INSTITUTE (June 23, 2016), https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/E-brief_Rights%20of%20Passage_June16.pdf (stating "we find that lifting the threshold would have a net economic benefit of up to C$648 million.").

threshold and align the three trading partners to better facilitate digital trade and empower small business.[81]

C. China

The Chinese market has long been hostile to foreign competitors, but in recent years the focus on U.S. information technologies and Internet services has intensified. An influx of anticompetitive laws directed at information infrastructure and cloud services combined with an uptick in Internet shutdowns has business more and more hesitant to enter the Chinese market, costing American firms. 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.[82] 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.[83] A EuroCham survey showed that 13% of respondents had recently deferred R&D investment in China or had become unwilling to set up R&D operations after Internet restrictions increased in early 2015.[84] Numerous scholars argue that China's actions violate WTO rules mandating open access and equitable treatment between foreign and domestic firms.[85]

---

[81] CCIA NAFTA Comments, *supra* note 76, at 9; Comments of the R Street Institute, Negotiating Objectives Regarding Modernization of the North American Free Trade Agreement with Canada and Mexico, Docket No. 2017-0006 (May 23, 2017), https://www.rstreet.org/wp-content/uploads/2017/06/R-Street-NAFTA-Comments.pdf ("Increasing the [de minimis threshold] up to $800 is ideal. . . raising it considerably should be a priority for USTR's negotiators."); Andrea Durkin, *'De Minimis' Thresholds Are Not Trivial*, TRADE VISTAS (June 16, 2017), https://tradevistas.csis.org/de-minimis-thresholds-not-trivial/ ("With smaller sized transactions, administrative costs such as tariffs and customs fees make a big difference. Raising the de minimis threshold opens the door to many more small purchases, which consumers the world over are growing to expect as a fact of life, and which U.S. exporters are more than happy to oblige.").

[82] *China Business Climate Survey Report 2017*, AmCham China, https://www.amchamchina.org/policy-advocacy/business-climate-survey/.

[83] 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.

[84] Press Release, EU Chamber of Commerce in China, Internet Restrictions Increasingly Harmful to Businesses, Say European Companies in China (Feb. 12, 2015), http://www.europeanchamber.com.cn/en/press-releases/2235.

[85] Kevin Holden, *Breaking Through China's Great Firewall*, THE DIPLOMAT (July 30, 2014), http://thediplomat.com/2014/07/breaking-through-chinas-great-firewall/.

The Administration recognizes the concerns of the U.S. Internet and technology community with respect to China, as evidenced by the initiation of a Section 301 investigation to determine whether the policies of the Chinese government relating to technology transfer, intellectual property, and innovation are actionable under the Trade Act.[86] CCIA asks USTR to remain vigilant and discourage policies restricting foreign companies' ability to enter the Chinese technology sector, and to promote policies focused on allowing free and open competition within China's borders.

Data and Infrastructure Mandates

Chinese authorities have issued comprehensive guidelines for the treatment of personal data within information systems, requiring either (1) express consent of the data subject or (2) explicit regulatory or legal approval before personal data may be transferred abroad.[87] Chinese national security regulations also prevent the transfer of data abroad if it contains a "state secret", which includes all communication of "matters that have a vital bearing on state security and national interests."[88] China, along with Taiwan, Turkey, and India, also implements local-presence requirements for processing of payment transactions.[89]

Similarly, discriminatory practices are also prevalent in Chinese information technology industries. As USTR has previously noted,[90] foreign companies operating in cloud computing are forced to enter into joint partnerships with Chinese firms if they wish to conduct business

---

[86] Initiation of Section 301 Investigation; Hearing; and Request for Public Comments: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation, Dkt. No. USTR 2017-0016 (Aug. 24, 2017).

[87] On July 16, 2013, China's Ministry of Industry and Information Technology (MIIT) promulgated the Provisions on Protecting the Personal Information of Telecommunication and Internet Users, which went into effect on September 1, 2013. Dianxin He Hulianwangyonghu Geren Xinxi Baohu Guiding (电信和互联网用户个人信息保护规定) [Provisions on Protecting the Personal Information of Telecommunications and Internet Users] (promulgated by the Ministry of Indus. & Info. Tech. July 16, 2013, effective, Sept. 1, 2013) (China), *available at* http://www.lawinfochina.com/display.aspx?id=14971.

[88] Law of the People's Republic of China on Guarding State Secrets, Art. 2, *available at* http://www.npc.gov.cn/englishnpc/Law/2007-12/12/content_1383925.htm.

[89] *2014 Digital Trade in the U.S. and Global Economies, Part 2*, *supra* note 26, at 86.

[90] *2017 Key Barriers to Digital Trade*, *supra* note 2 ("China does not allow foreign-invested enterprises to directly offer cloud computing services within China, which is of enormous concern to U.S. companies—both those that supply cloud computing services and those that need to source such services.").

within China,[91] and industry representatives have cited their inability to obtain Internet service provider licenses in China without partnering with a domestic company that holds a business license.[92] China seeks to further restrain foreign cloud service operators, in concert with its national plan to promote the Chinese cloud computing industry.[93] China's Ministry of Industry and Information Technology (MIIT) issued a draft Notice on Regulating the Operation Behaviors in the Cloud Services Market for comment last November. Under the draft Notice, cloud service providers must obtain a value-added telecommunications business license, must host facilities and keep data within China, and are prohibited from using services to connect to a network outside China.[94] While the draft Notice is not yet in its final form, the ongoing debate creates uncertainty for U.S. companies operating abroad.

China seeks to further disadvantage foreign access to the cloud computing market under the guise of strengthening cybersecurity.[95] In 2016, China passed three piece of anticompetitive legislation concerning data localization with negative implications to cloud computing:[96] (1) a "counter-terrorism" law that requires Internet and telecommunication companies to create methods for monitoring content for terror threats,[97] (2) an online publishing law that requires that

---

[91] U.S.-China Economic and Security Review Commission, *Red Cloud Rising: Cloud Computing in China*, at 5 (Sept. 2013, revised Mar. 2014), http://origin.www.uscc.gov/sites/default/files/Research/DGI_Red%20Cloud%20Rising_2014.pdf.

[92] U.S.-CHINA BUSINESS COUNCIL, *Technology Security and IT in China: Benchmarking and Best Practices*, at 2 (June 2016), https://www.uschina.org/sites/default/files/Technology%20Security%20and%20IT%20in%20China%20-%20%20Benchmarking%20and%20Best%20Practices.pdf.

[93] The State Council, People's Rep. of China, *China Sets Ambitious Goal in Cloud Computing* (Apr. 11, 2017), http://english.gov.cn/state_council/ministries/2017/04/11/content_281475623431686.htm.

[94] Hunton & Williams, LLP, *China Publishes Regulations Regarding Cloud Services for Public Comment*, LEXOLOGY (Dec. 21, 2016), https://www.lexology.com/library/detail.aspx?g=37377ead-0e71-4715-850d-0d7771ed623d.

[95] 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.

[96] AmCham China, *Protecting Data Flows in the US-China Bilateral Investment Treaty*, at 4 (Apr. 2015), http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization. *See also* CCIA NTE Comments 2015, *supra* note 16, at 6-7.

[97] Bruce Einhorn, *A Cybersecurity Law in China Squeezes Foreign Tech Companies*, BLOOMBERG BUSINESSWEEK (Jan. 21, 2016), http://www.bloomberg.com/news/articles/2016-01-21/a-cybersecurity-law-in-china-squeezes-foreign-tech-companies.

all servers used for online publications and press are located within China, and (3) the long-awaited Cybersecurity law which came into effect this year.[98]

China's Cybersecurity Law went into effect on June 1 after being adopted by the National People's Congress in November 2016 following a year of legislative hearings and close international scrutiny.[99] 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.[100] 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.[101] Further, it is not clear what constitutes a "critical information infrastructure," possibly sweeping companies outside traditional information communication technologies into these obligations.[102] Subsequent draft notices from Chinese 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. 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.[103] While the latest draft removes some concerning language,[104] the

---

[98] David Barboza & Paul Mozurfeb, *New Chinese Rules on Foreign Firms' Online Content*, N.Y. TIMES (Feb. 19, 2016), http://www.nytimes.com/2016/02/20/business/media/new-chinese-rules-on-foreign-firms-online-content.html.

[99] *2016 Cybersecurity Law* (unofficial translation), http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en.

[100] *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.

[101] 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).

[102] 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 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.").

[103] COVINGTON, *China Seeks Public Comments on Draft Regulation on Cross-Border Data Transfer* (Apr. 12, 2017),

constant evolution of this new regime creates significant and costly regulatory uncertainty to those in the Chinese market.[105]

These regulations reflect an effort by the Chinese government to centralize cybersecurity policy at a national level, rather than in lower-level regulations or private contracts.[106] As a result foreign ICT equipment manufacturers are justifiably concerned about the burdens it will place on their ability to operate and introduce new products into the Chinese market.[107]

Filtering & Blocking

As CCIA explained to the U.S.-China Economic and Security Review Commission in 2015, barriers to digital trade in China continue to present significant challenges to U.S. exporters.[108] USTR acknowledged these challenges in the 2017 NTE, highlighting the burdens that China's filtering of cross-border Internet traffic have imposed, and recognizing that outright

---

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 Cross-Border Data Transfers* (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.

[104] COVINGTON, *China Seeks Comments on Updated Draft of Cross-Border Data Transfer Security Assessment Standard* (Aug. 31, 2017), https://www.cov.com//media/files/corporate/publications/2017/08/china_seeks_comments_on_updated_draft_of_crossborder_data_transfer.pdf.

[105] Some have observed that the ambiguity in the Cybersecurity Law will not lead to worst-case scenarios. CCIA is hopeful that the reported ongoing discussion among Chinese stakeholders will lead to necessary clarity and recognition of the value of cross-border data flows in innovation. *See* Samm Sacks et al, *Beyond the Worst-Case Assumptions on China's Cybersecurity Law*, NEW AMERICA CYBERSECURITY INITIATIVE (Oct. 13, 2017), https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/.

[106] Austin Ramzy, *What You Need to Know About China's Draft Cybersecurity Law*, N.Y. TIMES (July 9, 2015), http://sinosphere.blogs.nytimes.com/2015/07/09/what-you-need-to-know-about-chinas-draft-cybersecurity-law/.

[107] *China's New Cybersecurity Law Sparks Fresh Censorship and Espionage Fear*, THE GUARDIAN (Nov. 7, 2016), https://www.theguardian.com/world/2016/nov/07/chinas-new-cybersecurity-law-sparks-fresh-censorship-and-espionage-fears?CMP=share_btn_tw; Michael Martina, *Business Groups Petition China's Premier on Cyber Rules*, REUTERS (Aug. 11, 2016), http://www.reuters.com/article/us-cyber-china-business-idUSKCN10M1DN.

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

blocking of websites has worsened.[109] High-profile examples of targeted blocking of whole services have included China's blocking of major U.S. services including Facebook, Picasa, Twitter, Tumblr, Google Search, Foursquare, Hulu, YouTube, Dropbox, LinkedIn, and Slideshare.[110] In June 2017, China shut down over 60 news outlets and social media accounts under the new Cybersecurity Law.[111] Informal estimates suggest that this blocking has easily cost American firms billions of dollars as they are pushed out of the market.[112]

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. 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.[113]

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.

MIIT issued a notice in January calling for Chinese telecoms to provide VPNs only to conduct cross-border business activities.[114] The government then reportedly ordered three state-

---

[109] *See 2017 Key Barriers to Digital Trade*, *supra* note 2 (noting that "Eleven of the 25 most popular websites globally are currently blocked in China, imposing significant costs on both suppliers and users of web-based services and products.").

[110] *2014 Digital Trade in the U.S. and Global Economies*, *Part 2*, *supra* note 26, at 98.

[111] Oiwan Lam, China Shutters *Entertainment News Sites, Citing "Socialist Values" and Cybersecurity*, HONG KONG FREE PRESS (June 18, 2017), https://www.hongkongfp.com/2017/06/18/china-shutters-entertainment-news-sites-citing-socialist-values-cybersecurity/.

[112] Julie Makinen, *Chinese Censorship Costing U.S. Tech Firms Billions in Revenue*, L.A. TIMES (Sept. 22, 2015), http://www.latimes.com/business/la-fi-china-tech-20150922-story.html.

[113] 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/.

[114] MIIT Notice on Cleaning Up and Regulating the Internet Access Service Market (Jan. 22, 2017), http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057709/n4704651/c5471876/content.html.

owned telecommunication providers to bar individuals from using all VPNs pursuant to this policy over the summer.[115] While the Chinese government has subsequently denied such an order was issued noting that only unauthorized VPNs would be restricted,[116] they failed to clarify the process for determining when a VPN is deemed authorized.[117] Further, this summer Apple removed all VPNs from the China App Store at the direction of the government.[118] These efforts are not new. In January 2015, China made moves to upgrade its Internet firewall to make it harder for people to circumvent it by using VPNs.[119] In 2015, the country cracked down on special software tools hosted on GitHub, a website popular with open source enthusiasts,[120] by launching distributed denial of service attacks against the site.

D. Colombia

Legal Liability for Online Intermediaries

As CCIA previously observed in its 2017 Special 301 filing, Colombia has failed to comply with its obligations under the U.S.-Colombia Free Trade Agreement to provide protections for Internet service providers.[121] A current bill that seeks to implement the U.S.-Colombia FTA copyright chapter includes no language on online intermediaries. Without such protections required under the FTA, intermediaries exporting services to Colombia remain exposed to potential civil liability for services and functionality that are lawful in the United

---

[115] *China Tells Carriers to Block Access to Personal VPNs by February*, BLOOMBERG TECHNOLOGY (July 10, 2017), https://www.bloomberg.com/news/articles/2017-07-10/china-is-said-to-order-carriers-to-bar-personal-vpns-by-february.

[116] Li Xiyin, *The Ministry of Industry and Commerce Denied That the Operator to Prohibit Personal VPN Business*, THE PAPER (July 12, 2017), http://www.thepaper.cn/newsDetail_forward_1730060 (unofficial translation).

[117] Chiam Gartenberg, *China May Not Be Blocking VPNs After All*, THE VERGE (July 13, 2017), https://www.theverge.com/2017/7/13/15966240/china-vpn-block-report-conflicting-ministry-industry-information-technology.

[118] 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-apps-used-to-evade-censorship-from-its-china-store.

[119] Elizabeth Weise & Calum MacLeod, *China Blocks VPN Access to the Internet*, USA TODAY (Jan. 24, 2015), http://www.usatoday.com/story/tech/2015/01/23/china-internet-vpn-google-facebook-twitter/22235707/.

[120] Michael Kan, *China Intensifies Internet Censorship Ahead of Military Parade*, PC WORLD (Aug. 30, 2015), http://www.pcworld.com/article/2977109/china-intensifies-internet-censorship-ahead-of-military-parade.html.

[121] *2017 CCIA Special 301 Comments*, *supra* note 39.

States and elsewhere. We urge USTR to take action with Colombian counterparts to prioritize implementation of a complete intermediary framework as required by the FTA.

Imbalanced Copyright

The current bill that seeks to implement the U.S.-Colombia FTA copyright chapter also does not include widely recognized exceptions such as text and data mining, display of snippets or quotations, and other non-expressive or non-consumptive uses.

Lack of Application of Ex-Ante Regulation to Wholesale Broadband Access Services

In Colombia, wholesale broadband access services have not been deemed to warrant ex-ante regulation in order to prevent abuse of dominance. This leads to discrimination towards other market participants and stifles competition. The Communications Regulation Commission (CRC) has not indicated a willingness to change their position. Consumer protection is at the heart of the CRC's agenda and it therefore focuses its analysis on the last mile access for residential services, but not for other access products (e.g. bitstream and leased lines). Those products are particularly relevant for providers of communications services and ICT solutions in non-residential markets, such as those provided to larger businesses and public institutions.

E. European Union

The European Union is currently negotiating a vast number of regulatory proposals, addressing subjects including copyright, telecommunications, audiovisual, and "ePrivacy." Common to most proposals is a focus on regulating principally U.S.-based "online platforms" such as search providers, social media, and online marketplaces. CCIA agrees with USTR's assessment in the 2017 NTE that the "well-intentioned goal of creating a harmonized digital market in Europe, if implemented through flawed regulation, could seriously undermine transatlantic trade and investment, stifle innovation, and undermine the Commission's own efforts to promote a more robust, EU-wide digital economy."[122] Unfortunately, USTR's concern is likely to become a reality.

---

[122] *2017 NTE*, *supra* note 44, at 178-79. In USTR's 2016 NTE's assessment, they appropriately observed that "these initiatives appear motivated, at least in part, by legacy businesses struggling to compete against the efficiencies provided by Internet-based commerce. This underscores the risk that even well-intentioned goals can, if implemented through heavy-handed regulation, or even just threat thereof, seriously undermine innovative business

Data Localization

Within the European Union, many EU 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."[123]

In May 2015, Germany proposed a draft telecom bill that would, among other things, require telecommunication service providers and Internet service providers to store data in Germany for a period of 10 weeks.[124] 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[125] for a period of four weeks.[126] The German Bundestag approved the bill in October 2015.[127] While policymakers might reasonably impose certain security-related

---

development and hurt the EU's own efforts to inject more dynamism into its markets." Office of the U.S. Trade Rep., *2016 National Trade Estimate Report on Foreign Trade Barriers* at 178 (2016), https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf [hereinafter "*2016 NTE*"].

[123] 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-Flows-in-the-EU.pdf.

[124] Glyn Moody, *Germany's Data Retention Bill Requires Metadata to Be Kept in the Country*, ARS TECHNICA UK (May 19, 2015), http://arstechnica.co.uk/tech-policy/2015/05/germanys-data-retention-bill-requires-metadata-to-be-kept-in-the-country/.

[125] Many companies have already been moving data resources to Germany preemptively out of general political pressure. *See* Katharine Kendrick, *Risky Business: Data Localization*, FORBES (Feb. 19, 2015), http://www.forbes.com/sites/realspin/2015/02/19/risky-business-data-localization/.

[126] *Germany Adopts a Draft Telecom Data Retention Law that Includes a Localization Requirement*, HUNTON & WILLIAMS PRIVACY & INFORMATION SECURITY LAW BLOG (June 4, 2015), https://www.huntonprivacyblog.com/2015/06/04/germany-adopts-telecom-data-retention-law-includes-localization-requirement/.

[127] Deutsche Welle, *German Parliament Votes for New Data Retention Law*, DW (Oct. 16, 2015), http://www.dw.com/en/german-parliament-votes-for-new-data-retention-law/a-18786345. Such bills have not come without controversy in Germany, due to the automatic nature of the data retention. The German Federal Constitutional Court struck down a previous data retention bill in 2010, citing concerns about data security. *See* Dr. Jan Geert Ments et al., *Germany: New Data Retention Act – Retention Obligations for Telecommunications and Internet Access Service Providers*, LEXOLOGY (Oct. 16, 2015), http://www.lexology.com/library/detail.aspx?g=a17dcbf9-dec8-40f5-9950-04bee4a4894a.

limits to some sets of secure data, centralization and streamlining efforts may effectively result in the application of localization mandates to all government services. Like other data localization measures discussed in this section, this may discriminate against foreign suppliers and be a violation of WTO commitments. The requirements that service providers ensure that foreign jurisdictions cannot obtain the data would also impose German law unilaterally on international operators wherever they are based.[128]

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.[129] The regulation aims to remove national mandated data localization laws within Member States. CCIA supports the proposal as it will limit forced data localizations in EU Member States and provide legal clarity for companies and users.

Intermediary Liability and Mandatory User Monitoring, Filtering, and Blocking

In September 2016, the European Commission (EC) submitted a copyright proposal to the European Parliament and European Council that proposes to eliminate protections that limit online services' liability for misconduct by those services' users, requires proactive screening by service providers, and creates a "neighboring" pseudo-copyright restriction.[130] These proposals would upend nearly two decades of established law, threatening U.S. digital exports by eliminating long-standing legal protections for online services that are a cornerstone of Internet policy. This subsection discusses the intermediary liability ramifications of this proposal; the next discusses the "link tax."

---

[128] Hosuk Lee-Makiyama & Matthias Bauer, *The Bundes Cloud: Germany on the Edge to Discriminate Against Foreign Suppliers of Digital Services*, ECIPE (Sept. 2015), http://ecipe.org/publications/the-bundes-cloud-germany-on-the-edge-to-discriminate-against-foreign-suppliers-of-digital-services/?chapter=all.

[129] European Commission, Digital Single Market, Free Flow of Non-Personal Data, https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data (last updated Oct. 5, 2017); Press Release, CCIA Welcomes Proposal to End Forced Data Localization in EU Member States (Sept. 13, 2017), *available at* http://www.ccianet.org/2017/09/ccia-welcomes-proposal-to-end-forced-data-localisation-in-eu-member-states/.

[130] 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"].

The EC proposal disrupts settled law protecting intermediaries by weakening established protections from U.S. Internet services in the 2000 EU E-Commerce Directive, and by imposing an unworkable filtering mandate on hosting providers that would require automated "notice-and-stay-down" for a wide variety of copyrighted works. The EC proposal would dramatically weaken these long-standing liability protections, and suggests that most modern service providers may be ineligible for its protections.[131]

Like U.S. law, EU law contains an explicit provision stating that online services have no obligation to surveil users, or monitor or filter online content.[132] Online services have invested heavily in developing international markets, including Europe, in reliance on these provisions. The EC copyright proposal now implies that online services must procure or develop and implement content recognition technology. The proposal to compel affirmative filtering of all Internet content, including audiovisual works, images, and text, based on that content's copyright status, is alarming, and profoundly misguided.

Moreover, the EC proposal provides no specifics for what filtering a hosting provider must implement, effectively empowering European rightsholders to dictate U.S. services' technology in potentially inconsistent ways across Europe.[133] In short, a provider will never know when it has done 'enough,' short of litigating in every EU Member State. Until the CJEU eventually addresses the question, affected hosting providers can expect inconsistent rulings and injunctions from lower courts in different countries.

The proposal also appears to compel online services to enter into contracts with an indeterminate set of copyright holders, involving indeterminate subject matter, and withholds protection on *all* subject matter (not just copyright) for failure to do so. The vagueness of the language in the EU's copyright proposal, and the likelihood of inconsistent rulings in different countries, threatens to give the EU control over U.S. innovation. U.S. platforms, especially small businesses and startups, will be deterred from innovating and competing due to the

---

[131] *Id*. at recital 38 (suggesting that entities engaged in "optimizing the presentation of the uploaded works or subject matter or promoting them" may now be ineligible for existing protection).

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

[133] *See* Copyright Proposal, *supra* note 130, at art. 11.

ambiguity, harming U.S. companies and their consumers across the world. This would likely cause incalculable damage to the U.S. economy.

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 this kind of ambiguous legal framework for intermediaries.[134] If the EU proposal were to pass, there would likely be a corresponding increase in risk for U.S. platforms doing business in the EU, resulting in significant economic consequences for the U.S. digital economy that depends on the EU market. Furthermore, there is likely to be a ripple effect on the rest of the world, given the EU's international influence. By effectively revoking long-established protections upon which U.S. services relied when entering European markets, the proposal would limit U.S. companies' investments for the benefit of EU rightsholders, establishing a market access barrier for many U.S. services and startups.

Brussels is not the sole risk to established norms on limiting intermediary liability. EU courts are increasingly hostile to this principle. For example, the June 2015 European Court on Human Rights decision against Estonia-based news portal Delfi, imposing liability for comments posted under news articles on its site, is another example of a growing tendency to "shoot the messenger."[135] *Delfi* is difficult to reconcile with more modern approaches to intermediary liability, such as 47 U.S.C. § 230 and Europe's own E-Commerce Directive. Absent suitable intermediary liability protection for third party content, many U.S. services may be unable to enter foreign markets like Estonia due to liability risks.[136]

Internet companies are also experiencing concerning developments across EU Member States. Germany adopted the Act to Improve the Enforcement of Rights on Social Networks (the "Network Enforcement Law" or "NetzDG") in June 2017. The NetzDG law mandates removal

---

[134] 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.

[135] Delfi AS v. Estonia, Eur. Ct. H.R. 64569/09 (2015).

[136] Beschlussempfehlung und Bericht [Resolution and Report], Deutscher Bundestag: Drucksache [BT] 18/13013, http://dip21.bundestag.de/dip21/btd/18/130/1813013.pdf (Ger.). Unofficial English translation available at https://medium.com/speech-privacy/what-might-germanys-new-hate-speech-take-down-law-mean-for-tech-companies-c352efbbb993.

of "manifestly unlawful" content within 24 hours, and provides for penalties of up to 50 million Euros.[137] Unlawful content under the law includes a wide range of content from hate speech to unlawful propaganda.[138]

Italy recently passed a new amendment that further[139] empowers the Italian Communications Authority (AGCOM). The amendment permits AGCOM to "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."[140] 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 (DMCA)[141] and the E-Commerce Directive. Departures from established law serve as a market access barrier for U.S. services in Italy.

Imbalanced Copyright

The EU Commission's copyright proposal does not harmonize the exceptions and limitations across the EU. The freedom of panorama exception (the right to take and use photos of public spaces) was left out of the proposal entirely. Moreover, while a provision on Text and Data Mining is included, the qualifying conditions are too restrictive. The beneficiaries of this exception are limited to "research organizations," excluding individual researchers and startups.

---

[137] *Id*. § 3(2).

[138] *Id*. §1(3) (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).

[139] Italy passed regulations in 2013 that granted AGCOM the authority to order the removal of alleged infringing content and block domains at the ISP level upon notice by rights holders, independent of judicial process. In March 2017, the Regional Administrative Court of Lazio upheld AGCOM's authority to grant injunctions without a court order. *See* Gianluca Campus, *Italian Public Enforcement on Online Copyright Infringements*, KLUWER COPYRIGHT BLOG (June 16, 2017), http://copyrightblog.kluweriplaw.com/2017/06/16/italian-public-enforcement-online-copyright-infringements-agcom-regulation-held-valid-regional-administrative-court-lazio-still-room-cjeu/.

[140] 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.

[141] Codified at 17 U.S.C. § 512.

Ancillary Copyright/Link Tax

In 2017, USTR identified the "link tax" as a key digital trade barrier in several EU Member States, noting that these measures "effectively impose a tax on firms that provide valuable services, helping drive traffic to publishing sites, thereby increasing viewership and revenue."[142] As CCIA has explained in previous proceedings, restrictions on the ability to quote (*inter alia*) news content violate Europe's international commitments. Unfortunately, there is now a European Union-wide proposal for a "neighboring right" that would be more expansive than these previous laws and would squarely violate international legal obligations.[143]

Article 10(1) of the Berne Convention provides: "It *shall be* permissible to make quotations from a work which has already been lawfully made available to the public, provided that their making is compatible with fair practice, and their extent does not exceed that justified by the purpose, including quotations from newspaper articles and periodicals in the form of press summaries." As TRIPS incorporates this Berne mandate, compliance is not optional for WTO Members. A neighboring right is another form of snippet restriction and would violate this TRIPS commitment.

The EC proposal advances a new *sui generis* entitlement, branded a "neighboring right", for publishers in news content they publish. The proposal is a more expansive, EU-wide version of previous German and Spanish efforts.

The proposal specifically contemplates a link tax, since the language of the proposal states that it excludes "acts of hyperlinking *which do not constitute communication to the public.*"[144] Acts of hyperlinking which *do* constitute communication to the public, therefore, would be subjected to varying taxes in dozens of EU Member States. Given how broadly EU courts appear to interpret Europe's sweeping "communication to the public right"[145] (a right not

---

[142] *2017 Key Barriers to Digital Trade*, *supra* note 2.

[143] *See* Copyright Proposal, *supra* note 130, at art. 13.

[144] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM (2016) 593, Recital 33.

[145] GS Media BV v. Sanoma Media Netherlands BV (C-160/15).

found in the corresponding section of the U.S. Copyright Act),[146] the breadth of this tax is potentially sweeping and, at best, highly uncertain.

The new approach extends beyond a link tax, however. It also empowers a new class of plaintiffs with a 20-year, retroactive, entitlement to control (at least) digital reproduction and digitally making available of the press publications, independent of journalists' underlying rights in the news content. Article 11 will restrict the ability of online platforms to include news links and the snippets necessary to explain those links. CCIA urges the U.S. Government to engage directly with European officials to address concerns about this potential market access barrier.

As described in greater detail in CCIA's 2015 NTE submission, Germany's 2013 ancillary copyright law (*Leistungsschutzrecht*) remains in effect, irrespective of EU-wide neighboring rights regulation. By extending copyright protection to small text excerpts in search results, this law violates international obligations that require free quotation.[147]

As discussed more fully in CCIA's 2015 Special 301 submission,[148] the Spanish partial reform of intellectual property laws instituted a similar "snippet tax" that violates Spain's international commitments by subjecting normal quotations to a form of levy. This too is independent of the neighboring rights and link tax proposal currently being considered in Brussels. The Spanish law modified the German approach by prohibiting news producers from waiving their right to compensation, such that there is no means by which a covered news creator can waive rights or license platforms to publish snippets. Faced with this measure, Google suspended its Google News service in the Spanish market.[149] An economic consultancy found that, as a result of Google News shutting down in Spain, web traffic to smaller publications declined by about 14% — more than double the average traffic decline.[150] Such measures hardly

---

[146] 17 U.S.C. § 106 (2012).

[147] *See generally* Comments of CCIA, *In re* 2013 Special 301 Review, Dkt. No. USTR-2012-0022, filed Feb. 8, 2013.

[148] *See* Comments of CCIA, *In re* 2015 Special 301 Review, Dkt. No. USTR-2014-0025, filed Feb. 26, 2015.

[149] Antonia Molloy, *Google News to Shut Down in Spain*, USA TODAY (Dec. 11, 2014), http://www.usatoday.com/story/money/business/2014/12/11/google-news-spain-to-cease-operations/20234251/.

[150] NERA Econ. Consulting, *Impacto del Nuevo Artículo 32.2 de la Ley de Propiedad Intelectual*, xi (July 9, 2015), http://www.nera.com/content/dam/nera/publications/2015/090715%20Informe%20de%20NERA%20para%20AEEPP%20(VERSION%20FINAL)pdf.

help Spanish consumers either. Since news aggregators are discouraged under this law, there are fewer paths for people to find news published by smaller publications with less brand recognition. Like the German *Leistungsschutzrecht*, the Spanish IP revision not only undermines market access for U.S. companies and distorts established copyright law, but it also violates the EU and Spain's treaty and WTO commitments.[151]

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. Last year, France passed legislation creating a new royalty for indexing images on the Internet.[152] The law took effect in January 2017. The law creates a compulsory collective management system for the reproduction and communication to the public of plastic, graphic, and photographic works by online public communication services. Under the new system, automated image search services must negotiate agreements with collecting societies for royalties and permissions regarding the publication of the work. While not a snippet tax, this law reflects the 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 indexing these "rights" in a domestic collecting society, the law targets an industry that consistently largely of U.S. exporters.[153] As several industry and civil society organizations (including CCIA) have previously noted, the law will impact many online services and mobile apps.[154]

Transatlantic Commercial Data Flows

The 2015 decision by the Court of Justice of the European Union (CJEU) invalidating the European Commission's adequacy determination for the EU-U.S. Safe Harbor framework led to considerable regulatory uncertainty for companies with transatlantic operations. The Safe

---

[151] *See* Raquel Xalabarder, *The Remunerated Statutory Limitation for News Aggregation and Search Engines Proposed by the Spanish Government - Its Compliance with International and EU Law*, IN3 WORKING PAPER SERIES (Sept. 30, 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2504596.

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

[153] 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).

[154] Open Letter to Minister Azoulay, *available at* http://www.ccianet.org/wp-content/uploads/2016/03/Open-Letter-to-Minister-Azoulay-Image-Index-Bill-on-Creation-Eng.pdf.

Harbor program allowed for thousands of companies (including U.S. subsidiaries of European companies) to transfer data relating to EU citizens who use their services. As USTR acknowledged in the 2016 NTE: "The CJEU ruling has created tremendous legal uncertainty for both U.S. and European businesses dependent on the framework."[155]

Fortunately, a renegotiated framework for transatlantic commercial data transfers, the EU-U.S. Privacy Shield, went into effect on August 1, 2016, after almost a year of uncertainty.[156] Like the Safe Harbor before it, the new framework allows companies to sign up with the U.S. Department of Commerce to verify that their privacy policies comply with the data protection standards of the Privacy Shield.[157] Over 2,400 companies are now certified under the Privacy Shield. The first annual review took place on September 18-19 in Washington, bringing together officials from across the U.S. government and the European Commission for in-depth discussions on the current operation of the Privacy Shield. Following the review, both sides signaled a strong commitment to the agreement and to "continued collaboration to ensure it functions as intended."[158]

While the Privacy Shield represents an important step forward in protecting customer data, its existence may be threatened in the future by court challenges or modifications made during future annual reviews. Any significant challenges to the Privacy Shield may threaten the viability of EU-U.S. commercial data transfers in the future. To date, two legal challenges have been filed at the lower court of the CJEU.[159]

---

[155] *2016 NTE*, *supra* note 122.

[156] INT'L TRADE ADMIN., *EU-U.S. Privacy Shield Program Overview*, https://www.privacyshield.gov/Program-Overview (last accessed Oct. 19, 2017).

[157] EUROPEAN COMM'N, *EU-U.S. Privacy Shield Fully Operational from Today* (Aug. 1, 2016), http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=33704.

[158] Joint Press Statement from Secretary Ross and Commissioner Jourova on the Privacy Shield Review, (Sept. 20, 2017), *available at* https://www.commerce.gov/news/press-releases/2017/09/joint-press-statement-secretary-ross-and-commissioner-jourova-privacy.

[159] Julia Fioretti & Dustin Volz, *Privacy Group Launches Legal Challenge Against EU-U.S. Data Pact: Sources*, REUTERS (Oct. 20, 2016), http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN12Q2JK; Julia Fioretti, *EU-U.S. Personal Data Pact Faces Second Legal Challenge from Privacy Groups*, REUTERS (Nov. 2, 2016), http://www.reuters.com/article/us-eu-dataprotection-usa/eu-u-s-personal-data-pact-faces-second-legal-challenge-from-privacy-groups-idUSKBN12X253?il=0.

An alternative mechanism for ensuring that data transfers meet EU adequacy requirements, standard contractual clauses, is currently facing a legal challenge at the CJEU by parties that allege such clauses are inadequate on grounds similar to those used to invalidate the Safe Harbor.[160] Standard contractual clauses were employed by many businesses in the period following the Safe Harbor's invalidation, and remain an important secondary compliance mechanism given the ongoing evaluation of the Privacy Shield by companies and European data protection authorities. If the Privacy Shield and alternative tools are again invalidated, there will be no mechanism through which companies can legally transfer the data of EU citizens across the Atlantic for commercial purposes. Forcing international companies to keep all personal data in Europe is not feasible and would hit small firms the hardest.[161]

General Data Protection Regulation and "Right to Be Forgotten"

The EU General Data Protection Regulation (GDPR) was adopted on April 27, 2016, and will go into effect on May 25, 2018.[162] 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.[163] However, latent ambiguities in the text of the GDPR mean that much of the impact the bill will have to be determined by how EU data protection authorities will interpret the text. While the Article 29 Working Party adopted guidelines on various aspects of the

---

[160] The Irish High Court referred the case to the CJEU on October 3, 2017, sharing the Irish Data Protection Commissioner's concerns about the validity of the standard contractual clauses. Data Protection Commissioner v. Facebook Ireland Ltd, [2016] No. 2016/4809 (Ir.) at 290 ("To my mind the arguments of the DPC that the laws - and indeed the practices - of the United States do not respect the essence of the right to an effective remedy before an independent tribunal as guaranteed by Article 47 of the Charter, which applies to the data of all EU data subjects transferred to the United States, are well founded.").

[161] Melissa Blaustein, *Opinion: 'Startup Europe', Silicon Valley Sessions This Weeks Tackle EU Privacy Shield*, MERCURY NEWS (Sept. 18, 2017), http://www.mercurynews.com/2017/09/18/opinion-startup-europe-silicon-valley-sessions-this-week-tackle-eu-privacy-shield/.

[162] 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"].

[163] *See* Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), June 11, 2015, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (Presidency of the Council: "Compromise text. Several partial general approaches have been instrumental in converging views in Council on the proposal for a General Data Protection Regulation in its entirety.").

Regulation over the past year,[164] it is critical that companies are clear about what is required of them under the law and that the Regulation 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 companies operating in the EU are high.[165]

The 2014 ruling by the CJEU on the "right to be forgotten" requires search engine operators to delist URLs from their search results at the request of individuals in the EU, if the website is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed."[166] In the three years that the CJEU ruling has been in effect, a lack of consistent guidance has raised concerns for companies with global consumer bases. Those concerns result from uncertainty about how the ruling affects search providers' ability to provide accurate information to users and the possible extraterritorial application of the ruling by EU national data protection authorities.

For example, some search engines have been instructed that they should not link to certain news stories about the ruling in their search results, since those stories may refer to individuals who had earlier successfully petitioned for the "right to be forgotten."[167] In August 2015, the UK's data protection authority ordered the removal of links to "current news stories about older reports which themselves were removed from search results under the 'right to be forgotten' ruling."[168]

Other authorities have asserted that search engines must erase links from *all* domains used by the company, even though they may be focused on international audiences. For example, the French Data Protection Authority (CNIL) mandated that Google must apply "right to be forgotten" search result removals not just to searches on the .fr or .co.uk domains, but also

---

[164] European Commission, DG Justice, Article 29 Working Party, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=5008 (last visited Oct. 10, 2017).

[165] GDPR, *supra* note 162, at art. 83.

[166] Court of Justice of the European Union, Press Release No 70/14 (May 13, 2014), http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf.

[167] Samuel Gibbs, *Google Ordered to Remove Links to 'Right to be Forgotten' Removal Stories*, THE GUARDIAN (Aug. 20, 2015), http://www.theguardian.com/technology/2015/aug/20/google-ordered-to-remove-links-to-stories-about-right-to-be-forgotten-removals.

[168] *Id*.

to those conducted on .com and other Google domains with worldwide reach. However, this case is currently on appeal to France's highest court,[169] which referred legal questions to the CJEU this past July. If this appeal were to fail, French authorities would have the ability to constrain what non-French Internet users are able to access under EU legal standards, essentially giving France extraterritorial control to stop citizens of other countries from finding legally published information.[170] Such a ruling would send a signal to other governments that their laws should have extraterritorial impact as well, potentially triggering international conflicts of law, and creating significant market uncertainty for companies seeking to host user content and communications on a global basis.[171]

The GDPR also includes a "right to erasure" provision, which codifies the "right to be forgotten" and applies it to all data controllers. Under Article 17, controllers must erase personal data "without undue delay" if the data is no longer needed, the data subject objects to the processing, or the processing was unlawful.[172] Under the GDPR, the fine for noncompliance with these and other provisions can be up to 4% of a company's global operating costs.

Putting the onus on companies to respond to all requests in compliance with the "right to be forgotten" ruling and Article 17 of the GDPR is administratively burdensome. For example, popular U.S. services have fielded hundreds of thousands of requests since the policy went into effect.[173] Processing these requests requires considerable resources because each request must be examined individually. Small and medium-sized enterprises that also offer similar services but without similar resources to field these requests could find that the "right to be forgotten" and

---

[169] Alex Hern, *Google Takes Right to be Forgotten Battle to France's Highest Court*, THE GUARDIAN (May 19, 2016), https://www.theguardian.com/technology/2016/may/19/google-right-to-be-forgotten-fight-france-highest-court.

[170] Greg Sterling, *Right to Be Forgotten: French Argue They Have Authority to Regulate Google Globally*, SEARCH ENGINE LAND (Sept. 21, 2015), http://searchengineland.com/right-to-be-forgotten-french-argue-they-have-authority-to-regulate-google-globally-231233.

[171] Samuel Gibbs, *French Data Regulator Rejects Google's Right-to-be-Forgotten Appeal*, THE GUARDIAN (Sept. 21, 2015), http://www.theguardian.com/technology/2015/sep/21/french-google-right-to-be-forgotten-appeal; *see also* Daphne Keller, *The new, worse 'right to be forgotten'*, POLITICO (Jan. 27, 2016), http://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/.

[172] GDPR, *supra* note 162, at art. 17

[173] *See, e.g.*, Alex Hern, *Google Takes Right to be Forgotten*, *supra* note 169.

"right to erasure" pose a barrier to entry into the EU. USTR should monitor the outcome of these requirements for adherence with international commitments.

Undue Restrictions on Rich Interaction Applications (RIAs)

In the European Union, there have been discussions about using regulations to "level the playing field"[174] and correct for supposed market advantages of online companies, most recently in the European Commission's review of the EU electronic communications code, the Audiovisual Media Services Directive,[175] and the proposed e-Privacy Regulation.[176]

In May 2016, the European Commission published its proposal to reform Europe's audiovisual rules. Notably, this proposal introduces two amendments that undermine market access for U.S. companies. The first amendment is a mandatory requirement for video-on-demand providers to include in their catalogues a 20% share of European works (i.e. a 20% quota of European content). The European Parliament's final opinion and the European Council's general approach increased this quota to 30%. This measure could either force U.S. companies to buy large volumes of inexpensive European content or to reduce the number of non-European works in their catalogues.

The second amendment allows European countries targeted by the services of a video-on-demand provider to impose levies on this provider to finance EU Member States' cultural funds. In practice, this amendment destroys the "country of origin principle" for video-on-demand providers, a cornerstone of the current European audiovisual rules and one of the main incentives for U.S. companies to invest in the EU's audiovisual market. Under the current rules, video-on-demand providers have to comply only with the rules from their country of establishment to operate across the EU. With these amendments, video-on-demand providers would have to contribute to the cultural funds of up to 28 Member States. This would fragment the Single Market and significantly hamper the activities of U.S. companies in the EU's audiovisual market.

---

[174] Directive 2010/13, of the European Parliament and of the Council of 10 March 2010 on the Audiovisual Media Services Directive, 2010 O.J. (l 95), *available at* https://ec.europa.eu/digital-single-market/en/audiovisual-media-services-directive-avmsd.

[175] *Id*.

[176] Press Release, European Commission, A Digital Single Market for Europe (May 6, 2015), http://europa.eu/rapid/press-release_IP-15-4919_en.htm.

This reform also includes provisions that undermine the intermediary liability regime applicable to video-sharing platforms, by stipulating that "in case of conflicts", audiovisual rules would prevail over the European intermediary liability provisions.

The proposal for an e-Privacy Regulation was published by the European Commission on January 10, 2017 and is designed to replace the current e-Privacy Directive.[177] The proposal seeks to expand the existing Directive, which only applies to telecommunication services, to all "electronic communication services" including RIAs.[178] Rules that were originally created to apply to traditional telecommunication services will now apply to a variety of online applications from those that provide communications and messaging services to personalized advertising and the Internet of Things.[179] The Commission justifies this expansion by observing that since the enactment of the e-Privacy Directive, services entered the market that "from a consumer perspective are substitutable to traditional services, but do not have to comply with the same set of rules."[180] This is based on a flawed understanding of the services at issue and a failure to recognize that the Internet has flourished largely due to *not* treating RIAs and other over-the-top services like traditional telecommunications providers. The new obligations under this proposal on notice and consent are also concerning as they go beyond what is required under the GDPR.

The proposed electronic communications code extends certain legacy telecommunications requirements to RIAs which will seriously eliminate their free or almost free business model and could result in several U.S. companies pulling out of EU markets leaving users with less choice and less competition.

Value Added Tax/Customs Rules

The EU Value Added Tax system for e-Commerce has consistently been identified[181] as a non-tariff trade barrier, even within the EU Single Market. To address some of the complexity,

---

[177] Proposal for a Regulation on Privacy and Electronic Communications 2017/003, *available at* http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241 [hereinafter "Proposal for ePrivacy Regulation"].

[178] *Id*. at art. 4 (CCIA is furthered concerned that the definition of an "electronic communication service" is not final and dependent on the also pending Electronic Communications Code).

[179] *Id*. at recital 12.

[180] *Id*. at recital 6.

[181] EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Understanding Non-Tariff Barriers in the Single Market* (Oct. 2017), http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608747/EPRS_BRI(2017)608747_EN.pdf.

the EU Commission has proposed a relatively fundamental overhaul of the system.[182] Most of the proposal deals with intra-EU commerce: the proposal introduces a simplified one-stop-shop mechanism which allows businesses to make a single VAT declaration and payment in their own Member State, rather than having to declare and pay VAT to each individual Member State where their customers are based. At the same time, the Commission is proposing to remove the current low value threshold for imports from non-EU countries (22 Euros), meaning that VAT is due on all transactions. This means that low value shipments from non-EU merchants to EU consumers will also be subject to the same lengthy customs process (including VAT collection) as high-value items, leading to considerable lead times. The only way a non-EU merchant will be able to access the EU market at equal speed as his local competitors is to find a local intermediary and sign up to the one-stop-shop through that intermediary. However, even in that case, the non-EU merchant will be required to charge and remit the standard VAT rate applicable in the country of the customer. In addition to the cost of complying with all different VAT rates in Europe (more than 150), non-EU merchants will be disadvantaged as they cannot apply the reduced or zero rates applicable in certain product categories.

F. India

Data Localization

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.[183] Indian authorities have contemplated extending localization

[182] Press Release, European Commission, Commission Proposes New Tax Rules to Support E-Commerce and Online Businesses in the EU (Dec. 1, 2016), http://europa.eu/rapid/press-release_IP-16-4010_en.htm.

[183] Chander & Lê, *Data Nationalism*, *supra* note 19, at 694-97.

policies to non-government communications as well,[184] which would require all private data of Indian citizens to be stored on servers within the country and prevent the mirroring of data on servers abroad.[185]

India's Telecommunications Regulatory Authority of India (TRAI) recently concluded a consultation on cloud computing. In their recommendations, they failed to adopt strong prohibitory language on mandated data localization.[186] Rather, they observed that any final view on this subject will have to be taken by the Government based on comprehensive review and its impact on the cloud industry.[187] 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.

Filtering & Blocking

The Indian government regularly shuts down mobile Internet services across regions in response to local unrest and protests, to prevent what it calls "anti-national activity."[188] Often the shutdowns are in response to or in preparation for actions that may cause disturbances or violence, ranging from protests over jobs, and wrestling tournaments to name a few.[189] These shutdowns stand in stark contrast to India's recent efforts to expand Internet services across the

---

[184] 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-council-proposes-3pronged-plan-to-protect-internet-users/article5685794.ece.

[185] Like many other countries, India may be contemplating data localization as an economic investment strategy: ECIPE estimates predict that India's data localization efforts will lead to a 1.4% decrease in domestic investment. *See* 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.

[186] TELECOMM. REGULATORY 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').

[187] *Id*.

[188] Hasit Shah, *Where 'Digital India' Ends*, SLATE (Sept. 7, 2016), http://www.slate.com/articles/technology/future_tense/2016/09/india_champion_of_web_access_cuts_off_mobile_internet_in_kashmir.html.

[189] Deji Bryce Olukotun, *The Absurd Excuses Countries Give for Shutting Off Internet Access*, SLATE (July 21, 2016), http://www.slate.com/blogs/future_tense/2016/07/21/excuses_officials_give_for_shutting_off_internet_access_include_wrestling.html.

country, and have led CCIA members including Facebook and Google to weigh in by developing Service Restriction Orders.[190] The Brookings research noted on page 8 estimates that Internet shutdowns cost India's GDP at least $968 million over 70 days it was shut down in 2016.[191]

Legal Liability for Online Intermediaries

While India has sought to limit service provider liability, an empirical study found that rules for the administration of takedowns by intermediaries passed in 2011 have a chilling effect on free expression by encouraging over-compliance with takedown notices in order to limit liability, and by not establishing sufficient safeguards to prevent misuse and abuse of the takedown process.[192] CCIA thanks USTR for highlighting the dangerous effects of these rules in the 2017 NTE.[193] For example in 2012, U.S. Internet services were threatened with criminal prosecution in India for hosting material that "seeks to create enmity, hatred and communal violence" and "will corrupt minds,"[194] and executives faced possible prison terms, in addition to financial penalties,[195] based on legal standards that are essentially strict liability.[196] Although India's Supreme Court earlier clarified and struck down some sections of the 2000 IT Act,[197] its

---

[190] *Id*.

[191] Darrell M. West, *Internet Shutdowns*, *supra* note 31, at 7.

[192] Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet,* CENTER FOR INTERNET & SOC'Y (2011), http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf.

[193] *See also 2017 NTE*, *supra* note 44, at 217 ("India's 2011 Information Technology Rules fail to provide a robust safe harbor framework to shield online intermediaries from liability for third-party user content. Any citizen can complain that certain content is "disparaging" or "harmful," and intermediaries must respond by removing that content within 36 hours. Failure to act, even in the absence of a court order, can lead to liability for the intermediary. The absence of a safe harbor framework discourages investment to Internet services that depend on user generated content.").

[194] Amol Sharma, *Facebook, Google to Stand Trial in India*, WALL ST. J. (Mar. 13, 2012), http://online.wsj.com/article/SB10001424052702304537904577277263704300998.html.

[195] Rebecca MacKinnon, *The War for India's Internet*, FOREIGN POLICY (June 6, 2012), http://www.foreignpolicy.com/articles/2012/06/06/the_war_for_india_s_internet?page=0,0.

[196] Amol Sharma, *In Search of Justice at the Google, Facebook Trial*, INDIA REAL TIME (Mar. 13, 2012), http://blogs.wsj.com/indiarealtime/2012/03/13/in-search-of-justice-at-the-google-facebook-trial.

[197] Shreya Singhal v. Union of India, A.I.R. 2015 SC 1523 (striking down a section of the IT Act which mandated intermediaries block content based on allegations that the content was "grossly offensive or has menacing character" or that false information was posted "for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will" due to overbreadth, and providing that "notice" for purpose of an intermediary's duty to remove content can only occur if an adjudicatory body issues an order on the intermediaries to remove the content). CCIA is glad to see revisions of prior decisions that limited safe harbor protections in copyright infringement cases, most recently with the Delhi High Court's order in the case of

existing provisions have still been harmful to intermediaries. In October 2015, an administrator of a WhatsApp group was arrested when someone in his group shared a video depicting violence toward a cow and the prime minister (notwithstanding the fact that group administrators in this application could not even delete members' posts in this app).[198] Imposing liability on an intermediary who cannot technologically respond to content is tantamount to a prohibition on use of the application.[199]

Last year,[200] the Supreme Court ordered Google, Microsoft, and Yahoo to filter terms related to online advertisements for prenatal gender determination kits, which are banned in India. When confronting industry's argument that banning by key terms will likely remove permitted speech as well, the Court informed them that they should stop operating in India if they cannot resolve those issues.[201] Last February, the Court further directed Google, Microsoft, and Yahoo to set up their own in-house experts to monitor and delete the prohibited ads.[202]

Myspace Inc. vs. Super Cassettes Industries. (2016) C.S(OS) 2682/2008, *available at* http://lobis.nic.in/ddir/dhc/SRB/judgement/24-12-2016/SRB23122016FAOOS5402011.pdf. The court upheld the original interpretation of the law, providing that intermediaries cannot be held liable for infringement absent "actual knowledge" rather than "general knowledge" and that Section 81 ("nothing in this Act shall restrict any person from exercising any right under the Copyright Act") of the IT Act does not bar application of the safe harbor in the cases of copyright infringement.

[198] Varun B. Krishnan, *Social Media Administrator? You Could Land in Trouble*, NEW INDIA EXPRESS (Oct. 10, 2015), http://www.newindianexpress.com/states/tamil_nadu/Social-Media-Administrator-You-Could-Land-in-Trouble/2015/10/10/article3071815.ece.

[199] A study by Copenhagen Economics found that online intermediaries can become a significant part of India's economy and their GDP contribution may increase to more than 1.3% by 2015 provided that the existing safe harbor regime is improved. Such opportunities would be valuable to American companies. *See* Copenhagen Economics, *Closing the Gap – Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose*, GLOBAL NETWORK INITIATIVE (Mar. 2014), https://globalnetworkinitiative.org//sites/default/files/Closing%20the%20Gap%20-%20Copenhagen%20Economics_March%202014_0.pdf.

[200] Arap Gupta, *The Supreme Court's Slow March Towards Eroding Online Intermediary Liability*, THE WIRE (Jul. 14, 2017), http://thewire.in/51399/ignorance-is-not-an-excuse-in-law/ (noting that the Supreme Court had failed to deliver a final ruling but instead repeatedly issuing orders to investigate the possibility of website blocking and key word filtering for search engine to remove generated ads).

[201] Manish Singh, *Google, Microsoft and Yahoo Slammed by India's Supreme Court Over Sex Selection*, CNET (Jul. 6, 2016), https://www.cnet.com/news/indias-supreme-court-orders-google-yahoo-and-microsoft-to-stop-showing-sex-determination-ads/.

[202] Krishnadas Rajagopal, *Banning Online Pre-Natal Sex Determination Content Dangerous: SC*, THE HINDU (Apr. 11, 2017), http://www.thehindu.com/news/national/general-ban-on-online-pre-natal-sex-determination-content-may-smother-citizens-right-to-know-supreme-court/article17926261.ece.

Undue Restrictions on Rich Interaction Applications (RIAs)

TRAI has indicated that it will soon release a consultation paper on RIAs to address "residual issues" which reportedly may include attempts at "leveling the playing field" between RIAs and licensed telecom provides and imposing security requirements on data records and logs on RIAs services.[203] In 2015, TRAI proposed introducing licensing and regulatory obligations targeted at OTT VoIP.[204] However, TRAI Chairman RS Sharma has said that, since that time, the telecom sector had undergone a "lot of significant changes" and cited TRAI's parallel work around differential pricing and net neutrality as a reason the original proposal may not be necessary.

G. Indonesia

Data and Infrastructure Localization

As USTR noted in the 2017 NTE, data localization requirements remain a serious concern in Indonesia.[205] Since 2012, service providers providing a "public service" have been required to localize data servers within the country.[206] USTR 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."[207] 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.[208]

As also noted in the 2017 NTE, 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

---

[203] *TRAI's Net Neutrality Views by October-End; OTT Consultation Soon*, THE ECONOMIC TIMES (Oct. 2, 2017), http://economictimes.indiatimes.com/tech/internet/trais-net-neutrality-views-by-october-end-ott-consultation-soon/articleshow/60910267.cms.

[204] *TRAI seeks to regulate OTT players like Skype, Viber, WhatsApp, and Google Talk*, THE INDIAN EXPRESS (Apr. 18, 2015), http://indianexpress.com/article/technology/social/trai-seeks-to-regulate-ott-players-like-skype-viber-whatsapp-and-google-talk/.

[205] *2017 NTE*, *supra* note 44, at 236.

[206] *2017 Key Barriers to Digital Trade*, *supra* note 2.

[207] *2017 NTE*, *supra* note 44, at 236.

[208] Chander & Lê, *Data Nationalism*, *supra* note 19, at 698.

locally sourced components and services.[209] Additionally, Indonesia has issued a regulation that requires 4G enabled devices to contain 30% local content.[210]

Undue Restrictions on Rich Interaction Applications (RIAs)

Indonesia's Ministry of Communications and Informatics released draft over-the-top service regulations that essentially require offshore online services to come onshore or face a higher tax rate in 2016.[211] This law would require data localization, new liability and monitoring requirements for online services, creation of a local entity or permanent establishment, and numerous other market access barriers. CCIA was pleased by reports that the implementation of this regulation would be delayed until officials can address the concerns about the implications of the proposal to the digital ecosystem in Indonesia.[212] However, the government has since stated that they will issue a new a decree aimed at regulating such services at the end of this year, a plan that was recently revealed at the ITU Telecom World Global Forum in September.[213]

H. Iran

Filtering & Blocking

In May 2014, Iran blocked access to Google's hosting platform, Google Sites, and censored at least two Wikipedia pages.[214] The country also continues to block Twitter and Facebook, with YouTube being blocked intermittently, while some government officials have pushed to block WhatsApp and Viber.[215] Freedom House also ranked Iran as the third worst country for Internet freedom in its 2016 report.[216] In late 2014, reports from Iran suggested that

---

[209] *2017 NTE*, *supra* note 44, at 234-35.

[210] *Id*. at 235.

[211] *MCIT Issues Draft Regulation on OTT in Indonesia*, TELEGEOGRAPHY (May 5, 2016), https://www.telegeography.com/products/commsupdate/articles/2016/05/05/mcit-issues-draft-regulation-on-ott-in-indonesia/.

[212] *2017 Global Digital Trade Part I*, *supra* note 18, at 308 ("According to a January 2017 press report, the Indonesian government plans to issue a final regulation after Indonesia's tax dispute with Google is resolved.").

[213] Winny Tang, *Indonesia Set to Regulate OTT Content Providers*, THE JAKARTA POST (Sept. 28, 2017), http://www.thejakartapost.com/news/2017/09/28/indonesia-set-regulate-ott-content-providers.html.

[214] Lorenzo Franceschi-Bicchierai, *Iran Takes Aim at Google, Wikipedia in Latest Internet Censorship Effort*, MASHABLE (May 16, 2014), http://mashable.com/2014/05/16/iran-google-wikipedia/.

[215] *Jokes and Medicine: the Viber Lives of Iranians*, BBC NEWS (Mar. 9, 2015), http://www.bbc.co.uk/monitoring/jokes-and-medicine-the-viber-lives-of-iranians.

[216] *Internet Freedom 2016*, *supra* note 28. Freedom House previously ranked Iran as the worst country for Internet freedom in its 2014 report, and Iran tied for second worst in 2015.

the country would impose a filtering system, rather than blocking websites outright. In February 2016, Iranian Communications and Information Technology Minister Ali Asghar Amidian announced that the Iranian government, in connection with several Iranian universities, spent $36 million to develop a "smart filtering" system intended to implement selective blocking of specific content.[217]

I. Mexico

Data Localization

Mexico should also resolve ambiguities surrounding the types of data that can be stored in the cloud following the cloud computing legislation. In January, Mexico passed the General Law on Data Protection. While the law was directed at the public sector, the law has implications for the private cloud computing market. The renegotiation of NAFTA provides a clear opportunity to resolve issues relating to cross-border data flows between U.S. and Mexico. In approaching the negotiations, USTR should adopt the policy of prohibiting government from interfering with data flows or the exchange of information online.[218]

Value Added Tax/Customs Rules

Mexico's Customs Agency seeks to drastically modify its simplified imports model by increasing the Value Added Tax and the duty for express shipments, transforming their simplified model into one more in line with the definite imports model.[219] The proposed changes would force higher prices, extend product shipment wait times, and decrease product selection for customers. Rejecting these proposed changes and sticking with a simplified imports model will help fuel the growth of the tech industry in Mexico, and will give consumers a wider selection of technology products at competitive prices. USTR should raise this issue in the

---

[217] *Iran to Spend $36 Million on Internet "Smart Filtering" to No Avail*, INTERNATIONAL CAMPAIGN FOR HUMAN RIGHTS IN IRAN (Feb. 23, 2016), https://www.iranhumanrights.org/2016/02/iran-will-spend-36m-on-smart-filtering/.

[218] Bijan Madhani, *Digital Issues In NAFTA: Cross-Border Data Flows and Cybersecurity*, DISRUPTIVE COMPETITION PROJECT (June 15, 2017), http://www.project-disco.org/21st-century-trade/061517-digital-issues-in-nafta-cross-border-data-flows-and-cybersecurity/.

[219] On June 22, 2016, Mexico's Tax Administration Service issued a ruling announcing amendments to the current Foreign Trade Rule 3.7.3 and proposed new rule 3.7.35. *See (Mexico) SAT publishes new amendments to general foreign trade rules*, EDICOM (July 19, 2016), http://www.edicomgroup.com/en_US/news/8488-mexico-sat-publishes-new-amendments-to-general-foreign-trade-rules.

upcoming NTE, and encourage the Mexican government to ensure compliance with international trade commitments.

J. Nigeria

Data and Infrastructure Localization

In December 2013, the National Information Technology Development Agency (NITDA), an agency of the Federal Ministry of Communication Technology, issued the Guidelines for Nigerian Content Development in the ICT sector. The guidelines require that within three years, makers of original ICT equipment utilize at least 50% of local manufactures in their products, and that ICT companies generally must use Nigerian companies to provide 80% of "value added services" on their networks. Other sections of concern require that all government data be hosted locally (unless officially exempted) and that all subscriber and consumer data be locally hosted. There remains a lack of clarification regarding the sanctions U.S. companies may face for not complying with the guidelines.

As a 2016 State Department report described the guidelines, "[t]he goal is to promote development of domestic production of ICT products and services for the Nigerian and global markets, but the guidelines present impediments and risks to foreign investment and U.S. companies by interrupting their global supply chain, increasing costs, disrupting global flow of data, and stifling innovative products and services."[220] One analysis concluded the guidelines "will prop up domestic technology enterprises at the expense of higher quality and/or more efficient foreign ones."[221]

K. Pakistan

Filtering & Blocking

Both Twitter and Facebook have intermittently been blocked in Pakistan, while Facebook is also routinely asked by the government to censor material deemed

---

[220] U.S. DEP'T OF STATE, *Nigeria Investment Climate 2015* at 13 (May 2015), http://www.state.gov/documents/organization/241898.pdf.

[221] Michelle A. Wein, *The Worst Innovation Mercantilist Policies of 2014*, ITIF (Dec. 2014), http://www2.itif.org/2014-worst-mercantilist-fourteen.pdf.

"blasphemous".[222] The popular blog platform WordPress was also temporarily blocked for several days earlier in 2015 with little explanation from authorities.[223] These blocks have cost the Pakistani GDP an estimated $69 million dollars so far, this year.[224]

L. Peru

Legal Liability for Online Intermediaries

Peru is out of compliance with key provisions under the U.S.-Peru Trade Promotion Agreement ("USPTPA") which require protections against copyright infringement claims for online intermediaries.[225] Understanding this threat to foreign investment in Peru, USTR rightly cited this discrepancy in its inclusion of Peru in the 2017 Special 301 Report.[226] We urge USTR to engage with Peruvian counterparts and push for full implementation of the agreement and establish limited liability for ISPs within the parameters of the USPTPA.

M. Russia

Data and Infrastructure Localization

Russia signed localization measures into law in July of 2014, which went into effect on September 1, 2015.[227] 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.[228] 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

---

[222] *See* Gibran Ashraf, *Facebook Censored 54 Posts for 'Blasphemy' in Pakistan in Second Half of 2014*, THE EXPRESS TRIBUNE (Mar. 18, 2015), http://tribune.com.pk/story/855030/facebook-censored-54-posts-for-blasphemy-in-pakistan-in-second-half-of-2014/; Yoree Coh, *Jack Dorsey's Challenge: Simplify Twitter for Users Like Its Chairman*, WALL ST. J. (Oct. 22, 2015), http://blogs.wsj.com/digits/2015/10/22/jack-dorseys-new-boss-finds-twitter-intimidating-to-use/.

[223] Bina Shah, *WordPress Ban*, DAWN (Mar. 26, 2015), http://www.dawn.com/news/1171842.

[224] Darrell M. West, *Internet Shutdowns*, *supra* note 31, at 3.

[225] U.S.-Peru Trade Promotion Agreement, art. 16.11, para. 29.

[226] U.S. TRADE REPRESENTATIVE, *2017 Special 301 Report*, at 68-69 (2017), https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF.

[227] 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.

[228] Reports have differed on whether regulators insist on data being *exclusively* located within Russia.

audience.[229] 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,[230] as well as the requirements to inform Russia's telecommunications authorities.[231] Further, Russia has yet to issue implementing regulations, creating further uncertainty as to what the rules actually require.[232] The threat to U.S. industry was illustrated when Russia blocked access to LinkedIn in 2016 over perceived violations of the law.[233] CCIA thanks USTR for emphasizing this issue in the 2017 NTE,[234] and hopes that USTR will continue to highlight this issue moving forward.

Roskomnadzor, the Russian agency responsible for enforcing the new data localization laws, conducted 302 inspections for compliance with the new law in 2015 alone, though Roskomnadzor Head Alexander Zharov reported the inspections revealed only minor infractions that he believed would be easily fixed, and would not lead to fines.[235] However, Zharov also stated that Roskomnadzor planned to evaluate at least 1,500 inspections in 2016 under the new law.[236] While initially Roskomnadzor indicated it would focus inspections on small to medium-

---

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

[230] News outlets have reported that the telecommunications authority has a list of 317 companies it will seek to investigate by the end of the year, and which may be banned from doing business in Russia if they are not found in compliance with the law. This may set a precedent for denial of market access in violation of Russia's trade agreements. *See, e.g.*, Georgy Bovt, *Will Data Law Isolate Russia Further? (Op-Ed)*, MOSCOW TIMES (Sept. 1, 2015), http://www.themoscowtimes.com/opinion/article/will-data-law-isolate-russia-further-op-ed/529229.html

[231] Courtney M. Bowman, *Primer on Russia's New Data Localization Law*, NAT'L LAW REVIEW (Aug. 28, 2015), http://www.natlawreview.com/article/primer-russia-s-new-data-localization-law/.

[232] *2017 NTE*, *supra* note 44, at 383.

[233] 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-to-linkedin-idUSKBN13D0ST.

[234] *2017 NTE*, *supra* note 44 at 382.

[235] Anthony L. Gallia, Luke P. McLoughlin, Maxim A. Voltchenko, *Russia's Personal Data Localization Law: Expanding Enforcement*, LEXOLOGY (Apr. 27, 2016), http: www.lexology.com/library/detail.aspx?g=b6eee37a-06b4-431a-9053-5400265739ed.

[236] Bret Cohen, Natalia Gulyaeva, Maria Sedykh, *Russia Data Localization Update: Results from Regulatory Inspections Clarify Enforcement Approach*, HOGAN LOVELLS: CHRONICLE OF DATA PROTECTION (June 23, 2016), http://www.hldataprotection.com/2016/06/articles/international-eu-privacy/russia-data-localization-update-results-from-regulatory-inspections-clarify-enforcement-approach/ [hereinafter Cohen, Gulyaeva, and Sedykh].

sized companies, Roskomnadzor notified Facebook and Twitter of the various requirements of the law, and indicated both companies could be subject to audit in the future.[237]

ECIPE predicts that, due to productivity losses associated with these policies, the Russian economy would shrink by 286 billion rubles (equivalent to $5.7 billion or -0.27% of Russia's GDP). Further, investment would drop by -1.41% or 187 billion rubles.[238] These losses also reflect lost export opportunities for U.S. service providers. In the wake of the new law, 45,000 companies have informed Roskomnadzor that they are currently in compliance with the law.[239]

Filtering & Blocking

Russia's 2012 Internet blacklist law, depending how expansively it is used, has the potential to block numerous American owned websites and services.[240] According to Freedom House, "blocking access to information on entire websites, IP addresses, and particular webpages has become the most common means in Russia to restrict user activity on the Internet."[241]

In August 2015, Russia temporarily took down the entire Wikipedia site, reportedly in response to a page regarding the preparation of a form of cannabis called "charas". After the page was edited to meet authorities' approval, the site came online again.[242] Russia also temporarily suspended Reddit in summer 2015 after a Russian user posted about psychedelic mushrooms. While the site was restored, Reddit now suppresses certain posts or subsections of its site for different countries, based on requests from authorities.[243]

---

[237] *See* Sergei Blagov, *Russia Pledges More Data Localization Audits*, BLOOMBERG BNA (Nov. 12, 2015), http://bna.com/russia-pledges-data-n57982063580/; *see also Interview with Alexander Zharov*, http://rkn.gov.ru/news/rsoc/news34448.htm (unofficial translation).

[238] Matthias Bauer, Hosuk Lee-Makiyama, & Erik van der Marel, *Data Localisation in Russia: A Self-imposed Sanction*, EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY (June 2015), http://ecipe.org/publications/data-localisation-russia-self-imposed-sanction/.

[239] Cohen, Gulyaeva, and Sedykh, *supra* note 236.

[240] Miriam Elder, *Censorship Row Over Russian Internet Blacklist*, THE GUARDIAN (Nov. 12, 2012), http://www.theguardian.com/world/2012/nov/12/censorship-row-russian-internet-blacklist.

[241] Freedom House, *Freedom on the Net 2013*, at 592 (Oct. 2013), http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf.

[242] Amar Toor, *Russia Banned Wikipedia Because It Couldn't Censor Pages*, THE VERGE (Aug. 27, 2015), http://www.theverge.com/2015/8/27/9210475/russia-wikipedia-ban-censorship.

[243] Rob Price, *Reddit is Now Censoring Posts and Communities on a Country-by-Country Basis*, BUSINESS INSIDER (Aug. 14, 2015), http://www.businessinsider.com/reddit-unbanned-russia-magic-mushrooms-germany-watchpeopledie-localised-censorship-2015-8.

Legal Liability for Online Intermediaries

The recently enacted "Mirrors Law" extends Russia's copyright strict enforcement rules[244] 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.[245] 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.

"Right to Be Forgotten"

In addition to the EU and France, Russia adopted a "right to be forgotten" law, which took effect January 1, 2016.[246] The law requires search engine operators to delete personal information that is false, obsolete, or violates Russian law; however, search engines working on behalf of the government are excluded from the law. The law requires search engine operators to remove the infringing content within 3 to 10 days, or the individual requesting deletion may go to court and get a warrant demanding removal of the information.[247]

Undue Restrictions on Over-the-Top Services

With the entry of Netflix in Russia in 2016, Russia sought immediately to further[248] restrict foreign ownership in media services, with a disproportionate effect on U.S.-based companies.[249] In May, Russia adopted amendments to the Federal Law on Information,

---

[244] 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.

[245] *Russia: New Law on Blocking Copies of Pirate Websites Without Launching a Lawsuit*, LEXOLOGY (Aug. 9, 2017), https://www.lexology.com/library/detail.aspx?g=ccd719d9-6628-4935-8ed9-e944dca4118e.

[246] *Russia's 'Right to be Forgotten' Bill Comes into Effect*, RT (Jan. 1, 2016), https://www.rt.com/politics/327681-russia-internet-delete-personal/.

[247] *Id*.

[248] A similar law directed at media companies was passed in January 2016 which limited foreign ownership to 20%.

[249] Vladimir Kozlov, *Netflix Continues Operating in Russia Despite Foreign Ownership Restrictions*, THE HOLLYWOOD REPORTER (Jul. 3, 2017), http://www.hollywoodreporter.com/news/netflix-continues-operating-russia-foreign-ownership-restrictions-1015525 ("The law on online video service ownership was largely provoked by Netflix's launch in Russia. In 2016, a number of local online video services complained that Netflix, as a global player, would present unfair competition to their operations.").

Information Technologies and Protection of Information and Certain Laws of the Russian Federation, targeted at over-the-top (OTT) platforms that also provide audiovisual content.[250] The law does not apply to services whose content is provided mostly by users, search engines, and network mass media. Under the new law, an OTT service qualifies as an "audiovisual resource" if it is used for organizing and providing online distribution of fee-based or ad-supported audiovisual products, directed at Russian users, and has more than 100,000 average daily users.[251] All audiovisual resources registered in Russia must either be owned (1) by a Russian entity with no more than 20% of foreign-owned shares or (2) by a Russian citizen without foreign citizenship.[252]

Under the law, OTT services that qualify as an audiovisual resource must prevent the use of their services for "illegitimate purposes" such as disseminating information, inciting or advocating violence or other illegal activities; classify and label content directed at children; comply with mass media distribution requirements which include preventing the broadcasting of content not registered as mass media under Russian law; and install software for keeping records of users.[253] Failure to comply may result in a country-wide block of the service.

N. South Korea

Extraterritorial Regulation

On September 23, 2016, South Korea's Amendment to the Act on the Promotion of IT Network Use and Information Protection became law. The Amendment provides for stricter

---

[250] Federal Law No. 87-FZ on Amendments to the Federal Law on Information, Information Technologies and Protection of Information and Certain Laws of the Russian Federation (2017).

[251] Gail Crawford and Ksenia Koroleva, *Russia Introduces New Definition and Obligations for Audiovisual Service Owners*, LATHAM & WATKINS GLOBAL PRIVACY AND SECURITY COMPLIANCE BLOG (July 20, 2017), http://www.globalprivacyblog.com/legislative-regulatory-developments/russia-introduces-new-definition-and-obligations-for-audiovisual-service-owners/.

[252] The restrictions are also dependent on the Russian audience size of the service. If more than 50% of the service's users are Russian users, then there is no restriction on foreign ownership. If less than 50% of the service's users are Russian users and they have greater than 20% foreign ownership, the service needs approval of a government commission.

[253] Dmitri Nikiforov et al, *Client Update: New Regulation of Online Cinemas in Russia*, DEBEVOISE & PLIMPTON (May 31, 2017), https://www.debevoise.com/~/media/files/insights/publications/2017/05/20170531en_new_regulation_of_online_cinemas_in_russia.pdf.

penalties in the case of a data breach than were originally provided for in the Act, in addition to heavy fines for noncompliant overseas transfer of information.[254] U.S. tech firms have been threatened with investigations and fines for not complying with the more stringent regime, even though the data at issue is not subject to South Korea's physical jurisdiction. The extraterritorial enforcement of South Korean laws forces these firms to adjust the way they operate both in South Korea and globally.

O. Thailand

Filtering and Blocking

In December 2016, Thailand's National Legislative Assembly passed amendments to the 2007 Computer Crime Act.[255] The amendments became effective earlier this year and five Ministerial Notifications were issued in August outlining regulations and procedures pursuant to the amendments to the Act.[256] These changes greatly expanded the authority of the Thai government to regulate content online.[257] Among the changes is the creation of a "Computer Data Filtering Committee" comprised of five individuals with the power to obtain court approval to block a website that is contrary to the "good morality" of the people or violation of public order.[258]

The government regularly blocks social media accounts of users that criticize the royal family under *lèse-majesté* laws, an action that has increased since the 2014 military coup. In

---

[254] Colleen Theresa Brown, Yuet Ming Tham, Samuel Yim, *South Korea Enacts Stricter Penalties for Data Protection Violations by Telecommunications and Online Service Providers*, SIDLEY AUSTIN LLP DATA MATTERS (Apr. 22, 2016), http://datamatters.sidley.com/south-korea-enacts-stricter-penalties-for-data-protection-violations-by-telecommunications-and-online-services-providers/.

[255] Computer Crime Act B.E. 2550 (2007).

[256] Dhiraphol Suwanprateep, *Five Ministerial Notifications Under the Computer Crime Act Finally Come into Forc*e, BAKER MCKENZIE (Aug. 4, 2017), http://www.bakermckenzie.com/en/insight/publications/2017/08/five-ministerial-notifications/.

[257] Further, the amendments lack clarity with respect to what constitutes illegal content or an offensive online activity. Officials are given broad authority to judge the illegality of online activities of users based on vague offenses including distributing false information threatening national security or distributing obscene data. This will significantly impact users online, and human rights organizations have spoken out in response to the law. *See Thailand: Cyber Crime Act Tightens Internet Control*, HUMAN RIGHTS WATCH (Dec. 21, 2016), https://www.hrw.org/news/2016/12/21/thailand-cyber-crime-act-tightens-internet-control.

[258] Dhiraphol Suwanprateep, *Thailand: NLA Finally Approves Amendment to Thai Computer Crime Act*, BAKER MCKENZIE (Dec. 29, 2016), http://www.bakermckenzie.com/en/insight/publications/2016/12/the-amendment-to-the-thai-computer.

2017, the government asked Facebook to block over 300 posts from users compared to the 80 blocking instances from mid-2014 to the end of 2016.[259] The government is also developing legislation to further expand government surveillance powers to enforce such laws.[260]

Legal Liability for Online Intermediaries

The lack of intermediary liability protections in Thailand has long been a concern to service providers. A notable case in 2012 involved a criminal conviction under Thailand's Computer Crimes Act of a webmaster whose only crime was "failing to quickly delete posts considered insulting to Thailand's royal family."[261] The 2016 amendments only furthered this trend. While the recent amendments created a safe harbor for service providers for the first time in Thai law, the mandated timeframes for removal vary across content types.[262] Without strict compliance with the notification requirements,[263] the service provider will be subject to the same penalty as if they uploaded the content themselves.[264]

---

[259] Patpicha Tanakasempipat, *Thailand Plans Cyber Network Scrutiny, Law to Toughen Online Monitoring*, U.S. NEWS (June 19, 2017), https://www.usnews.com/news/world/articles/2017-06-19/thailand-plans-cyber-network-scrutiny-law-to-toughen-online-monitoring.

[260] Wendy Zeldin, *Thailand: New, Tough Law on Cyber Security Drafted*, LIBRARY OF CONGRESS (July 21, 2017), http://www.loc.gov/law/foreign-news/article/thailand-new-tough-law-on-cyber-security-drafted/ ("The cyber security bill calls for the establishment of a National Cyber Security Committee, led by Prayuth Chan-ocha, interim Prime Minister. The Committee would have the broad authority to order public agencies and private businesses alike to assist in cyber security investigations."); *Id*. ("[T]he authorities would be empowered 'to order anyone to report for questioning or hand over information' and 'to tap all communication devices including phones and computers in 'emergency cases,' without court approval.'").

[261] James Hookway, *Conviction in Thailand Worries Web Users*, WALL ST. J. (May 30, 2012), http://online.wsj.com/article/SB10001424052702303674004577435373324265632.html (noting that this "sets a concerning precedent for prosecuting website owners for what their users say online."). *See also* Ctr. for Democracy & Technology, Comments on Thailand's Proposed Computer-Related Offenses Commission Act, (March 2012), *available at* https://cdt.org/files/pdfs/Comments-Thailand-CCA-Draft.pdf.

[262] Dhiraphol Suwanprateep, *Five Ministerial Notifications Under the Computer Crime Act Finally Come into Force*, BAKER MCKENZIE (Aug. 4, 2017), http://www.bakermckenzie.com/en/insight/publications/2017/08/five-ministerial-notifications/.

[263] The procedures were laid out in a Ministerial Notification issues in August 2017. There are specific timelines during which providers must take down content, corresponding to different types of illegal content. In cases such as national security, the content must be removed within 24 hours. *See* Dhiraphol Suwanprateep, *Five Ministerial Notifications Under the Computer Crime Act Finally Come into Force*, BAKER MCKENZIE (Aug. 4, 2017), http://www.bakermckenzie.com/en/insight/publications/2017/08/five-ministerial-notifications/.

[264] Danny O'Brien and Gennie Gebhart, *The Amended Computer Crime Act and the State of Internet Freedoms in Thailand*, THE ELECTRONIC FRONTIER FOUNDATION (Dec. 21, 2016), https://www.eff.org/deeplinks/2016/12/amended-computer-crime-act-and-state-internet-freedoms-thailand ("While

P. Turkey

Filtering & Blocking

CCIA has previously noted barriers to social media such as Twitter and YouTube in Turkey,[265] which adopted laws in February 2014 "allowing it to 'preventively' block websites on such vague grounds as the presence of content that is 'discriminatory or insulting towards certain members of society.'"[266] The recent unrest in Syria, and subsequent attempted coup of Turkey's government, has led to further government censorship, with Turkish authorities recently censoring websites and Twitter accounts accused of spreading Kurdish propaganda, including journalism sites.[267]

In June 2016, Turkey passed a law featuring an "Internet kill switch", which allows Turkey's Information and Communication Technologies authority to "partially or entirely" suspend Internet access due to war or in matters related to national security, without seeking ministerial oversight first.[268] Use of this law may have led to immediate shutdowns of various social media sites in Turkey.[269]

This past June, Cloudflare was taken offline making multiple popular websites hosted on the Cloudflare content delivery network unavailable.[270] While the underlying causes were not

---

that may be seen as relieving the pressure on ISPs, putting the burden of proof on them will actually result in more censorship—whether intermediaries take down content at the state's request or preemptively censor themselves and their users to avoid state scrutiny.").

[265] Joe Parkinson *et al*., *Turkey's Erdogan: One of the World's Most Determined Internet Censors*, WALL ST. J. (May 2, 2014), http://online.wsj.com/articles/SB10001424052702304626304579505912518706936.

[266] Reporters Without Borders, *Turkey, Enemy of the Internet?* (Aug. 28, 2014), http://en.rsf.org/turquie-turkey-enemy-of-the-internet-28-08-2014,46856.html; Emre Peker, Joe Parkinson & Sam Schechner, *Google, Others Blast Turkey Over Internet Clampdown*, WALL ST. J. (Apr. 1, 2014), http://online.wsj.com/articles/SB10001424052702303978304579473190997035788.

[267] Zeynep Karataş, *Ongoing Censorship Blocks Kurdish, Critical, Data-based Media During Time of Crisis*, TODAY'S ZAMAN (Aug. 15, 2015), http://www.todayszaman.com/anasayfa_ongoing-censorship-blocks-kurdish-critical-data-based-media-during-time-of-crisis_396569.html.

[268] *Social Media Blocked in Turkey*, TURKEY BLOCKS (Aug. 25, 2016), https://turkeyblocks.org/2016/08/25/social-media-blocked-turkey/.

[269] *Id*.

[270] *Major Internet Access Issues in Turkey as Cloudflare Knocked Offline*, TURKEY BLOCKS (June 5, 2017), https://turkeyblocks.org/2017/06/05/major-internet-access-issues-turkey-cloudflare-knocked-offline/.

clear, "similar issues have previously been connected to attempts by [Turkish] authorities to block individual websites or filter specific content."[271]

Q. Ukraine

Legal Liability for Online Intermediaries

Ukraine adopted "On State Support of Cinematography in Ukraine" in March 2017 which established a notice and takedown system for copyright enforcement.[272] However, the final law goes beyond what the notice and takedown system under Section 512 of the DMCA 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 who can devote entire departments to takedown compliance, but will effectively deny market access to smaller firms and startups, and are inconsistent with the "expeditious" standard under U.S. copyright law.[273] 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. This is inconsistent with Section 512 of the DMCA, parallel FTA provisions, and article 15 of the 2000 EU E-Commerce Directive.

R. Vietnam

Forced Data Localization and Intermediary Liability

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

---

[271] *Id*.

[272] Law of Ukraine No. 1977-VIII of March 23, 2017, on State Support of Cinematography in Ukraine, (translation *available at* http://www.wipo.int/wipolex/en/text.jsp?file_id=438250).

[273] 17 U.S.C. § 512(1)(C).

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.

The Vietnamese authorities are also considering other forms of forced localization. For instance, the draft decree on IT services would require offshore web-based services to establish a local representative in the country in order to continue providing the service to Vietnamese companies and individuals. A recent proposal from the Vietnamese government involved "banning people from copying and pasting news articles and other information on blogs—which could restrict the growth of informal news portals," noting that Vietnam's Communist rulers are subjected to criticism online. Government officials denied any intent to limit free speech, indicating that they aimed to "manage" growth and "protect intellectual property."[274]

Vietnam's Decree No. 55 also contains provisions that require Internet exchange providers, "ISPs, online service providers (OSPs), ICPs, and Internet service agents to act as gatekeepers in adopting appropriate measures to block the prohibited content defined under the Press Law and the Publication Law, among others."[275] This prohibited content includes behaviors that are, in the law's words, "seditious, libelous, defamatory, obscene and violent, and those that constitute hate speech or disclose State secrets."[276]

Undue Restrictions on Rich Interaction Applications (RIAs)

In October 2014, Vietnam's government released a draft "Circular on Managing the Provision and Use of Internet-based Voice and Text Services" that proposed unreasonable restrictions on VoIP and Internet Based Text Services provided over IP broadband connections.[277] These restrictions would require foreign providers of RIAs to install a local server to store data or enter into a commercial agreement with a Vietnam-licensed

---

[274] James Hookway, *Vietnam Rights Record Cools U.S. Ties*, WALL ST. J. (Aug. 8, 2013), http://online.wsj.com/article/SB10001424127887323838204579000160962041046.html.

[275] Thuy Nguyen, *Online Intermediaries Case Studies Series: Roles and Liabilities of Online Intermediaries in Vietnam – Regulations in the Mixture of Hope and Fear*, THE GLOBAL NETWORK OF INTERNET & SOCIETY RESEARCH CENTERS, at 8 (2015) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566364.

[276] *Id*. at 3.

[277] *Circular Regulates OTT Services*, VIET NAM NEWS (Nov. 15, 2014), http://vietnamnews.vn/economy/262825/circular-regulates-ott-services.html.

telecommunications company. In addition, foreign providers of RIAs would only be permitted to place a server in Vietnam through cooperation with Vietnam's telecommunications companies. Such requirements are significant market access barriers for foreign competitors that seek to supply Internet-based services in Vietnam, and may be designed to raise the costs of rivals providing service in Vietnam.

IV. CONCLUSION

As numerous studies have pointed out,[278] Internet platforms and services empower small and medium-sized businesses to participate in international trade like never before. Therefore, positive efforts on the digital trade front will also expand the base of U.S. and foreign exporters that directly benefit from U.S. trade policy.

As the global Internet continues to grow and becomes even more tightly intertwined with international commerce, CCIA worries that — if left unchecked — digital trade barriers like those discussed above will continue to proliferate. To push back against these barriers, U.S. trade policy and enforcement priorities must continue to reflect the large and growing importance of the Internet to the U.S. economy and U.S. trade performance. CCIA welcomes USTR's deepened focus on barriers to digital trade which we hope will be reflected in this year's NTE.[279]

October 25, 2017

---

[278] *See, e.g.*, Andreas Lendle, *et al*., *There Goes Gravity: How eBay Reduces Trade Costs*, THE WORLD BANK POVERTY REDUCTION AND ECONOMIC MANAGEMENT NETWORK INTERNATIONAL TRADE DEPARTMENT (Oct. 2012), http://wwwwds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2012/10/25/000158349_20121025161729/Rendered/PDF/wps6253.pdf; *see also* Matthieu Pélissié du Rausas *et al*., *Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity*, MCKINSEY GLOBAL INSTITUTE (2011), http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

[279] *See 2017 Key Barriers to Digital Trade*, *supra* note 2.