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. 2018 - 0029

COMMENTS OF THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION REGARDING FOREIGN TRADE BARRIERS TO U.S. EXPORTS FOR 2019 REPORTING

October 30, 2018

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 83 Fed. Reg. 42,966 (Aug. 24, 2018), 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. The U.S. International Trade Commission 2018 Trade in Services Report illustrated how e-commerce is a key driver to U.S. trade. Value added by the U.S. electronic services sector was $989.0 billion, and the sector accounted for 6.9 % of U.S. private sector GDP in 2016.[1] Further, the United States exported $439.1 billion and imported $266.6 billion in digitally deliverable services, resulting in a trade surplus of $172.5 billion.[2]

However, in recent years countries have begun to adopt laws and regulations that hinder the further growth and 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 recommendations to continue positive dialogue with key trading partners as exemplified in the U.S.-Mexico-Canada Agreement (USMCA). Second, the comments provide a general overview of the following 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, (f) undue restrictions on "rich interaction applications", and (g) inappropriate taxation of online services. 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.

[1] U.S. INT'L TRADE COMM'N, *Recent Trends in U.S. Services Trade: 2018 Annual Report*, *available at* https://www.usitc.gov/publications/332/pub4789.pdf (2018) [hereinafter "2018 Recent Trends in U.S. Services Trade*"*].

[2] BUREAU OF ECON. AFFAIRS, U.S. Trade in ICT and Potentially ICT-Enabled Services, https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=6&isuri=1&tablelist=357&product=4 (last updated Oct. 19, 2018).

Table of Contents

I. INTRODUCTION

CCIA represents technology products and services providers of all sizes, including computer hardware and software, electronic commerce, and telecommunications and Internet products and services. CCIA members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.[3]

CCIA thanks USTR for highlighting digital trade as a key priority for the Administration in the 2018 NTE,[4] 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.[5] 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.[6] 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. Internet-enabled commerce represents a significant, yet still growing, sector of the global economy. From 2012 to 2016, global e-commerce grew 44% from $19.3 trillion to $27.7 trillion.[7]

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.[8] Today, seven of those leading brands are U.S.-based,[9] vying for over 4

---

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

[4] OFFICE OF THE U.S. TRADE REP., 2018 National Trade Estimate Report on Foreign Trade Barriers [hereinafter "2018 NTE"].

[5] *See* OFFICE OF THE U.S. TRADE REP., *Key Barriers to Digital Trade* (Mar. 2018), https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital ("In this year's National Trade Estimate (NTE), USTR maintains and deepens its focus on barriers to digital trade, a critical element of U.S. competitiveness and a key source of U.S. innovation and growth.") [hereinafter "2018 Key Barriers to Digital Trade"].

[6] In the cloud computing industry alone, four U.S.-based companies (Amazon Web Services, Microsoft, IBM, and Google) furnish more than half of the cloud computing services consumed worldwide. This dominance is projected to grow. For example, Amazon Web Services' third quarter revenue jumped from $2.56 billion in 2016 to $3.66 billion 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.

[7] U.S. INT'L TRADE COMM'N, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions* (Aug. 2017), available at https://www.usitc.gov/publications/332/pub4716_0.pdf.

[8] Mary Meeker, *Internet Trends 2014*, at 130 (2014), http://www.kpcb.com/blog/2014-internet-trends.

billion Internet users across the world.[10] In 2016 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.[11] Today, China's share is 39% compared to 18% for the United States.[12]

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.[13]

The United States must retain its advantage 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.

The USMCA is a prime example of steps that the Administration can take to update U.S. trade policies and priorities for the digital era, but more work needs to be done 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.[14]

---

[9] Mary Meeker, *Internet Trends 2018*, at 218 (2018), https://www.slideshare.net/kleinerperkins/internet-trends-report-2018-99574140.

[10] *Internet Live Stats*, http://www.internetlivestats.com/internet-users/ (last visited Sept. 19, 2018).

[11] 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/).

[12] James Cook, *China is Dominating the App Store*, BUSINESS INSIDER (Mar. 1, 2018), https://www.businessinsider.com/china-is-dominating-the-app-store-2018-3.

[13] 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 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.").

[14] BUREAU OF LABOR STATISTICS, Current Employment Statistics, Employees on Nonfarm Payrolls by Industry Sector (last modified Oct. 5, 2018), http://www.bls.gov/web/empsit/ceseeb1a.htm.

Meanwhile, the United States is the largest global exporter of services, exporting $761.7 billion in 2017.[15] 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.[16] The U.S. trade agenda should recognize these trends and commit to removing barriers in the delivery of such services. Value added by the U.S. electronic services sector was $989.0 billion, and the sector accounted for 6.9% of U.S. private sector GDP in 2016. Further, the United States exported $93.4 billion in cross-border electronic services and imported $54.3 billion, resulting in a trade surplus of $39.1 billion.[17] When digitally deliverable services are factored in, the U.S. digital trade surplus balloons to $172 billion[18] — and this surplus would be even higher if digital advertising services (and other software services) were fully captured in government trade statistics.[19]

Digital trade and trade liberalization generally is threatened when countries adopt protectionist policies, and utilize tools that undermine the benefits of free trade and impede global economic growth.

CCIA encourages USTR to instead continue engagement with key trading partners and foster positive dialogues. The preliminary discussions with the UK, EU, and Japan are encouraging and strong digital trade outcomes in these negotiations would further strengthen these trading relationships.[20] The Administration would miss a key opportunity with three of our most important trading partners if digital trade was not included in these negotiations.

CCIA also applauds USTR's work to update existing trade agreements to better reflect the digital economy. 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

---

[15] *2018 Recent Trends in U.S. Services Trade*, *supra note* 1.

[16] *Id*.

[17] *Id*.

[18] BUREAU OF ECON. AFFAIRS, U.S. Trade in ICT and Potentially ICT-Enabled Services, *available at* https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=6&isuri=1&tablelist=357&product=4 (last updated Oct. 19, 2018).

[19] BEA notes that their estimates "captures the output of these service providers as intermediate consumption of the unit that pays for the advertising" but that "the initial digital economy estimates published by BEA in March 2018 do not include this revenue" and "BEA currently does not have the data needed to identify what portion of advertising revenue is associated with these websites." BUREAU OF ECON. AFFAIRS, Frequently Asked Questions, https://www.bea.gov/help/faq/1250 (last visited Oct. 29, 2018).

[20] Press Release, Office of the U.S. Trade Rep., Trump Administration Announces Intent to Negotiate Trade Agreements with Japan, The European Union and the United Kingdom (Oct. 16, 2018), https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/october/trump-administration-announces.

been a net economic success for the United States,[21] a modern overhaul is much needed for the 24-year-old agreement to factor in the growth of the digital economy and the strong digital trade relationship the U.S. enjoys with Mexico and Canada.[22] The new United States-Mexico-Canada Agreement (USMCA) represents significant progress in facilitating a more robust North American trading partnership.[23] This is particularly true with respect to sections that are critical to the digital economy.[24] Positive provisions include intermediary protections for third-party content, restrictions on data localization, source code protection, and an intermediary liability framework for copyrighted content consistent with U.S. law.[25] USMCA has also advanced the competition policy section to cover due process related matters.

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 2018 NTE Report and encourages USTR to continue to highlight digital trade barriers in the 2019 Report.

---

[21] U.S. CHAMBER OF COMMERCE, *NAFTA Works for America*, https://www.uschamber.com/nafta-works (last visited Oct. 30, 2018) (noting that trade with Canada and Mexico supports 14 million American jobs and nearly four million of those jobs are supported by the increase in trade generated by NAFTA); Amanda Waldron, *NAFTA 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.").

[22] The Bureau of Economic Analysis at the U.S. Department of Commerce released a study in 2018 on the value of digital trade in North America, highlighting just what was at stake in the renegotiation of NAFTA. The BEA's report estimates the value of this industry by examining the international trade of information and communications technology (ICT) services and "potentially" ICT-enabled (PICTE) services — "services that can be traded remotely using the internet or some other digital network." U.S. PICTE services trade in total was $403.5 billion in exports and $244.0 billion in imports. U.S. PICTE service exports to Canada totaled $27.8 billion, accounting for 52 % of all U.S. service exports to Canada. PICTE exports to Canada grew at an annual growth rate of 4% from 2006 to 2016. U.S. PICTE service exports to Mexico totaled $8.8 billion, accounting for 27 % of U.S. service exports to Mexico. PICTE exports to Mexico grew at an annual rate of 5.5. % from 2006 to 2016. These numbers show that almost half of all services traded from the U.S. to Canada and Mexico are likely delivered through cross-border data flows. This confirms that the growth of digitally-enabled services is critical to the trading relationship with our North American partners. *See* U.S. DEPT. OF COMMERCE, Fact Sheet, Digital Trade in North America (Jan. 5, 2018), https://www.commerce.gov/news/fact-sheets/2018/01/digital-trade-north-america.

[23] OFFICE OF THE U.S. TRADE REP., U.S.-Mexico-Canada Agreement Text, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/united-states-mexico [hereinafter "USMCA"].

[24] Press Release, CCIA Welcomes Provisions in Canada, Mexico Trade Agreement to Reduce Digital Trade Barriers (Oct. 1, 2018), http://www.ccianet.org/2018/10/ccia-welcomes-provisions-in-canada-mexico-trade-agreement-to-reduce-digital-trade-barriers/.

[25] OFFICE OF THE U.S. TRADE REP., United States-Mexico Trade Fact Sheet: Modernizing NAFTA into a 21st Century Agreement, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/august/united-states%E2%80%93mexico-trade-fact-sheet-1.

II. PROMINENT DIGITAL TRADE-RELATED BARRIERS

A. Data and Infrastructure Localization Mandates

Open data flows are critical for continued global economic growth.[26] As CCIA has noted in previous NTE filings,[27] a number of countries continue to pursue data localization policies, including mandated server localization and data storage.[28] In a 2017 report, the ITC included estimates that such localization measures have doubled in the last six years.[29] 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.[30] 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

---

[26] MCKINSEY GLOBAL INSTITUTE, *Digital Globalization: The New Era of Global Flows* (2016), *available at* https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-ofglobal-flows (Global flows of all types support growth by raising productivity, and data flows are amplifying this effect by broadening participation and creating more efficient markets. MGI's analysis finds that over a decade, all types of flows acting together have raised world GDP by 10.1% over what would have resulted in a world without any cross-border flows. This value amounted to some $7.8 trillion in 2014 alone, and data flows account for $2.8 trillion of this impact.).

[27] 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. 2017-0013, filed Oct. 27, 2017, *available at* http://www.ccianet.org/wp-content/uploads/2017/10/CCIA-Comments-for-2018-NTE-1.pdf [hereinafter "CCIA 2018 NTE Comments']; 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.

[28] A study by the Information Technology & Innovation Foundation listed most of the world'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.

[29] 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"].

[30] 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.

decentralization over single points of failure.[31] Another concerning trend is in Latin American countries that are advancing legislation that will further restrict data transfer across borders.[32]

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.[33] Rather than promote domestic industry, data localization policies are likely to hinder economic development,[34] restrict domestic economic activity,[35] and impede global competitiveness.[36] Data localization policies are also frequently in violation of international obligations, including GATS commitments. To remain compliant with international

---

[31] 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.

[32] Panamá, Chile, Ecuador, Argentina, and Honduras have proposed or are considering legislation that would negatively impact U.S. exporters. These proposals seek to align their frameworks with that of the EU's General Data Protection Regulation but fail to consider the impact to the domestic market and implementation and compliance costs. Industry's reported concerns are directed at the extraterritoriality component of these provisions, an introduction of the "right to be forgotten", mandated express consent, and the need for prior authorization for international data transfer. *See Data Protection Regulation in Latin America and the Impact of the GDPR*, GARRIGUES (May 24, 2018), https://www.lexology.com/library/detail.aspx?g=9eef3453-f88e-442d-9c70-499021bed7da; *Latin America Privacy With GDPR As Model*, BAKER MCKENZIE (Feb. 26, 2018), https://www.intlprivacysecurityforum.com/wp-content/uploads/2018/02/LatAm_Privacy_with_GDPR_as_Model-v2.pdf.

[33] 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.

[34] *See* Leviathan Security Group, *Quantifying the Costs of Forced Localization* (2015), http://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/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). ECIPE: full data localization reduces GDP by 0.8% in Brazil, 1.1% in China, Korea, and the EU, 0.8% in India, 0.7% in Indonesia, and 1.7% in Vietnam.

[35] 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.

[36] 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 28 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.").

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.[37] 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.[38]

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.[39] Despite these costs, governments continue to filter and block Internet content, platforms, and 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 2017 report, Freedom House assessed that global Internet freedom declined for the sixth consecutive year due to government manipulation of Internet services, mobile Internet services shutdowns, and online censorship and monitoring practices.[40] It also reported that since June 2015, 34 out of the 65 countries assessed in the report have been on a negative trajectory[41] by increasing political censorship, prosecutions for speech, and surveillance. Freedom House's 2016 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.[42] The 2017

---

[37] 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).

[38] *See* Chander & Lê, *Data Nationalism*, *supra* note 30; 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"].

[39] 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.

[40] FREEDOM HOUSE, *Freedom on the Net 2017* (2017), https://freedomhouse.org/report/freedom-net/freedom-net-2017 [hereinafter "Freedom House 2017"].

[41] FREEDOM HOUSE, *Freedom on the Net* (2016), https://freedomhouse.org/sites/default/files/FOTN_2016_BOOKLET_FINAL.pdf [hereinafter "Freedom House 2016"] at 2.

[42] *Id*. at 1 ("Users in some countries were put behind bars 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.").

report highlighted an increase in government restrictions on live streaming on social media platforms.[43]

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.[44] 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.[45] Known offenders who use some or all of these practices have included Afghanistan, Burma, China, Cuba, Egypt, Guatemala, Indonesia, Iran, Kazakhstan, North Korea, Pakistan, Saudi Arabia, Syria, Tunisia, Turkey, Turkmenistan, Uzbekistan, and Vietnam.[46] 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.[47]

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.[48]

---

[43] *Freedom House 2017*, *supra* note 40, at 17.

[44] 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*].

[45] *Internet Fragmentation*, *supra* note 13.

[46] Darrell M. West, *Internet Shutdowns*, *supra* note 44; *Freedom House 2016 supra* note 41.

[47] *2014 Digital Trade in the U.S. and Global Economies, Part 2*, *supra* note 38, at 98.

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

As CCIA has previously stated,[49] 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.[50] 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 domestic startups.[51] While U.S. Internet businesses have thrived domestically under carefully crafted legal frameworks, international asymmetries in liability rules frequently favor domestic plaintiffs.[52]

International trade rules must be modernized in a manner that promotes liability rules that are consistent, clear, and work for Internet companies of all stages of development to encourage the export of Internet services. This approach to trade policy that recognizes the frameworks that have enabled the success of the Internet age will benefit developed and emerging markets alike. From the perspective of developed markets, predictability in international liability rules is increasingly important as domestic Internet markets are relatively saturated compared to international markets. Further growth and maturity is dependent on the ability to access and export to international markets.

---

[49] *CCIA 2018 NTE Comments*, *supra* note 27.

[50] *See generally* CCIA, *Modernizing Liability Rules to Promote Internet Trade* (2018), http://www.ccianet.org/wp-content/uploads/2018/07/Modernizing-Liability-Rules-2018.pdf.

[51] 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.

[52] 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).

Several major Internet companies already make up more than 50% of their revenue from markets outside their home markets.[53]

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. The USMCA illustrates a successful iteration of this policy.[54] 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.[55]

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. A 2017 study illustrated how U.S. firms operating abroad in regimes with balanced copyright law reported high incomes and increased total sales, encouraging foreign investment.[56] A CCIA study showed that in 2014 fair use industries accounted for 16% of the U.S. economy, employed 1 in 8 workers, and contributed $2.8 trillion to GDP.[57] Driven by increases in service-sector exports, U.S. exports of goods and services related to fair use increased by 21% from $304 billion in 2010 to $368 billion in 2014.[58] These economic benefits are lost when a country fails to uphold similar protections in their own copyright laws, impeding market access for U.S. companies looking to export while also deterring local innovation.

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

---

[53] Steve Goldstein, *S&P 500 Companies Generate Barely Over Half Their Revenue at Home*, MARKETWATCH (Aug. 19, 2015), https://www.marketwatch.com/story/sp-500- companies-generate-barely-over-half-their-revenue-at-home-2015-08-19.

[54] *USMCA*, *supra* note 23 at art. 19.17; *USMCA*, *supra* note 23 at art. 20.J.11.

[55] CCIA has further expanded on this issue in other consultations. *See* Comments of CCIA, *In re* 2018 Special 301 Review, Dkt. No. USTR-2017-0024, filed Feb. 8, 2018 [hereinafter "2018 CCIA Special 301 Comments"].

[56] Sean Flynn & Mike Palmedo, The User Rights Database: Measuring the Impact of Copyright Balance, Program on Information Justice and Intellectual Property (Oct. 30, 2017), http://infojustice.org/archives/38981.

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

[58] *Id*. at 6.

copyright balance, at least through the inclusion of intermediary protections.[59] USTR also stated in 2017 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."[60]

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.[61] While many of the countries outlined below and discussed in prior NTE Reports have either adopted or proposed strong copyright enforcement rules, fewer 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 2018 NTE described (discussed *infra* pp. 41), 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

[59] *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, 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.

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

[61] 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.").

notes, raise concerns from a trade perspective.[62] A recent USITC report also observed that these laws tend to have "generated unintended consequences" to small online publishers.[63] 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.[64] 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.

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.[65] 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 continued lack of compliance (discussed *infra* pp. 19 and pp. 33). USTR has highlighted failures to comply with trading

---

[62] *2018 NTE*, *supra* note 4, at 199-200; OFFICE OF THE U.S. TRADE REP., *2018 Fact Sheet: Key Barriers to Digital Trade* (2018), https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital.

[63] *2017 Global Digital Trade I*, *supra* note 29, 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.").

[64] By imposing a tax on quotations, these entitlements violate Berne Convention Article 10(1)'s mandate that "quotations from a work . . . lawfully made available to the public" shall be permissible. Berne Convention for the Protection of Literary and Artistic Works, Sept. 28, 1979, art. 10(1), amended Oct. 2, 1979. Moreover, if the function of quotations in this context – driving millions of ad-revenues generating Internet users to the websites of domestic news producers – cannot satisfy "fair practice", then the term "fair practice" has little meaning. Imposing a levy on quotation similarly renders meaningless the use of the word "free" in the title of Article 10(1). The impairment of the mandatory quotation right represents a TRIPS violation, because Berne Article 10 is incorporated into TRIPS Article 9. *See* TRIPS Agreement, art. 9 ("Members shall comply with Articles 1 through 21 of the Berne Convention (1971).") TRIPS compliance, in turn, is a WTO obligation. As TRIPs incorporates this Berne mandate, compliance is not optional for WTO Members.

[65] 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.

obligations and inadequate intermediary liability protections in past Special 301 Reports, indicating the importance of such projections to trade relations and should include these concerns in its upcoming NTE report.[66]

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.[67]

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 that are considering or have recently implemented anti-encryption laws include the United Kingdom, France, Germany, Australia,[68] Brazil, India, and China.[69] Russia has already imposed this requirement on companies operating in its jurisdiction through its "Yarovaya" laws.[70]

These exceptional access regimes run contrary to the consensus assessments of security technologists because they are technically and economically infeasible to develop and implement.[71] Companies already operating in countries that have or are considering anti-encryption laws will be

---

[66] 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").

[67] 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/.

[68] Jadzia Pierce, *Australia Proposes New Encryption Legislation*, INSIDE PRIVACY (Sept. 19, 2018), https://www.insideprivacy.com/international/australia-proposes-new-encryption-legislation/

[69] 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.

[70] 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.

[71] 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.

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.[72]

F. Undue Restrictions on "Rich Interaction Applications"

Several countries have proposed or implemented undue or unreasonable regulatory restrictions on rich interaction applications (RIAs)[73] — 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.[74] When regulating these services, foreign governments often refer to them as "over-the-top" or OTT services and presume that they impede local economic growth. However, a study has shown the vast economic and societal benefits stemming from the use of RIAs.[75] Global GDP has increased $5.6 trillion for every 10% increase in the usage of RIAs across 164 countries over 16 years (2000 to 2015).[76] 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.[77] Instead of raising regulatory barriers, Kenya has attempted to promote RIAs and other

---

[72] 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/.

[73] *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.

[74] 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.

[75] 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"].

[76] *Id*.

[77] *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.

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 therefore 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 can also help governments respond to emergencies and public health crises more quickly and accurately, and 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.[78] 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, which increasingly include mobile services but also include fixed broadband.[79] 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."[80] In addition, online services also present cost-saving and product-enhancement opportunities for telecommunication providers, such as the opportunity to substitute fully featured VoIP for circuit-switched voice.

G. Taxation of Digital Services

An alarming trend among foreign countries is the singling out of the U.S. digital economy for additional taxation. Often based on inaccurate estimates, some countries assert that digital services fail to pay adequate taxes and should be subject to additional taxation.[81] These proposals that have

---

[78] *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").

[79] *RIA Study*, *supra* note 75, at 19.

[80] *Id*.

[81] The European Centre for International Political Economy (ECIPE) released a study in February 2018 calculating the effective rate digital companies pay in taxes, and dispelling many myths that perpetuate the discussion on digital taxation. The study finds that digital companies pay between 26.8% to 29.4%, on average. *See* ECIPE, *Digital Companies and Their Fair Share of Taxes: Myths and Misconceptions* (Feb. 2018), *available at* http://ecipe.org/publications/digital-companies-and-their-fair-share-of-taxes/.

surfaced in the EU and elsewhere discourage foreign investment and are inconsistent with international treaty obligations. The United States should push back strongly on proposals that seek to disadvantage American companies.

Changes to international taxation may be warranted in the increasingly globalized economy, but these changes should not be carried out by disproportionately focusing on a single sector of the global economy, or by singling out U.S. digital services for unique treatment. If reform is needed to the international tax system, an international collaborative approach that considers all aspects of the changing global economy should be championed rather than a country-by-country approach. As the OECD noted in its report, "it would be difficult, if not impossible, to ring-fence the digital economy from the rest of the economy" and there is "no consensus on either the merit or need for interim measures" as contemplated by the EU.[82] CCIA welcomed Treasury Secretary Mnuchin's statements[83] encouraging this approach and would encourage USTR to echo these concerns in its 2019 NTE.[84]

III. COUNTRY-SPECIFIC CONSIDERATIONS

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

[82] OECD, Tax Challenges Arising from Digitilisation – Interim Report 2018, http://www.oecd.org/tax/tax-challenges-arising-from-digitalisation-interim-report-9789264293083-en.htm.

[83] Press Release, U.S. Dept. of Treasury, Secretary Mnuchin Statement on Digital Economy Taxation Efforts (Oct. 25, 2018) ("I highlight against our strong concern with countries' consideration of a unilateral and unfair gross sales tax that targets our technology and internet companies."); Secretary Mnuchin Statement on OECD's Digital Economy Taxation Report (Mar. 16, 2018) ("The U.S. firmly opposes proposals by any country to single out digital companies. Some of these companies are among the greatest contributors to U.S. job creation and economic growth. Imposing new and redundant tax burdens would inhibit growth and ultimately harm workers and consumers. I fully support international cooperation to address broader tax challenges arising from the modern economy and to put the international tax system on a more sustainable footing.").

[84] The G7 also recognized this as the preferred approach in its 2018 communique. The Charlevoix G7 Summit Communique (June 9, 2018), https://www.reuters.com/article/us-g7-summit-communique-text/the-charlevoix-g7-summit-communique-idUSKCN1J5107 ("In order to ensure that everyone pays their fair share, we will exchange approaches and support international efforts to deliver fair, progressive, effective and efficient tax systems. We will continue to fight tax evasion and avoidance by promoting the global implementation of international standards and addressing base erosion and profit shifting. The impacts of the digitalization of the economy on the international tax system remain key outstanding issues. We welcome the OECD interim report analyzing the impact of digitalization of the economy on the international tax system. We are committed to work together to seek a consensus based solution by 2020.").

A. Argentina

Additional Barriers to E-Commerce

Industry has expressed difficulties with Argentina's recently reformed import policies set out in the Comprehensive Import Monitoring System.[85] The new system established three different low-value import regimes: "postal", "express", and "general." Due to continued challenges in clearing goods in the "general" regime, only the "express courier" is functional for e-commerce transactions.[86] However, industry reports that there are still limits within the "express" regime that make it difficult to export to Argentina and some U.S. companies have had to stop exporting to the Argentinian market completely.

There is another concerning trend regarding tax policies taking place in Latin America where many countries in the region are departing from international best practices and OECD principles through indirect taxes (VAT/GST) on cross-border supplies of electronically supplied services. For example, Argentina implemented a "Financial Intermediary" Tax Collection Model that creates an unleveled playing field. Argentina should be encouraged to instead employ the "Non-resident Registration" Tax Collection model. Countries including Chile, Colombia, and Costa Rica are considering following Argentina's approach. U.S. suppliers of these cross-border electronically supplied services report instances of double taxation in the region.

B. 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[87] 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.[88] 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

[85] Argentina Country Commercial Guide, Export.Gov, https://www.export.gov/apex/article2?id=Argentina-transparency-of-the-regulatory-system (last updated Nov. 20, 2017).

[86] Under the "express" regime, shipments are limited to packages under 50 kilograms and under $1000 and there is a limit of three of the same items per shipment (with duties and taxes assessed). The government limits the number of shipments per year per person to five and industry reports that this limitation is strictly enforced.

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

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

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.[89] This oversight was not addressed by passage of new amendments to Australia's Copyright Act,[90] which expanded intermediary protections to some public organizations but pointedly excluded commercial service providers including online platforms. These amendments specifically exclude U.S. digital services and platforms from the operation of the framework.[91] The failure to include online services such as search engines and commercial content distribution services disadvantages U.S. digital services in Australia and serves as a deterrent for investment in the Australian market.

Backdoor Access to Secure Technologies

This August, the Government of Australia unveiled a new proposal that would grant the country's national security and law enforcement agencies additional powers when confronting encrypted communications and devices.[92] Among other provisions, the draft bill authorizes the Australian government to use three new tools to seek or compel assistance from technology companies in accessing electronic communications information. These tools are technical assistance requests (TARs), which seek voluntary assistance from communications providers; and technical assistance notices (TANs) and technical capability notices (TCNs). Both call upon providers to do one or more specified acts which could include building new technical capabilities as required by the Attorney-General. While the legislation specifically forbids a notice to provide a "systemic weakness or vulnerability" into an encrypted system, it does provide sufficiently broad authority to

[89] 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.

[90] Copyright Amendment (Disability Access and Other Measures) Bill 2017, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5832. *See also* Jonathan Band, *Australian Copyright Law Thumbs Nose at U.S. Trade Commitments*, DISRUPTIVE COMPETITION PROJECT (July 6, 2018), http://www.project-disco.org/intellectual-property/070518-australian-copyright-law-thumbs-nose-at-u-s-trade-commitments/.

[91] *Id*.

[92] The Assistance and Access Bill 2018, https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018.

undermine encryption through other technical means with little oversight. Australia, despite opposition from civil society[93] and industry, intends to move forward with the bill.

Taxation of Digital Services

The Australian Treasury Office issued a discussion paper in October that contemplates changes to its domestic tax regime and "explores options to move towards a fairer and more sustainable tax system for the digitalized economy." While the paper mentions engagement through the multilateral process through the OECD and the G20 for a long-term solution, the paper also considers including a digital services tax similar to that of the EU's interim proposal.[94] Any "interim" solution proposed by individual countries would only serve to discourage foreign investment by offering a non-permanent additional taxation regime that singles out the digital economy.

C. Brazil

Brazilian policymakers have implemented policies which prevent 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;[95] (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;[96] or (c) the CERTICS Decree implemented to check whether software programs are the result of Brazilian innovation.[97] Brazil is also home to various local content requirements, filtering obligations, and tax incentives for locally-sourced ICT goods.[98] 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

[93] Letter to Australian Government (July 17, 2018) (global coalition led by civil society and technology experts calling government to reject plans to undermine encryption), https://www.accessnow.org/cms/assets/uploads/2018/07/Australia-Encryption-Coalition-Letter.pdf.

[94] THE TREASURY, *The Digital Economy and Australia's Corporate Tax System* (Oct. 2018), https://static.treasury.gov.au/uploads/sites/1/2018/10/c2018-t306182-discussion-paper-1.pdf at 20, 24.

[95] 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).

[96] Pursuant to Presidential Decree 8135 of November 5, 2013 and subsequent Ordinances (No. 141 of May 2, 2014, and No. 54 of May 6, 2014), Brazil's federal agencies must procure these services from "federal public entities" including the Serviço Federal de Processamento de Dados (or "Serpro") — the largest government-owned corporation of IT services in Brazil. While the government announced in 2016 that Decree 8135 would be revoked, actual revocation has not taken place and industry reports significant uncertainty.

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

[98] Passed in 2014, the Marco Civil imposed restrictions on cross-border data flows.

below, will help increase international trade of information and communications technology goods and equipment, thereby allowing more U.S. tech companies to do business in Brazil.

Data Localization

Brazil continues to adopt policies that mandate data localizations and restrict cross-border data flows. The Institutional Security Office of Brazil (GSI) revised its cloud guidelines and determined that government data should have localize at least some types of data. This precedent raises serious concerns. Other localization barriers reported include tax incentives for locally sourced information and communication technology (ICT) goods and equipment,[99] government procurement preferences for local ICT hardware and software,[100] and non-recognition of the results of conformity assessment procedures performed outside of Brazil for equipment connected to telecommunications networks.[101]

Filtering & Blocking

Judicial orders to intermediaries to temporarily or permanently block certain application or service is a common practice in Brazil.[102] Since 2012, Internet services such as YouTube, Facebook, WhatsApp, and Secret have all been affected by these orders.[103] 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.[104] 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."[105] Fortunately, the decision was reversed by an appellate court, citing the

[99] Basic Production Process (PPB) – Law 8387/91, Law 8248/91, and Ordinance 87/2013.

[100] 2014 Decrees 8184, 8185, 8186, 8194, and 2013 Decree 7903.

[101] ANATEL's Resolution 323.

[102] "Based on the review of the legal issues underlying the decisions, a report illustrated that a common threat is the scenario of "regulatory disruption" which is used to "refer to a context of lack of convention on how to solve a legal conflict, either because current regulations fails to deal with a new set of facts posed or affected by technology or because the prima facie applicable legal regime is in contradiction with policy considerations and/or outdated in light of new technologies. Jacqueline de Souza Abreu, *Disrupting the Disruptive: Making Sense of App Blocking in Brazil*, INTERNET POLICY REVIEW (July 2018), *available at* https://policyreview.info/node/928/pdf at 4.

[103] *Id*.

[104] 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 [hereinafter "Watts"].

[105] 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.

disproportionate impact caused by shutting down the whole service over a local investigation.[106] 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.[107] Nevertheless, the May 2016 WhatsApp ban cost the Brazilian economy an estimated $39 million in just one day.[108]

The Supreme Court of Brazil held public hearings in 2017 to further address the issue of banning secure communications technologies, but it is not clear whether Brazil will take steps to stop this practice and reign in control of the judiciary in issuing blocking orders.[109] 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. This level is not commercially significant. The low threshold increases the time and cost of the customs clearance process for businesses of all size and serves as an e-commerce barrier. It also does not apply to business-to-consumer or business-to-business transactions.[110] 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.

D. Canada

While an updated trilateral agreement with our North American trading partners will reduce barriers, some challenges remain for U.S. Internet exporters in Canada.

---

[106] Watts, *supra* note 104.

[107] *Id*.

[108] Darrell M. West, *Internet Shutdowns*, *supra* note 44, at 9.

[109] 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/.

[110] Decree No. 1804 of 1980 and Ministry of Finance Ordinance No. 156 of 1999; Export.gov Brazil Country Commercial Guide (last updated June 29, 2017), https://www.export.gov/article?id=Brazil-Express-Delivery.

Data Localization

The Canadian federal government has endeavored to consolidate information and communications technology services across dozens of Canadian federal entities into a single central agency called "Shared Services Canada."[111] 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.[112] 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. With the exceptions provided for in the USMCA, it is uncertain whether these will be affected.

Intermediary Liability

Rulings regarding intermediary responsibility that have extraterritorial effects present a significant barrier to trade by creating significant market uncertainty for companies seeking to host user content and communications on a global basis. In *Equustek Solutions v. Jack*, Google was compelled by the Supreme Court of British Columbia to remove—from all its domains worldwide—indexes and references to the website of Datalink, a competitor to Equustek that had been found to have violated Canadian trade secrets and consumer protection laws.[113] Following two unsuccessful Canadian appeals, Google successfully obtained permanent injunctive relief in the United States District Court in the Northern District of California, which held that the Canadian order could not be enforced in the United States because it undermined U.S. law and free speech on the Internet.[114]

---

[111] Comments of the Computer & Commc'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"].

[112] 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.

[113] Equustek Sols. v. Jack, [2014] B.C.S.C. 1063, https://www.canlii.org/en/bc/bcsc/doc/2014/2014bcsc1063/2014bcsc1063.pdf.

[114] Google v. Equustek Sols., No. 5:17-cv-04207-EJD, 2017 U.S. Dist. LEXIS 206818 (N.D. Cal. Dec. 14, 2017); *but see* Google v. Equustek Sols., [2017] 1 S.C.R. 824, https://scc-csc.lexum.com/scc-csc/scccsc/en/item/16701/index.do (earlier holding that the Canadian worldwide interlocutory injunction against Google should be upheld).

However, the Canadian Supreme Court has refused to amend the injunction in light of the U.S. judgment.[115]

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.[116] This de minimis level — the lowest among major U.S. trading partners[117] — 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.[118] 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 threshold and align the three trading partners to better facilitate digital trade and empower small business.[119] While there is some improvement with the new USMCA deal, more can be done to address inequalities to U.S. exporters.

[115] Equustek Solutions Inc. v. Jack *et al*., 2018 BCSC 610, http://www.courts.gov.bc.ca/jdb-txt/sc/18/06/2018BCSC0610.htm.

[116] 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.

[117] *2017 Global Digital Trade I*, *supra* note 29 at 310.

[118] *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.").

[119] *CCIA NAFTA Comments*, *supra* note 111, 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.").

E. Chile

Taxation of Digital Services

A bill has been introduced in Congress that includes a digital tax for services provided by foreign companies to Chilean individuals.[120] It is being discussed in the Lower Chamber. In a speech to Congress, the Chilean Minister of Finance established that this is a new specific tax, as opposed to a modification of the current VAT system.[121] As with the similar digital tax proposals in the EU and Colombia, this tax will likely have a disproportionate impact on U.S. firms and raises the risk of double taxation.

F. 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 have businesses growing more concerned and hesitant to enter the Chinese market, costing American firms. AmCham China's survey of its members showed that 75% felt less welcome in China in 2017 citing inconsistent regulatory interpretation and unclear laws as the primary challenge to doing business in China.[122] The survey also showed that 33% of its members said the investment environment was deteriorating — up from last year's 31% which was the most dire response AmCham has received from its members since it started asking the question in 2011.[123] Numerous scholars argue that China's actions violate WTO rules mandating open access and equitable treatment between foreign and domestic firms.[124]

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,

---

[120] *Chile Proposes Tax Reform*, ERNST & YOUNG (Aug. 29, 2018), https://www.ey.com/gl/en/services/tax/international-tax/alert--chile-proposes-tax-reform.

[121] Press Release, Chile Ministry of Finance, Minister of Finance: "We want to focus on the challenges that the Chilean tax system will face in the 21st century" (Aug. 24, 2018), http://www.hacienda.cl/english/press-room/news/archive/minister-of-finance-we-want-to-focus.html.

[122] AMCHAM CHINA, *China Business Climate Survey Report 2018*, https://www.amchamchina.org/policy-advocacy/business-climate-survey/.

[123] *Id.*; 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.

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

and innovation are actionable under the Trade Act.[125] 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.[126] 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."[127] China, along with Taiwan, Turkey, and India, also implement local-presence requirements for processing of payment transactions.[128]

Similarly, discriminatory practices are also prevalent in Chinese information technology industries. As USTR has previously noted,[129] foreign companies operating in cloud computing are forced to enter into joint partnerships with Chinese firms if they wish to conduct business within China,[130] 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.[131]

---

[125] 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).

[126] 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.

[127] 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.

[128] *2014 Digital Trade in the U.S. and Global Economies, Part 2*, *supra* note 38, at 86.

[129] *2018 Key Barriers to Digital Trade*, *supra* note 5 ("China severely restricts investment in cloud computing services, which affects companies that supply cloud computing services and those that need to source such services.").

[130] 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.

[131] 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.

China seeks to further restrain foreign cloud service operators, in concert with its national plan to promote the Chinese cloud computing industry.[132] U.S. cloud service providers are worldwide[133] leaders and are strong U.S exporters.[134] The International Trade Administration estimated that there was a surplus of cloud computing services of approximately $18 billion in 2015.[135] China has adopted discriminatory practices against U.S. cloud service providers with increasing frequency in recent years. There are two draft regulations that threaten to significantly disadvantage U.S. providers issued by the Ministry of Industry and Information Technology (MIIT): Regulating Business Operation in Cloud Services Market (2016) and Cleaning Up and Regulating the Internet Access Service Market (2017).[136] These proposals, together with existing licensing and foreign direct investment restrictions on foreign exporters in China, would require foreign cloud service providers to turn over essentially all ownership and operations to a Chinese company – including valuable U.S. intellectual property and know-how to China.[137] These measures are fundamentally protectionist and anticompetitive, threaten to further discourage foreign investment, and are in contrast with China's WTO commitments and separate commitments to the United States.

Foreign access to the cloud computing market is also restricted under the guise of strengthening cybersecurity.[138] In 2016, China passed three piece of anticompetitive legislation

[132] 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.

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

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

[135] U.S. DEPT. OF COMMERCE, 2017 TOP MARKETS REPORT CLOUD COMPUTING, *available at* https://www.trade.gov/topmarkets/pdf/Sector%20Snapshot%20Cloud%20Computing%202017.pdf.

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

[137] Specifically, these measures do the following: prohibit licensing foreign CSPs for operations; actively restrict direct foreign equity participation of foreign CSPs in Chinese companies; prohibit foreign CSPs from signing contracts directly with Chinese customers; prohibit foreign CSPs from independently using their brands and logos to market their services; prohibit foreign CSPs from contracting with Chinese telecommunication carriers for Internet connectivity; restrict foreign CSPs from broadcasting IP addresses within China; prohibit foreign CSPs from providing customer support to Chinese customers; and require any cooperation between foreign CSPs and Chinese companies to be disclosed in detail to regulators.

[138] 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.

concerning data localization with negative implications to cloud computing:[139] (1) a "counter-terrorism" law that requires Internet and telecommunication companies to create methods for monitoring content for terror threats;[140] (2) an online publishing law that requires that all servers used for online publications and press are located within China; and (3) the long-awaited Cybersecurity Law which came into effect last year.[141]

China's Cybersecurity Law went into effect on June 1, 2017 after being adopted by the National People's Congress in November 2016, following a year of legislative hearings and close international scrutiny.[142] 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.[143] 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"[144] gathered or produced in China by "critical information infrastructure" must be stored on servers physically located within China, with extremely limited exceptions.[145] Further, it is not clear what constitutes a "critical information infrastructure," possibly sweeping companies outside traditional information communication technologies into these obligations.[146]

---

[139] 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.

[140] 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.

[141] 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.

[142] *2016 Cybersecurity Law* (unofficial translation), http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en.

[143] *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.

[144] The *Information Security Technology Personal Information Security Specification* (GB/T 35273-2017), a specification that took effect in May 2018, expanded the definition. See Personal Information Security Specification, NORTON ROSE FULBRIGHT (Jan. 2018), http://www.nortonrosefulbright.com/knowledge/publications/163195/personal-information-security-specification.

[145] Article 37 provides 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.

[146] 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.").

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 2017. Article 2 of the measure goes beyond what is in the Cybersecurity law to mandate that all personal information and "important data" must be localized in mainland China.[147] The constant evolution of this new regime creates significant and costly regulatory uncertainty to those in the Chinese market.[148]

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.[149] 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.[150]

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.[151] USTR acknowledged these challenges in the 2018 NTE, highlighting the burdens that China's filtering of cross-border Internet traffic have imposed, and recognizing that outright blocking of websites has worsened.[152] High-profile examples of targeted blocking of whole services have included China's blocking of major U.S. services including Facebook, Picasa, Twitter, Tumblr,

---

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

[148] Sui-Lee Wee, *China's New Cybersecurity Law Leaves Foreign Firms Guidelines*, N.Y. TIMES (May 31, 2017), https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html.

[149] 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/.

[150] *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; 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.

[151] *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.

[152] *See 2018 Key Barriers to Digital Trade*, *supra* note 5 (noting that "China currently blocks 12 of the top 30 global sites and up to 3,000 sites in total, affecting billions of dollars in potential U.S. business.").

Google Search, Foursquare, Hulu, YouTube, Dropbox, LinkedIn, and Slideshare.[153] In June 2017, China shut down over 60 news outlets and social media accounts under the new Cybersecurity Law.[154] Informal estimates suggest that this blocking has easily cost American firms billions of dollars as they are pushed out of the market.[155]

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.[156]

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 of last year calling for Chinese telecoms to provide VPNs only to conduct cross-border business activities.[157] The government then reportedly ordered three state-owned telecommunication providers to bar individuals from using all VPNs pursuant to this policy over the summer.[158] While the Chinese government has subsequently denied such an order was issued noting that only unauthorized VPNs would be restricted,[159] they failed to clarify the

[153] *2014 Digital Trade in the U.S. and Global Economies*, *Part 2*, *supra* note 38, at 98.

[154] 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/.

[155] 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.

[156] 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/.

[157] 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.

[158] *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.

[159] 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).

process for determining when a VPN is deemed authorized.[160] The VPN ban was supposed to go into effect in March of this year.[161] In 2017 Apple removed all VPNs from the China App Store at the direction of the government.[162] These efforts to restrict VPNs are not new. In January 2015, China attempted to upgrade its Internet firewall to make it harder for people to circumvent it by using VPNs.[163] Additionally in 2015, China had cracked down on special software tools hosted on GitHub, a website popular with open source enthusiasts,[164] by launching distributed denial of service attacks against the site.

Other Barriers to E-commerce

China passed its first law regulating "e-commerce" in August 2018. The law will take effect in January 2019. The law is broadly written, applying new regulations and requirements on all e-commerce activities in China defined as the "sale of goods or services through the internet or any other information network."[165] Requirements include the need to obtain a business licenses to operate, which could place a burden on small businesses.

China also seeks to further restrict electronic payment systems from foreign competitors. In March 2018, the People's Bank of China released Notification No. 7 that will require foreign electronic payment companies to obtain a license and set up a Chinese entity. Industry reports that applications for these licenses by American and other non-Chinese companies have been held up or blocked by the PBOC due to inconsistent interpretation of the law, delaying the launch and operation of new electronic payment services.

---

[160] Chaim 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.

[161] Asha McLean, *VPNs Can Still Be Used in China Despite March 31 Ban*, ZDNet (April 5, 2018), https://www.zdnet.com/article/vpns-can-still-be-used-in-china-despite-march-31-ban/.

[162] 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.

[163] 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/.

[164] 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.

[165] Hogan Lovells, *A Game Changer? China Enacts First E-Commerce Law*, LEXOLOGY (Sept. 21, 2018), https://www.lexology.com/library/detail.aspx?g=f96bf736-db32-49fa-bec6-2e0a813ae03c.

G. Colombia

Legal Liability for Online Intermediaries

As CCIA observed in its 2018 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.[166] Recently passed legislation that sought to implement the U.S.-Colombia FTA copyright chapter includes no language on online intermediaries.[167] 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 States and elsewhere. CCIA urges USTR to take action with Colombian counterparts to prioritize implementation of a complete intermediary framework as required by the FTA.

Further, a bill was introduced in the Congress on October 9 intending to protect the "honor and good name of citizens" in relation to publications on the Internet. The bill focuses on the prevention of "fake news" and "other harmful and slanderous content" published on digital platforms. The bill applies to all online platforms that allow the publication of content directly or from third parties on the Internet. The bill requires that platforms register in a "Registry of Telecommunications Networks and Services Providers," which will be administered by the Ministry of Information and Communication Technologies (MINTIC). Providers would also be required to handle complaints and take action to prevent the continued distribution of the content on their platforms, tools, and services, and the Ministry would be empowered to impose fines on noncompliant providers. The proposed measure poses an unreasonable burden on online platforms by creating legal obligations without offering reasonable criteria to comply with the proposed legislation. The requirements for Internet services to also register as a telecommunications service provider would place significant burdens not conceived for such types of platforms including reporting requirements and additional fees.

---

[166] *2018 CCIA Special 301 Comments*, *supra* note 55.

[167] L. 1915, julio 12, 2018 (Colom.), *available at* http://es.presidencia.gov.co/normativa/normativa/LEY%201915%20DEL%2012%20DE%20JULIO%20DE%202018.pdf; José Roberto Herrera, *The Recent and Relevant Copyright Bill in Colombia (Law 1915-2018)*, KLUWER COPYRIGHT BLOG (Sept. 5, 2018), http://copyrightblog.kluweriplaw.com/2018/09/05/recent-relevant-copyright-bill-colombia-law-1915-2018/.

Imbalanced Copyright

The recent legislation that seeks to implement the U.S.-Colombia FTA copyright chapter also does not appear to 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 its position. Due to the focus of the CRCs agenda, it 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.

Taxation of Digital Services

Colombia's Tax Authority has announced that the Financing Law bill will include a Permanent Establishment obligation for foreign companies that "have significant economic activities in the country." The bill appears to be designed to require digital economy companies to pay taxes on the same income that is taxed in the United States. The Financing Law bill is expected to be enacted by December 2018.

H. 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 2018 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."[168] Unfortunately, USTR's concern is now becoming a reality.

[168] *2018 NTE*, *supra* note 4, at 197. 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

USTR should be proactive in identifying how relevant regulations impact U.S. industry and engage with the EU, using the ongoing bilateral discussions with the EU to discourage over-regulation and market access restrictions for U.S. companies.

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."[169]

Among other restrictive measures, France requires any institution that produces public documents to store and process this data only in France.[170] This is pursuant to a ministerial regulation on "public archives" that effectively function as data localization requirements for U.S. cloud providers seeking to provide services to the French public sector.

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 and a political agreement was reached in June 2018.[171] The regulation aims to remove national mandated data localization laws within Member States. CCIA welcomes the new rules as they will limit many types of forced data localization in EU Member States and provide more legal clarity for companies and users.[172]

---

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"].

[169] 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.

[170] Ministerial Circular from 5 April 2016, *Note d'information du 5 avril 2016 relative à l'informatique en nuage*, https://francearchives.fr/file/f7ace4517613a246583fd2dd673a0e6d0f86c039/static_9151.pdf.

[171] European Commission, Digital Single Market: EU Negotiators Reach a Political Agreement on Free Flow of Non-Personal Data (June 19, 2018), http://europa.eu/rapid/press-release_IP-18-4227_en.htm.

[172] Press Release, CCIA Welcomes Political Agreement on the Free Flow of Data in the EU (June 20, 2018), http://www.ccianet.org/2018/06/ccia-welcomes-political-agreement-on-the-free-flow-of-data-in-the-eu/

In the trade negotiation context, it is unfortunate that the EU's proposed text to facilitate cross-border data flows and digital trade includes provisions that would increase the likelihood of data localization rather than reduce barriers.[173]

Intermediary Liability and Mandatory User Monitoring, Filtering, and Blocking

Controversial updates to EU copyright law are expected to be politically agreed to in the coming months, which will have a detrimental impact on Internet services exporting to the EU and to the EU's own startup community. EU officials have explicitly said that this proposal is targeted at U.S. tech companies.[174] In September 2016, the European Commission (EC) submitted a copyright proposal to the European Parliament and European Council that would eliminate protections that limit online services' liability for misconduct by those services' users, require proactive screening by service providers, and create a "neighboring" pseudo-copyright restriction.[175] In September 2018, the European Parliament adopted its own position, creating a broad neighboring right for press publishers and undermining European safe harbors.[176] Negotiations to reconcile the positions of the European Commission, European Council and European Parliament have started and are expected to conclude by early 2019.[177] These changes will upend nearly two decades of established law, threatening U.S. digital exports by eliminating long-standing legal protections for online services that

[173] Christian Borggreen, *How the EU's New Trade Provision Could End Up Justifying More Data Localisation Globally*, DISRUPTIVE COMPETITION PROJECT (May 14, 2018), http://www.project-disco.org/european-union/051418eus-new-trade-provision-end-justifying-data-localisation-globally/ ("The risk, as recently highlighted by the European Parliament, is that third countries will justify data localisation measures for data protection reasons. Unfortunately, the European Commission's proposed text will encourage exactly that. Its article B2 states that "each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy." This is essentially a carte blanche for non-EU countries to introduce data protectionism under the guise of "data protection". It doesn't even require that countries can demonstrate that such laws are necessary and done in the least trade restrictive way, as under existing international trade law, which the EU has long been a party to.").

[174] Matt Schruers, *EU Copyright Changes Poised to Upset Critical Internet Policies*, DISRUPTIVE COMPETITION PROJECT (Oct. 18, 2018), https://www.project-disco.org/intellectual-property/101818-eu-copyright-changes-could-upset-internet-policies/#.W9ObT2JKhTb (citing that in defending the bill after a preliminary procedural defeat, one parliamentary backer of the bill removed any doubt about this focus, claiming "the ones [firms] that are reacting are mostly the ones we are targeting, which are the GAFA," referring to prominent U.S. companies).

[175] *Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market*, COM (2016)593.

[176] Press Release, European Parliament, Parliament Adopts Its Position on Digital Copyright Rules (Sept. 12, 2018), http://www.europarl.europa.eu/news/en/press-room/20180906IPR12103/parliament-adopts-its-position-on-digital-copyright-rules.

[177] James Vincent, *EU Approves Controversial Copyright Directive, Including Internet 'Link Tax' And 'Upload Filter'*, THE VERGE (Sept. 12, 2018), https://www.theverge.com/2018/9/12/17849868/eu-internet-copyright-reform-article-11-13-approved.

are a cornerstone of Internet policy. This subsection discusses the intermediary liability ramifications of this reform; the next discusses the "link tax."

The proposed Copyright Directive 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. If adopted, the Directive would dramatically weaken these long-standing liability protections, which suggests that most modern service providers may be ineligible for its protections.[178] These concerns remain with the amended text that the European Parliament voted on in September[179] and with the position of the European Council adopted in May 2018.

Like U.S. law, EU law presently contains an explicit provision stating that online services have no obligation to surveil users, or monitor or filter online content.[180] Online services have invested heavily in developing international markets, including Europe, in reliance on these provisions. The proposal now implies that online services must procure or develop and implement content recognition technology. The decision 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 proposal provides no specifics for what filtering mechanisms a hosting provider must implement, effectively empowering European rightsholders to dictate U.S. services' technology in potentially inconsistent ways across Europe.[181] Until the CJEU eventually addresses the question, affected hosting providers can expect inconsistent rulings and injunctions from lower courts in different countries.

As drafted, the Parliament text threatens significant 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

---

[178] *Copyright in the Digital Single Market, Amendments adopted by the European Parliament on 12 September 2018 on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market*, COM (2016) 0593 – C8-0383/2016 – 2016/0280(COD) (Sept. 12, 2018), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0337+0+DOC+PDF+V0//EN [hereinafter "September 2018 Draft Copyright Directive"].

[179] *Id*.

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

[181] *See September 2018 Draft Copyright Directive*, *supra* note 178, at art. 13.

intermediaries.[182] If the final EU reform does include these provisions, 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 new Directive would limit U.S. companies' investments for the benefit of EU rightsholders, establishing a market access barrier for many U.S. services and startups.[183]

Another Commission proposal on regulating terrorist content could also increase the burden on service providers to monitor and filter content.[184] The proposal would do the following: impose a legally binding one-hour deadline for content to be removed following a removal order from "national competent authorities"; create a new definition of terrorist content; impose a duty of care obligation for all platforms "to ensure that they are not misused for the dissemination of terrorist content online" with a requirement to take proactive measures "depending on the risk of terrorist content being disseminated" on each platforms; and impose strong financial penalties up to 4% of global turnover in case of "systematic failures to remove such content following removal orders".[185] CCIA supports the EU's goal of tackling terrorist content online and notes that hosting services remain committed to this goal through multiple efforts. However, the one-hour removal deadline, coupled with draconian penalties, will incentivize hosting services to take down all reported content, thereby chilling freedom of expression online. Broad implementation of mandated proactive measures across the Internet is likely to also incentivize hosting services to suppress potentially legal content and public interest speech.

---

[182] 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.

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

[184] *Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online*, COM (2018) 640 final (Sept, 12, 2018), https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-regulation-640_en.pdf.

[185] *Id*.

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.[186] The NetzDG law mandates removal of "manifestly unlawful" content within 24 hours, and provides for penalties of up to 50 million euros.[187] Unlawful content under the law includes a wide range of content from hate speech to unlawful propaganda.[188] The large fines and broad considerations of "manifestly unlawful content" and potential scope[189] have led to companies removing lawful content, erring on the side of caution in attempts to comply. Since coming into force in January 2018, the law has already led to high profile cases of content removal and wrongful account suspensions, groups have expressed concerns about its threats to free expression,[190] and the German government has already indicated that changes were needed to protect lawful speech online.[191] Further concerning is its potential domino effect on other regimes. Russia, Singapore, and the Philippines have cited this law as a positive example they

[186] 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.

[187] *Id*. § 3(2).

[188] *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).

[189] The law is designed to only apply to social media companies (it was informally referred to as the 'Facebook law'), but a wide variety of sources may also be implicated as the law is so broadly written to include sites that host third party content including Tumblr, Flickr, and Vimeo. Social media networks are defined as a tele-media service provider that operate online platforms (1) with the intent to make a profit, and (2) on which users can share content with other users or make that content publically available. *See Germany: Social Media Platforms to Be Held Accountable for Hosted Content Under "Facebook Act"*, LIBRARY OF CONGRESS (June 30, 2017), http://www.loc.gov/law/foreign-news/article/germany-social-mediaplatforms-to-be-held-accountable-for-hosted-content-under-facebook-act/.

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

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

intend to copy in the future to regulate speech.[192] Cases arising under this law will also have implications on extraterritoriality.[193]

Modeled on Germany's NetzDG law, Prime Minister Edouard Philippe of France recently announced a proposal on hate speech that includes a similar one-day removal requirement and a possible one-hour removal requirements for terrorist content.[194] The latter could be extended to other forms of problematic content such as "obvious" hate speech. Proposed fines for violations would reach up to 37 million euros. Furthermore, the law would create a new status for online intermediaries called "accélérateur de contenus," which would attach additional obligations to companies that "promote, reference, and rank online content."

Italy recently passed a new amendment that further empowers the Italian Communications Authority (AGCOM).[195] 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."[196] 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)[197] and the E-Commerce Directive. Departures from established law serve as a market access barrier for U.S. services in Italy.

---

[192] *See Germany: Flawed Social Media Law*, HUMAN RIGHTS WATCH (Feb. 14, 2018), https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.

[193] A case arising in Austria has been referred to the ECJ on Facebook's obligations to remove content that the court deemed defamatory. Notably, the questions referred include whether or not the hosting provider must remove identical flagged content worldwide, in the relevant Member State, or the relevant user worldwide, or of the relevant user in the relevant Member State. *Request for A Preliminary Ruling from the Oberster Gerichtshof (Austria)*, Eva Glawischnig-Piesczek v. Facebook Ireland Limited, Case C-18/18, https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2018.104.01.0021.01.ENG.

[194] The Fight Against Online Racism and Anti-Semitism, Government of France (2018), https://www.gouvernement.fr/en/the-fight-against-online-racism-and-anti-semitism.

[195] 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/.

[196] 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.

[197] Codified at 17 U.S.C. § 512.

Imbalanced Copyright

The EU Commission's copyright directive also 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, startups, and a wide range of commercial entities.

Ancillary Copyright/Link Tax

In 2018, USTR identified the "link tax" as a key digital trade barrier in several EU Member States, accurately noting that these measures "impose financial and operational burdens on U.S. firms that help drive traffic to publishing sites."[198] As CCIA has explained in previous proceedings, restrictions on the ability to quote (*inter alia*) news content violate Europe's international commitments. Unfortunately, the European Union-wide proposal for a "neighboring right" that would be a more expansive, EU-wide version of previous German and Spanish efforts than these previous laws, is progressing. A link tax is likely to become a reality as per the adopted positions of the European Council and the European Parliament, respectively in May and September 2018.[199]

As CCIA has previously explained in the NTE process,[200] the proposal would squarely violate international legal obligations. 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.

Of note, the European Parliament's amended text, as adopted in September, provides that publishers of press publications and news agencies become beneficiaries of the rights provided by

---

[198] *2018 Key Barriers to Digital Trade*, *supra* note 5; *2018 NTE*, *supra* note 4, at 199-200.

[199] EUROPEAN COMMISSION, Joint Statement by Vice-President Ansip and Commissioner Gabriel on the European Parliament's vote to start negotiations on modern copyright rules (Sept. 12, 2018), *available at* http://europa.eu/rapid/press-release_STATEMENT-18-5761_en.htm; *September 2018 Draft Copyright Directive*, *supra* note 179.

[200] Comments of the CCIA, *In re Request for Public Comments To Compile the National Trade Estimate Report on Foreign Trade Barriers*, Dkt. No. 2015-0014, filed Nov. 9, 2015, *available at* http://www.ccianet.org/wp-content/uploads/2015/10/CCIA-NTE-2016.pdf [hereinafter "CCIA 2016 NTE Comments"].

Article 2 and 3(3) of the EU Infosoc Directive for the digital use of their press publications by "information society providers." The text also states that "the listing in a search engine should not be considered as fair and proportionate remuneration."[201]

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 submission for the 2016 NTE, Germany's 2013 ancillary copyright law (*Leistungsschutzrecht*) remains in effect, irrespective of EU-wide neighboring rights regulation.[202] By extending copyright protection to small text excerpts in search results, this law violates international obligations that require free quotation.

As discussed more fully in CCIA's 2015 Special 301 submission,[203] 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.[204] 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.[205] Such measures hardly 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

[201] *September 2018 Draft Copyright Directive*, *supra* note 178 at recital 32.

[202] *CCIA 2016 NTE Comments*, *supra* note 200.

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

[204] 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/.

[205] 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.

and distorts established copyright law, but it also violates the EU and Spain's treaty and WTO commitments.[206]

Other EU proposals are expanding the scope of existing exclusive rights of reproduction and communication to the public. In 2016 France passed legislation creating a new royalty for indexing images on the Internet.[207] As CCIA previously explained in the NTE process, the law took effect in January 2017. One provision of this legislation transfers rights in reproduction and communication to the public of pictures that are automatically indexed by search and ranking services to a French collecting society. While not a snippet tax per se, this law reflects the same intent as the German and Spanish taxes, insofar as it creates a regulatory structure intended to be exploited against U.S. exporters — a "right to be indexed." By vesting indexing these "rights" in a domestic collecting society, the law targets an industry that consists largely of U.S. exporters.[208] CCIA is among several industry and civil society organizations that have highlighted how the law will impact online services and mobile applications.[209] The law creates a cloud of legal uncertainty, affecting everyday activities of online users, such as posting, linking, and embedding images online.[210] CCIA appreciates USTR inclusion of this law in the 2018 NTE as a trade barrier and supports its inclusion in the 2019 NTE.[211] However, as the French law remained largely unchallenged, it was incorporated into the EU Copyright Directive in the form of article 13b and now threatens to become an EU-wide barrier.[212]

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

---

[206] *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.

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

[208] 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).

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

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

[211] *2018 NTE*, *supra note* 4, at 200.

[212] *See September 2018 Draft Copyright Directive*, *supra* note 178.

considerable regulatory uncertainty for companies with transatlantic operations. The Safe 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."[213]

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.[214] 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.[215] Over 3,700 companies are now certified under the Privacy Shield.[216] The first annual review took place on September 18th and 19th 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."[217] Consistent with that commitment, a second annual review took place on October 18th and 19th in Brussels.

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.[218] While one challenge was dismissed for lack of standing, the other remains pending.[219]

---

[213] *2016 NTE*, *supra* note 168, at 179.

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

[215] 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.

[216] Privacy Shield Framework, https://www.privacyshield.gov/list (last visited Oct. 30, 2018).

[217] 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.

[218] 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.

[219] *Challenge to Privacy Shield Dismissed By EU General Court*, ALSTON & BIRD, https://www.alstonprivacy.com/challenge-privacy-shield-dismissed-eu-general-court/.

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.[220] 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.[221]

General Data Protection Regulation and "Right to Be Forgotten"

The EU General Data Protection Regulation (GDPR) was adopted on April 27, 2016, and went into effect on May 25, 2018.[222] 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.[223] However, ambiguities in the text of the GDPR mean that much of the impact of the bill will 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 Regulation over the past year,[224] 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

[220] 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.").

[221] 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/.

[222] 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"].

[223] *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), available at 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.").

[224] 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).

of key provisions of up to 4% of global operating costs, the stakes for companies operating in the EU are high.[225]

The 2014 ruling by the CJEU on the "right to be forgotten" (RTBF) 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."[226] In the four 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. Domestic courts in the EU are also extending the applicability of RTBF cases.[227]

For example, some search engines have been instructed that they should not link to independent media coverage 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."[228] 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."[229]

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 to those conducted on .com and other Google domains with worldwide reach.[230] The case is currently on appeal to France's

---

[225] GDPR, *supra* note 222, at art. 83.

[226] 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.

[227] The Spanish Constitutional Court recently decided a case that extended the RTBF to the de-indexation of a newspaper's own digital repository search engine. *Landmark Decision Regarding The Implementation Of The "Right To Be Forgotten"* (Oct. 4, 2018), https://www.lexology.com/library/detail.aspx?g=9f7db79b-d75c-4a7f-b6fe-91825ba27392.

[228] 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.

[229] *Id*.

[230] Google released a report recently illustrating how it fulfills its obligations under the "right to be forgotten." The report also shows how complex implementation can be for an Internet services provider. Google,

highest court,[231] which referred legal questions to the CJEU last year.[232] 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.[233] CCIA thanks USTR for highlighting this case in the 2018 NTE and supports its inclusion in the 2019 NTE.[234] As domestic courts in EU Member States begin to impose injunctions pursuant to the RTBF, the decision of the ECJ will have significant consequences.[235] There are already indications that the practice of worldwide injunctions against Internet services to remove links is becoming more common.[236]

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.[237] Under the GDPR, the fine for noncompliance with these and other provisions can be up to 4% of a company's global operating costs.

Three Years of the Right to be Forgotten (2018), https://drive.google.com/file/d/1H4MKNwf5MgeztG7OnJRnl3ym3gIT3HUK/view.

[231] 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-highestcourt.

[232] Request for a preliminary ruling from the Conseil d'État (France), Case C-507/17, Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) (2017), http://curia.europa.eu/juris/document/document.jsf?text=&docid=195494&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=369957.

[233] 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-authorityto-regulate-google-globally-231233.

[234] *NTE 2018*, *supra* note 4.

[235] *See, e.g.*, *Belgian Court of Cassation Rules on Right to Be Forgotten*, HUNTON PRIVACY BLOG (June 1, 2016), https://www.huntonprivacyblog.com/2016/06/01/belgian- court-of-cassation-rules-on-right-to-be-forgotten/; Andrew Griffin, *Google Loses 'Right to Be Forgotten' Fight Against Businessman And Must Delete Information About Him*, THE INDEPENDENT (Apr. 13, 2018), https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-right-to-be-forgotten-ruling-latest-london-high-courteurope-a8302981.html. Other countries that are also starting to consider the RTBF including Argentina and India. *See* Edward Carter, *Argentina's Right to Be Forgotten*, 27 EMORY L. REV. 23 (2013), *available at* http://law.emory.edu/eilr/_documents/volumes/27/1/recent-developments/carter.pdf (noting that the courts are inconsistent in their recognition of the RTBF; Telecom Regulatory Authority of India, Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector (2018), *available at* https://www.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf (recommending that the right to be forgotten should be conferred upon the telecommunications consumers).

[236] For example, a French court recently ordered Google to de-index sites and "make them inaccessible worldwide". Court Order Complaint to Google (2018), *available at* https://www.lumendatabase.org/notices/16919104#.

[237] *GDPR*, *supra* note 222, at art. 17.

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.[238] 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 "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 Online Applications

In the European Union, there have been discussions about using regulations to "level the playing field"[239] 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,[240] and the proposed e-Privacy Regulation.[241]

In May 2016, the European Commission published its proposal for a Directive to reform Europe's audiovisual rules. This Directive will enter into force by the end of 2018, with Member States having 21 months to transpose it into their national legislation.[242] Notably, this reform introduces two measures that undermine market access for U.S. companies. The first is a mandatory requirement for video-on-demand providers to include in their catalogues a 30% share of European works (*i.e.*, a 30% quota of European content). 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 measure 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 measure 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.

---

[238] *See, e.g.*, Alex Hern, *Google Takes Right to be Forgotten*, *supra* note 231.

[239] 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.

[240] *Id*.

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

[242] Press Release, European Commission, European Parliament Approves Revised Rules for Audiovisual Media Across Europe (Oct. 2, 2018), https://ec.europa.eu/digital-single-market/en/news/european-parliament-approves-revised-rules-audiovisual-media-across-europe.

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 this new provision, video-on-demand providers will have to contribute to the cultural funds of up to 28 Member States. This will fragment the Single Market and significantly hamper the activities of U.S. companies in the EU's audiovisual market.

The proposal for an e-Privacy Regulation was published by the European Commission in January 2017 and is designed to replace the current e-Privacy Directive.[243] The proposal seeks to expand the existing Directive, which only applies to telecommunication services, to all "electronic communication services".[244] 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 (IoT).[245] The proposal effectively replaces core parts of the GDPR for these services. Specifically, the proposal over-relies on consent and restricts some of the flexibility afforded by the GDPR for the processing of communications data and device data.

Furthermore, third-party vendors, including those which are essential to how the Internet functions today (e.g. cloud infrastructure service providers, cybersecurity vendors, content delivery network providers), may not be able to process communications data and would severely undermine the security, latency and overall provision of emails, instant messaging, and IoT services.

Lastly, some policy proposals suggest that free, ad-supported services should not block access to users who do not consent to the placing of cookies and processing of device data to provide them with relevant advertisement.[246] This would severely disrupt the vibrant app and free content economy, infringe upon the freedom to conduct a business, and ultimately reduce consumer choice on the market.

The proposed electronic communications code extends certain legacy telecommunications requirements to online applications which will seriously eliminate their free or almost free business

---

[243] 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"].

[244] *Id*. at art. 4.

[245] *Id*. at recital 12.

[246] See European Parliament text (Amendment 92), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0324+0+DOC+XML+V0//EN. Similar discussions are taking place in Council. See http://data.consilium.europa.eu/doc/document/ST-12336-2018-INIT/en/pdf.

model and could ultimately 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 as a non-tariff trade barrier, even within the EU Single Market.[247] To address some of the complexities, the EU Commission has proposed a relatively fundamental overhaul of the system.[248] 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 EU has decided 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.

Taxation of Digital Services

The European Commission presented a package of two digital tax proposals in March 2018.[249] The package contains two legislative proposals, including a Directive introducing "an interim tax on certain revenue from digital activities." This controversial digital services tax (DST)

[247] 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.

[248] 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.

[249] Proposal for a Council Directive on the Common System of A Digital Services Tax on Revenues Resulting from the Provisions of Certain Digital Services, https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en.

will be set at 3% of companies' gross revenues from making available advertisement space, intermediation services and transmission of user data.[250]

The DST is clearly, and disproportionately, aimed at U.S. tech companies,[251] and therefore may violate the EU's commitments under the WTO's General Agreement on Trade in Services by discriminating against primarily U.S. companies in favor of EU companies.[252] Many of the targeted U.S. companies are mentioned by name in an internal Commission document.[253]

The DST proposal relied on a study that suggests that digital businesses in Europe only pay an effective tax rate of 9.5%, compared to traditional companies who pay a corporate tax rate of 23.2%, as evidence that digital services do not pay sufficient taxes. This estimate is not accurate, and the EC's characterization of the study has been disputed by the study's own authors. The estimates that the EC relies on come from studies produced by ZEW and PwC. The author of this research, Professor Christoph Spendel, has repeatedly criticized the EC's characterization of the finding of the report to support a proposed Directive to tax predominantly American digital firms.[254] He urges that it should not be used to justify the assertion that digital companies are undertaxed, and disputes the EC's claim that digital companies pay less.[255]

---

[250] Specifically, the DST proposal would require each EU Member State to impose a tax of 3% on gross revenues obtained in that Member State resulting from the provision of any one of the following services: (a) placing advertising on a digital interface, where the advertising appears on a user's device in the EU; (b) making available a multi-sided digital interface that allows users to find and interact with other users, and which may facilitate the provision of underlying supplies of goods or services directly between users where a user is located or based in the EU; and (c) the transmission (e.g., sale) of data collected about users and generated from users' activities on digital interfaces where the user is in the EU.

[251] The DST discriminates against US digital firms in the following ways: (a) the DST thresholds — at least $750 million in global gross revenue and at least $50 million in EU gross revenue — are designed to capture Google, Facebook, Amazon, eBay, Uber, Airbnb but few EU firms; (b) the revenues subject to the proposal DST are defined to capture business models of US firms but not EU digital firms; and (c) the proposal allows value added taxes and similar taxes to be subtracted from 'taxable revenue' in calculating the base from the 3% impost which would increase the tax base since the United States does not have value added taxes. *See* Gary Clyde Hufbauer & Zhiyao Lu, *The European Union's Proposed Digital Services Tax: A De Facto Tariff*, PETERSON INSTITUTE FOR INTERNATIONAL ECONOMICS (June 2018), *available at* https://piie.com/system/files/documents/pb18-15.pdf at 7.

[252] Under GATS, the EU agrees to provide national treatment to services and service suppliers of other WTO Members in the economic sectors that are covered by the DST. This means that the EU may not discriminate against those services and service suppliers in favor of its own "like" domestic services and service suppliers.

[253] European Commission, *Taxation of Digital Activities in the Single Market* (Feb. 26, 2018), https://www.politico.eu/wp-content/uploads/2018/02/taxation-of-digital-economy-2.pdf.

[254] PwC, *Understanding the ZEW-PwC Report, 'Digital Tax Index, 2017'* (June 2018), *available at* https://www.pwc.com/us/en/press-releases/2018/understanding-the-zew-pwc-report.html.

[255] *EU Plans 3 Percent Turnover Tax for Amazon, Google, Facebook*, BLOOMBERG (Mar. 21, 2018), *available at* https://www.bna.com/eu-plans-percent-n57982090189/ ("effective tax rates for digital and traditional businesses cannot be compared one-by-one because digital businesses earn different types of income, such as royalties").

Paradoxically, the proposal fails to acknowledge that U.S. firms are already taxed on their overseas profits as part of the recent U.S. tax reform, while the EU does not tax EU firms' overseas profits. An additional digital tax targeted on the revenue of U.S. firms in Europe would result in a severe over-taxation of U.S. firms compared to their EU competitors.[256] The DST can be considered disguised protectionism and inconsistent with the EU's trade commitments. The Peterson Institute for International Economics has argued that it is a de facto tariff.[257] The Commission's own internal document questions whether the tax would "be consistent with WTO obligations as it would only apply the new tax to situations involving third countries and not to intra-EU situations, and could therefore be viewed as discriminatory."[258]

CCIA agrees with Senators Hatch and Wyden, who on October 18, 2018 warned that the EU DST "has been designed to discriminate against U.S. companies and undermine the international tax system, creating a significant new transatlantic trade barrier."[259]

There are several EU Member States that are taking unilateral action to implement a DST modeled on the EU's proposal in their own country. On October 19, Spain presented a draft digital tax bill that would set a 3% tax on three types digital services that are also all targeted by the EU's DST.[260] Following a public consultation period before final parliamentary approval, this tax could be implemented in Spain before a wider EU agreement is reached. The UK Government has also made

[256] CCIA commissioned a recently-released study that illustrated the effects of the DST on welfare, growth, and revenues that will negatively impact Europe's digitizing economy. *See* Copenhagen Economics, The Proposed EU Digital Services Tax: Effects on Welfare, Growth, and Revenues (Sept. 2018), *available at* https://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/7/457/1537162175/copenhagen-economics-study-on-the-eu-dst-proposal-13-september.pdf.

[257] *The European Union's Proposed Digital Services Tax: A De Facto Tariff*, *supra* note 251.

[258] *Taxation of Digital Activities in the Single Market*, *supra* note 243.

[259] Letter to President Donald Tusk of the European Council and President Jean-Claud Juncker of the European Commission from Senators Orrin Hatch and Ron Wyden, Oct. 18, 2018, *available at* https://www.finance.senate.gov/imo/media/doc/2018-10-18%20OGH%20RW%20to%20Juncker%20Tusk.pdf.

[260] Similar to the EU DST, the tax rate will be set at 3%. The Spanish Government has estimated the revenue to 1,200 million euros. Companies subject to this tax will be those with a net turnover of more than 750 million euros worldwide and whose revenues derived from digital services affected by the tax exceed three million euros in Spain. The EU DST the Spanish tax would also tax three types of services: (1) Provision of online advertising services; (2) Online intermediation services; and (3) The sale of data generated from information provided by the user. *See* http://www.hacienda.gob.es/Documentacion/Publico/NormativaDoctrina/Proyectos/Tributarios/ANTEPROYECTO%20LEY%20IDSD.pdf.

recent statements about targeting U.S. companies with new taxes, and may include a variant of the DST in an upcoming budget.[261]

Another example of a unilateral approach to international tax policy is the UK's diverted profits tax.[262] This tax is a significant departure from the multilateral tax system, diverging from international treaties and norms, and is designed to privilege the UK over its trading partners. Under this approach, the UK can levy taxes on structures and payments that are not related to UK activities. This serves as an impediment to cross-border investment and creates a significant source of uncertainty among multinational companies with any ties to the UK market.

CCIA concurs with U.S. Treasury Secretary Mnuchin, who in October 2018 stated concern with the "consideration of a unilateral and unfair gross sales tax that targets our technology and internet companies."[263] CCIA agrees with the Secretary's view that a "tax should be based on income, not sales, and should not single out a specific industry for taxation under a different standard" and would discourage countries from taking unilateral action in this area.[264]

Other Platform Regulation

The EU is finalizing negotiations on a new regulation on "platform-to-business" (P2B) relations that would require online intermediaries to provide redress mechanisms and meet aggressive transparency obligations concerning delisting, ranking, differentiated treatment, and access to data. These rules would apply to all online intermediation services facilitating the initiating of direct transactions between these services' business users and consumers. Some of the regulation's provisions would also apply to online search engines. Among other obligations, online intermediaries would be required to "outline the main parameters determining ranking and the reasons for the relative importance of those main parameters as opposed to other parameters." These and other obligations represent burdensome requirements that could create market access barriers for intermediation services, large and small, seeking access to the EU market. They could make it much harder for multi-sided businesses to strike the right balance between the interests of their various users while preserving their own interests, for example, brand protection. Recently proposed

[261] *UK Could Go It Alone on Digital Services Tax: Finance Minister*, REUTERS (Oct. 1, 2018), https://www.reuters.com/article/us-britain-digital-tax/uk-could-go-it-alone-on-digital-services-tax-finance-minister-idUSKCN1MB2E2

[262] Finance Act 2015, Ch. 11 [26 Mar. 2015] (U.K.).

[263] Press Release, Secretary Mnuchin Statement on Digital Economy Taxation Efforts (Oct. 25, 2018), https://home.treasury.gov/news/press-releases/sm534.

[264] *Id*.

amendments could increase the types of platforms covered (including mobile operating systems), affect vertical integration, mandate default settings, and include additional disclosure requirements. CCIA encourages USTR to monitor these developments closely and encourage EU counterparts to avoid market access barriers through this regulation.

Goods Package

Last December, the EC introduced a pair of proposed regulations collectively referred to as the "Goods Package". The Goods Package includes a Proposal for a Regulation on Enforcement and Compliance in the Single Market for Goods (the Enforcement Regulation)[265] which is aimed at increasing enforcement of existing EU product legislation and advancing customer safety. However, industry has expressed concerns that the current draft of the proposal will do little to improve overall customer safety and have unintended effects. There is currently a requirement for a dedicated "responsible person for compliance information." More specifically, the manufacturers of all goods sold in the EU must appoint a person located in the EU to hold compliance documentation who will likely be accountable for non-compliance more broadly with liability for sellers who offer a product where such Responsible Person has not been appointed. The requirement does not distinguish between types of goods, nor does it provide any waivers for these requires to SMEs or small volume sellers.

There are concerns that will significantly limit access to the EU marketplace for U.S. small businesses and the "responsible person" requirement will particularly hurt U.S. resellers. Industry observes that manufacturers of low-risk merchandise that are not primarily focused on the EU market won't appoint a "responsible person" required under the proposal, making resale into the EU virtually impossible. Industry has also expressed doubt that the proposed legislation would be consistent with the EU's technical barriers to trade obligations on conformity assessment measures, as well as have the effect of creating unnecessary obstacles to international trade.[266]

Cybersecurity Certifications

The EU is currently negotiating a new regulation ("Cybersecurity Act") which introduces a pan-European framework to develop cyber security certifications for any kind of ICT products

[265] Proposal for a Regulation on Enforcement and Compliance in the Single Market for Goods (Goods Package), https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-795_en.

[266] *See* EUROPEAN COMMISSION, *Fact Sheet: Technical Barriers to Trade*, *available at* http://trade.ec.europa.eu/doclib/docs/2013/april/tradoc_150987.pdf.

launched in the EU market.[267] The Commission's proposal exclusively focused on the development of *voluntary* certification schemes, but the Parliament amended the Regulation and introduced the development of *mandatory* certification scheme for ICT products "requiring a high level of assurance". It is not clear which products would be subject to mandatory certifications as the definitions of different thresholds of assurance levels ("low", "substantial", and "high") are vague and refer to a single non-quantitative criterion that is likely to be interpreted in a number of different ways.[268]

Market players, especially smaller ones, may face increased entry costs if the outcome of the final negotiations disregard the possibility of self-conformity assessments — as the Council text[269] seems to suggest. This would effectively lead to costly third-party audits and validation for all products, regardless of the security risks of the products.

I. India

Data Localization

CCIA has raised concerns with the government of India's practices around data localization in previous NTEs. The climate for market access has not only not improved, but has gotten worse with the government of India's several recent actions that are in deep conflict with global best practices on data protection and data localization.

The Reserve Bank of India issued a directive (RBI/2017-18/153) mandating aggressive localization requirements for data related to payment transactions. The directive is now in force and requires "storage of data in a system in India" but does not clarify whether the data can be accessed from or transferred outside the country, even if a copy is kept in India.

India's draft Data Protection bill was released in July 2018. As drafted, the law would require companies to store a copy of all "personal data" in India. "Sensitive" personal data would be subject to even stricter requirements and "critical" personal data can only be processed within

[267] Cybersecurity, Digital Single Market Policy, European Commission, https://ec.europa.eu/digital-single-market/en/cyber-security (last updated Apr. 16, 2018).

[268] See definitions in Article 46 of the Commission proposal, Parliament text, and Council text. Proposal for a Regulation of the European Parliament and of the Council on ENISA (Sep. 13, 2017), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN; Draft European Parliament Legislative Resolution on Proposal for a Regulation on ENISA (July 30, 2018), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA8-2018-0264%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN; Council of the European Union, 2017/0225, http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf.

[269] Council of the European Union, 2017/0225, http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf.

India.[270] Only limited exceptions are provided for both the transfer of "personal" and "critical" personal data. The bill as currently drafted places prescriptive requirements on data localization that will harm a wide range of U.S. exporters as well as India's domestic digital economy. Support for this bill would also legitimize other proceedings in India focused on data localization addressed below. USTR should take immediate steps to address these barriers and ask for commitments, including through the GSP review process, to remove data localization requirements from current and proposed regulations.

In addition, 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.[271] Indian authorities have contemplated extending localization policies to non-government communications as well,[272] 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.[273]

Industry reports that U.S. cloud computing services already face a number of service barriers when exporting to India. These reports include an inability to buy dark fiber needed to build new networks and a prohibition on the purchase of dual-use equipment used to run the networks, high submarine cable landing station charges, and an inability to own and manage a network to cross-connect data centers and connect directly to an Internet Exchange Point. Industry reports that these restrictions impact the ability of cloud services to effectively manage their own networks to optimize access, minimize latency, and reduce costs.

---

[270] The Personal Data Protection Bill (India) (2018), http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

[271] Chander & Lê, *Data Nationalism*, *supra* note 30, at 694-97.

[272] 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.

[273] 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.

However, the regulatory environment is poised to worsen for cloud services. In 2018, a cloud policy panel recommended that India mandate data localization in the country in a report set to be released later this year.[274] The Ministry of Electronics and Information Technology (MEITY) is now reviewing the proposed Cloud Storage Policy. If the policy is adopted, then all such data generated in India by tech and cloud computing companies would be required to be stored within the country. Little information has been publically available on the draft policy.

Across different ministries in India, localizations requirements are also being added to a variety of new policies that will further disrupt online services in India and discourage foreign direct investment.[275] These include a set of recommendations to form a new e-commerce policy, which is being developed by a think tank headed by India's Commerce Minister Suresh Prabhu. If adopted, the policy would require all e-commerce companies to store their data exclusively in India. The development of the draft policy had significant process and representation concerns.[276] The draft also included restrictions on foreign direct investment that would affect business to consumer e-commerce firms.[277] There are reports that India is reconsidering its proposal and industry is closely following developments.[278]

---

[274] *India Panel Wants Localisation of Cloud Storage Data In Possible Blow to Big Tech Firms*, REUTERS (Aug. 4, 2018), https://www.reuters.com/article/us-india-data-localisation-exclusive/exclusive-india-panel-wants-localization-of-cloud-storage-data-in-possible-blow-to-big-tech-firms-idUSKBN1KP08J ("A panel working on the Indian government's cloud computing policy wants data generated in India to be stored within the country . . . The policy will be the latest in a series of proposals that seek to spur data localization in India, as the government finalizes an overarching data protection law. Local data storage requirements for digital payments and e-commerce sectors are also being planned.").

[275] *Amazon Has a New Rival in India, and It Isn't Walmart*, BLOOMBERG (Aug. 15, 2018), https://www.bloomberg.com/view/articles/2018-08-16/amazon-has-a-new-rival-in-india-and-it-isn-t-walmart.

[276] The draft e-commerce policy was developed by a "think tank" formed by the Ministry of Commerce of India. The draft policy did not have any representation of foreign companies with investments in India. Industry reports that this bias is shown through some provisions that would grant competitive advantages to domestic companies including mandatory disclosure of source code to the government and provisions that will enable founders of domestic companies to retain control of companies they have minority stakes in, and over-regulation.

[277] India continues to treat different models of "business to consumer" (B2C) e-commerce firms differently, due to pressure exerted by Indian e-commerce firms who are looking to subvert dominance of foreign players. Globally, B2C e-commerce firms are classified under models such as "marketplace", "inventory", and "hybrid." India is the only country to define the "marketplace" model. Currently, FDI is not permitted in the inventory model and is permitted only in the marketplace model, with the exception of food retail. The draft e-commerce policy recommended that limited inventory model be allowed for 100% made-in-India goods sold through platforms whose founder and or promoter would be a resident Indian, where the company would be controlled by an Indian management, and foreign equity would not exceed 49%. Despite significant criticism for such a proposal, industry reports that this provision is likely to remain in the proposal. India currently does not allow a hybrid model in e-commerce and has issued multiple regulations which have sought to restrict the inventory model in India, including effecting a 25% cap on sales from a single seller or its group companies on ecommerce platforms. The draft policy proposed to allow Indian companies to follow an inventory model for made-in-India products, a provision which

Filtering & Blocking

The Indian government regularly shuts down mobile Internet services across regions in response to local unrest and protests, in order to prevent what it calls "anti-national activity."[279] Often the shutdowns are in response to or in preparation for actions that may cause disturbances or violence.[280] These shutdowns stand in stark contrast to India's recent efforts to expand Internet services across the country, and have led CCIA members including Facebook and Google to weigh in by developing Service Restriction Orders.[281] Brookings estimates that Internet shutdowns cost India's GDP at least $968 million over the 70 days during which it was shut down in 2016.[282]

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.[283] CCIA commends USTR for highlighting the dangerous effects of these rules in the 2018 NTE.[284] 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

---

wasn't extended to companies with foreign equity and protects the interests of companies promoted by Indian entrepreneurs over foreign equity-held companies.

[278] *India Review E-Commerce Policy Draft After Criticism*, BLOOMBERG (Aug. 14, 2018), https://www.bloomberg.com/news/articles/2018-08-14/india-is-said-to-review-e-commerce-policy-draft-after-criticism.

[279] 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.

[280] 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.

[281] *Id*.

[282] Darrell M. West, *Internet Shutdowns*, *supra* note 44, at 7.

[283] 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.

[284] *See also 2018 NTE*, *supra* note 4, at 234 ("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.").

minds."[285] Executives faced possible prison terms, in addition to financial penalties,[286] based on legal standards that are essentially strict liability.[287] Although India's Supreme Court earlier clarified and struck down some sections of the 2000 IT Act,[288] its 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).[289] Imposing liability on an intermediary who cannot technologically respond to content is tantamount to a prohibition on use of the application.[290]

Last year,[291] the Supreme Court of India 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

---

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

[286] 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.

[287] 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.

[288] 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 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.

[289] 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.

[290] 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.

[291] Arap Gupta, *The Supreme Court's Slow March Towards Eroding Online Intermediary Liability*, THE WIRE (July 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 issues orders to investigate the possibility of website blocking and key word filtering for search engine to remove generated ads).

speech as well, the Court informed them that they should stop operating in India if they cannot resolve those issues.[292] The Court further directed Google, Microsoft, and Yahoo! to set up their own in-house experts to monitor and delete the prohibited ads.[293] India is hardly the only country whose authorities are demanding speech and content restrictions by intermediaries.[294] However, as a quickly emerging player in the global Internet economy, India should have an intermediary framework that further enables innovation.[295]

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.[296] In 2015, TRAI proposed introducing licensing and regulatory obligations targeted at OTT VoIP.[297] However, TRAI Chairman R.S. 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.

Taxation of Digital Services

India is also contemplating changes to its taxation regime that further target the Internet economy by expanding the definition of a "business connection" in India to include "significant

---

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

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

[294] 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." 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. Without strict compliance with the notification requirements, the service provider will be subject to the same penalty as if they uploaded the content themselves. *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/.

[295] THE BOSTON CONSULTING GROUP, *The $250 Billion Digital Volcano: Dormant No More* (2017), *available at* https://media-publications.bcg.com/BCG-TiE-Digital-Volcano-Apr2017.pdf (mentioning that by 2020, India's Internet Industry is expected to comprise of 7.5% of its GDP).

[296] *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.

[297] *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/.

economic presence." This change could impose a 40% tax on foreign companies exporting digital goods or services to India.[298]

India has also been critical of the World Trade Organization's moratorium on customs duties on electronic transmissions. Any imposition of new duties on electronic transmission would be inconsistent with their WTO commitments and would significantly impact an exporter's ability to operate in India's increasingly growing digital economy.

J. Indonesia

Data and Infrastructure Localization

As USTR noted in the 2018 NTE, data localization requirements remain a serious concern in Indonesia.[299] Since 2012, service providers providing a "public service" have been required to localize data servers within the country.[300] 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."[301] 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.[302]

Indonesia has continued to establish requirements for foreign services to locate servers within Indonesian territory through a series of forced data localization measures including Ministry of Communication and Informatics Regulation 82/2012 and the Draft Regulation Regarding the Provision of Application and/or Content Services Through the Internet. While Indonesia is considering amendments to its data localization policies, no action has been taken to finalize these revisions, creating continued uncertainty for businesses looking to operate in the country.

As also noted in the 2018 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

---

[298] *India Goes After Digital Giants in Budget 2018*, BLOOMBERG BNA (Feb. 1, 2018) https://www.bna.com/india-goes-digital-n73014474964/.

[299] *2018 NTE*, *supra* note 4, at 254-55.

[300] *2018 Key Barriers to Digital Trade*, *supra* note 5.

[301] *2018 NTE*, *supra* note 4, at 255.

[302] Chander & Lê, *Data Nationalism*, *supra* note 30, at 698.

locally sourced components and services.[303] Additionally, Indonesia has issued a regulation that requires 4G-enabled devices to contain 30% local content.[304]

Duties on Electronic Transmissions

Indonesia recently issued Regulation No.17/PMK.010/2018 (Regulation 17).[305] The Regulation amends Indonesia's Harmonized Tariff Schedule (HTS) Chapter 99 to add: "Software and other digital products transmitted electronically." This makes Indonesia the only country in the world that has added electronic transmissions to its HTS. This unprecedented step to imposing customs requirements on purely digital transactions will impose significant and unnecessary compliance burdens on nearly every enterprise, including many SMEs. The policy is also in conflict with Indonesia commitment under the WTO's moratorium on custom duties on electronic transmissions, dating back to 1998[306] and most recently reaffirmed in December 2017.[307] Left unchecked, Indonesia's actions will set a dangerous precedent and may encourage other countries to violate the WTO moratorium. This is especially critical as members at the WTO continue discussions on e-commerce. Indonesia must rescind Regulation 17 and remove Chapter 99 from its HTS.

Undue Restrictions on Rich Interaction Applications (RIAs)

Indonesia's Ministry of Communications and Informatics issued the Draft OTT Regulation in 2017.[308] This proposed law would require new liability and monitoring requirements for online services, creation of a local entity or permanent establishment, requirements to assist law enforcement in providing access and lawful interception of communications, and numerous other market access barriers.[309] The proposal as drafted would impede the emergence of SMEs in a

[303] *2018 NTE*, *supra* note 4, at 254.

[304] *Id*. at 235.

[305] Regulation No.17/PMK.010/2018 (Regulation 17) (Indonesia) (2018), http://www.jdih.kemenkeu.go.id/fullText/2018/17~PMK.010~2018Per.pdf.

[306] The Geneva Ministerial Declaration on Global Electronic Commerce (May 1998), https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm.

[307] Work Programme on Electronic Commerce, Ministerial Decision (Dec. 2017), https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN17/65.pdf.

[308] *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/.

[309] Yose Rizal Damur *et al*., *Rich-Interactive-Applications (RIA) in Indonesia: Value to the Society and the Importance of an Enabling Regulatory Framework*, Centre for Strategic and International Studies & Asia Internet Coalition (2018), *available at* https://www.aicasia.org/wp-content/uploads/2018/05/Rich-Interactive-Application-RIA-Final-Report.pdf.

country where digital platforms and the apps-based industry is growing.[310] Indonesia is also considering a tax on foreign OTT service providers that have a "permanent establishment" in Indonesia.[311]

Investment Restrictions on E-Commerce

U.S. firms face additional barriers in Indonesia through the country's restriction on foreign direct investment for e-commerce services. Foreign firms cannot directly retail many products through electronic services. Ownership for physical distribution, warehousing, and further logistics is limited to 67%, provided that each of these services is not ancillary to the main business line.

K. Iran

Filtering & Blocking

In May 2014, Iran blocked access to Google's hosting platform, Google Sites, and censored at least two Wikipedia pages.[312] 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.[313] Freedom House also ranked Iran as the third worst country for Internet freedom in its 2016 report.[314] In late 2014, reports from Iran suggested that 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, had spent $36 million to develop a "smart filtering" system intended to implement selective blocking of specific content.[315]

---

[310] *Id.* at 37 ("RIAs such as social media have been used to expand SMEs' transactions to wider consumers from different parts of the country. For example, 58% of SMEs on Facebook in Asia Pacific built their business on Facebook and 74% of SMEs on Facebook in Asia Pacific were able to increase sales because of Facebook. RIAs have also enabled people to communicate more efficiently and to disseminate information more effectively. Those apps have also helped Indonesian society in terms of addressing some of education and health issues.").

[311] *Indonesia and Thailand Target OTT Services*, LEXOLOGY (Feb. 5, 2018), https://www.lexology.com/library/detail.aspx?g=44d84bcc-652d-4a5a-a3e3-4778fae2e383 ("A foreign OTT service provider may be regarded as having a permanent establishment in Indonesia if (i) it owns, leases or controls any fixed premises in Indonesia, which may include a computer, a server, a data centre, an electronic agent or other automatic equipment; or (ii) it has employees or parties acting for or on its behalf to conduct business activities in Indonesia.").

[312] 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/.

[313] *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.

[314] *Internet Freedom 2016*, *supra* note 41. Freedom House previously ranked Iran as the worst country for Internet freedom in its 2014 report, and Iran tied for second worst in 2015.

[315] *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/.

L. Korea

Data and Infrastructure Localization

Industry reports that foreign Internet services are impeded from offering online maps, navigational tools, and related applications in Korea due to localization barriers on geospatial data. A new proposed bill would affect online service providers by imposing requirements to establish local servers in order to ensure user protection from deliberate diversion of traffic and slowed service. Penalties for not complying with this requirement would include up to a 3% fine based on revenue.

Localization requirements are in violation of the U.S.-Korea Free Trade Agreement (KORUS). By requiring foreign suppliers of data-related services to establish in-country processing facilities, these requirements violate KORUS Art. 12.5, which prohibits Korea from requiring U.S. firms to "establish or maintain . . . any form of enterprise . . . in its territory as a condition for the cross-border supply of a service."[316] Korea is further obligated under KORUS Art. 15.8 to "refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[317]

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 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.[318] 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.

---

[316] U.S.-S. Kor. Free Trade Agreement, June 30, 2007, art. 12.5, *available at* https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file315_12711.pdf.

[317] U.S.-S. Kor. Free Trade Agreement, June 30, 2007, art. 15.8, *available at* https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf.

[318] 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/.

Interconnection Pricing

Industry continues to express concerns over government attempts to regulate the Internet by asserting jurisdiction over transmissions through interconnection pricing.[319] Industry is becoming increasingly alarmed at foreign governments' attempts to regulate Internet interconnections using outdated approaches more apt to apply to traditional telephony. This approach artificially inflates bandwidth costs and limits competition. The effects of these measures are illustrated in the Republic of Korea. Korean regulations favor three Korean ISPs at the expense of foreign ISPs and smaller domestic ISPs. U.S. company Cloudflare's aggregate pricing per region jumped from $2.50 to $6.00 under new regulations that were introduced in 2016.

M. Mexico

Data Localization

Mexico should also resolve ambiguities surrounding the types of data that can be stored in the cloud following its recently enacted 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 Federal Government also published amendments to its ICT Policy on July 23 of this year. The amendments were directed to government institutions, and established that when contracting cloud computing services, public institutions must favor the processing of data within Mexico unless the amount of data exceeds the computing capacities of service providers located in Mexico. Many provisions in the amendments, including the data localization measures, are general and applicable to any kind of service required by federal institutions, but the amendment was exempted from public consultation and pre-publication rules on grounds of national security.

The USMCA provides a clear opportunity to resolve issues relating to cross-border data flows between U.S. and Mexico. The agreement is an important step in prohibiting government from interfering with data flows or the exchange of information online.

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

[319] CCIA Comments to USITC, In re Investigations No. 332-566 and No. 332-563 (Apr. 6, 2018), *available at* http://www.ccianet.org/wp-content/uploads/2018/04/CCIA-Comments-for-ITC-GDT-2-Report-GDT-3-Report.pdf at 17.

model into one more in line with the definite imports model.[320] 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 upcoming NTE, and encourage the Mexican government to ensure compliance with international trade commitments.

Taxation of Digital Services

Mexico is also considering a proposal that aims to tax online revenue generated within its borders, potentially based on a method of determining the "input" or "contribution" from domestic users.

N. 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

[320] 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.

innovative products and services."[321] One analysis concluded the guidelines "will prop up domestic technology enterprises at the expense of higher quality and/or more efficient foreign ones."[322]

O. Pakistan

Filtering & Blocking

Pakistan continues to intermittently block Twitter, YouTube, and Facebook,[323] while Facebook is also routinely asked by the government to censor material deemed "blasphemous".[324] The popular blog platform WordPress was also temporarily blocked for several days in 2015 with little explanation from authorities.[325] These blocks have cost the Pakistani GDP an estimated $69 million dollars in 2017.[326] Passed in August 2016, the Prevention of Electronic Crimes Act also introduced stronger censorship powers for authorities.[327]

P. 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 from copyright infringement claims against online intermediaries arising out of user activities.[328] Understanding this threat to foreign investment in Peru, USTR rightly cited this discrepancy in its inclusion of Peru in the 2017 Special 301 Report.[329] 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.

---

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

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

[323] Steve Kovach, *Twitter says it's being blocked by Pakistan's government*, BUSINESS INSIDER, Nov. 25, 2017, https://www.businessinsider.com/social-media-services-blocked-in-pakistan-2017-11.

[324] *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/.

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

[326] Darrell M. West, *Internet Shutdowns*, *supra* note 44, at 3.

[327] FREEDOM HOUSE, *Freedom on the Net 2017, Pakistan Country Profile* (2017), https://freedomhouse.org/report/freedom-net/2017/pakistan.

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

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

Q. Russia

Data and Infrastructure Localization

Russia signed localization measures into law in July of 2014, which went into effect on September 1, 2015.[330] 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.[331] In August 2015, the Ministry of Communications and Mass Media issued "clarifications" explaining the law's provisions, indicating that the localization requirements will apply to business activities that are "oriented towards" a Russian audience.[332] 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,[333] as well as the requirements to inform Russia's telecommunications authorities.[334] The threat to U.S. industry was illustrated when Russia blocked access to LinkedIn in 2016 over perceived violations of the law.[335] CCIA thanks USTR for emphasizing this issue in the 2018 NTE,[336] and hopes that USTR will continue to highlight this issue moving forward.

---

[330] 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.

[331] ECIPE predicted 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. These losses also reflect lost export opportunities for U.S. service providers. In the wake of the new law, 45,000 companies informed Roskomnadzor that they are currently in compliance with the law. 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/; Cohen, Gulyaeva, and Sedykh, *supra* note 236.

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

[333] 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

[334] 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/.

[335] 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.

[336] *2018 NTE*, *supra* note 4, at 400-01.

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.[337] 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."[338]

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.[339] 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.[340]

Russia amended its Information Law in 2017 to imposed additional requirements on virtual private networks (VPNs) and similar technologies.[341] While the law does not ban the use of VPNs, it does require VPN operators to prevent users in Russia from accessing websites that are blocked in Russia. Failure to comply can result in Russian authorities blocking the VPN and an additional rule is expected to impose administrative fines in cases where the operators fail to provide required information to authorities. In 2018, Russia blocked over 50 VPN and similar anonymization services that were being used to access Telegram, which Russia previously blocked following Telegram's refusal to share encryption keys to with Russian authorities.[342]

---

[337] 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.

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

[339] 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.

[340] 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.

[341] *Russian Telecommunications and Media Laws: Latest Developments*, MORGAN LEWIS (Feb. 28, 2018) (describing the changes made by Federal Law No. 276-FZ of July 29, 2017).

[342] Matthew Humphries, *Russia Blocks VPNs in Bid to Kill Telegram* PCMAG, (May 4, 2018), https://www.pcmag.com/news/360866/russia-starts-blocking-vpns-as-it-tries-to-kill-telegram.

Legal Liability for Online Intermediaries

The recently enacted "Mirrors Law" extends Russia's copyright strict enforcement rules[343] 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.[344] 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. Russia is considering possible amendments to the law due to mass uncertainty.[345]

"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.[346] 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 content at issue within 3 to 10 days, or the individual requesting deletion may go to court and get a warrant demanding removal of the information.[347]

Undue Restrictions on Over-the-Top Services

With the entry of Netflix into Russia in 2016, Russia sought immediately to further[348] restrict foreign ownership in media services, with a disproportionate effect on U.S.-based companies.[349] Last year, Russia adopted amendments to the Federal Law on Information, Information Technologies and Protection of Information and Certain Laws of the Russian Federation, targeted at over-the-top

---

[343] 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.

[344] *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.

[345] Andy, *Russia to Amend Copyright Law After Yandex was Forced to Remove Pirate TV Content*, TORRENTFREAK (Sept. 15, 2018), https://torrentfreak.com/russia-to-amend-copyright-law-after-yandex-forced-to-remove-pirate-tv-content-180915/

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

[347] *Id*.

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

[349] Vladimir Kozlov, *Netflix Continues Operating in Russia Despite Foreign Ownership Restrictions*, THE HOLLYWOOD REPORTER (July 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.").

(OTT) platforms that also provide audiovisual content.[350] 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.[351] 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.[352]

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.[353] Failure to comply may result in a country-wide block of the service.

R. Saudi Arabia

Data and Infrastructure Localization

The Communications and Information Technology Council of Saudi Arabia (CITC) issued the Cloud Computing Regulatory Framework in 2018.[354] The document contains a provision on data localization that may restrict access to the Saudi market for foreign Internet services. The regulation will also increase ISP liability, create burdensome new data protection and classification obligations, and require compliance with cybersecurity and law enforcement access provisions that depart from

[350] 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).

[351] Gail Crawford & 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/.

[352] 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.

[353] 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.

[354] Communications and Information Technology Commission, Cloud Computing Regulatory Framework (Saudi Arabia) (2018), http://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx.

global norms and security standards. CITC would be granted broad powers to require cloud and ICT service providers to install and maintain governmental filtering software on their networks.

Customs Barriers

In 2018, Saudi Arabia began enforcing a new product compliance regulation that imposes import barriers to the Saudi market.[355] The new regulations impose several additional requirements on international shipments, including registration requirements, additional documentation that must be uploaded to online portals,[356] obtaining prior authorization for officials, payment of additional fees, and submission of legal declarations. Specific product categories such as wireless electronic devices require additional permits from the Saudi Telecom regulator. Industry also reports extensive documentation requirements that depart from global practice in developed countries.[357]

S. Thailand

Filtering and Blocking

In December 2016, Thailand's National Legislative Assembly passed amendments to the 2007 Computer Crime Act.[358] The amendments became effective in 2017 and five Ministerial Notifications were issued last August outlining regulations and procedures pursuant to the amendments to the Act.[359] These changes greatly expanded the authority of the Thai government to regulate content online and led to the "lowest level" of Internet freedom yet in Thailand.[360]

[355] International Electrotechnical Commission for Electrotechnical Equipment (IECEE Certification).

[356] Industry reports that these include several technical documents from foreign manufactures including test reports, manufacturer certifications, and translations.

[357] Industry reports that customs officials require several sets of original signed and stamped international shipping and customs documents. In most developed countries customs formalities are completed with commercial invoice copies only, Saudi custom rules require importers to provide original copies from the origin shipper signed, stamped, and legalized by origin Chamber of Commerce offices. Failure to satisfy these requirements results in fines and shipment delays.

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

[359] 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/.

[360] 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. Freedom House, Freedom on the Net 2017, Thailand Country Profile (2017), https://freedomhouse.org/report/freedom-net/2017/thailand.

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.[361]

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 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.[362] The government is also developing legislation to further expand government surveillance powers to enforce such laws, which is expected to be submitted for cabinet approval in 2018.[363]

Legal Liability for Online Intermediaries

The lack of clear 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."[364] 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

[361] 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.

[362] 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.

[363] *Updates on the Thai Cybersecurity Bill*, BAKER MCKENZIE (Oct. 12, 2018), https://www.bakermckenzie.com/en/insight/publications/2018/10/updates-on-the-thai-cybersecurity-bill; 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.'"). The bill is expected to be submitted for cabinet consideration at the end of 2018. *Cybersecurity Bill to be Presented to Cabinet This Month*, BANGKOK POST (Sept. 15, 2018), https://www.bangkokpost.com/business/news/1540202/cybersecurity-bill-to-be-presented-to-cabinet-this-month.

[364] 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.

mandated timeframes for removal vary across content types.[365] Without strict compliance with the notification requirements,[366] a service provider will be subject to the same penalty as if they uploaded the content themselves.[367]

T. Turkey

Data Localization

The Capital Markets Board of Turkey published the Communique on Information Systems Management (VII-128.9) in early 2018.[368] This requires publicly traded companies to keep their primary and secondary information systems, data and infrastructure in the country.

Filtering & Blocking

CCIA has previously noted barriers to social media such as Twitter and YouTube in Turkey,[369] 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.'"[370] The recent unrest in Syria, and subsequent attempted coup against 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

[365] 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/.

[366] 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/.

[367] Danny O'Brien & 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 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.").

[368] Serra Hiziroglu & Ayça Sarıkamış, *Communiqués Recently Published by Capital Markets Board on Information Systems Management and Independent Audit of Information Systems*, LEXOLOGY (Feb. 7, 2018), https://www.lexology.com/library/detail.aspx?g=c6601e1b-6d4b-40c6-81ed-834fc60cea3c.

[369] 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.

[370] *Turkey, Enemy of the Internet?*, REPORTERS WITHOUT BORDERS (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.

sites.[371] 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.[372] Use of this law may have led to immediate shutdowns of various social media sites in Turkey.[373]

In 2017, Cloudflare was taken offline making multiple popular websites hosted on the Cloudflare content delivery network unavailable.[374] While the underlying causes were not clear, "similar issues have previously been connected to attempts by [Turkish] authorities to block individual websites or filter specific content."[375] During 2018 elections, Turkish authorities utilized a "rapid response team" to block "abnormal" content on social media and online platforms.[376]

U. Uganda

Undue Restrictions on Over-the-Top Services

The Ugandan government began collecting a tax on OTTs this past July and is expected to have a negative impact on local Internet services.[377] This "social media" tax requires end users to pay UGX 200 (USD $0.05) per day for the use of 60 mobile apps, including Facebook, Instagram,

---

[371] 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.

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

[373] *Id*.

[374] *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/.

[375] *Id*.

[376] *Turkey to Implement Cyber-security and Social Media Blocking Measures During June Elections*, TURKEY BLOCKS (May 25, 2018), https://turkeyblocks.org/2018/05/25/turkey-cyber-security-social-media-blocking-june-elections/.

[377] The tax is expected to have a negative impact on local Internet services. *See* Elias Biryabarema, *Uganda's Social Media Tax Will Harm Business, Deter Investment: Executives*, REUTERS (July 30, 2018), https://www.reuters.com/article/us-uganda-internet/ugandas-social-media-tax-will-harm-business-deter-investment-executives-idUSKBN1KK1T3 ("Sefik Bagdadioglu, regional director for online retailer Jumia, told Reuters he worried the tax measure would curb Internet use by lower-income Ugandans, potentially putting them beyond the firm's reach. 'A significant portion of Jumia customers use social media to log into their accounts, see what we do, share our deals and events,' Bagdadioglu said. 'A decline in social media use is likely to have an adverse impact on our business.'"); Emily Dreyfuss, *Uganda's Regressive Social Media Tax Stays, at Least For Now*, WIRED (July 19, 2018), https://www.wired.com/story/uganda-social-media-tax-stays-for-now/ ("'The primary motivation behind [the social media tax] is to silence speech, to reduce the spaces where people can exchange information, and to really be able to control, with the recognition that online platforms have become the more commonly used way for sharing information,' says Joan Nyanyuki, Amnesty International Regional Director for East Africa, the Horn, and the Great Lakes.").

WhatsApp, and Twitter. An end user's failure to pay the tax on any given day results in the person being blocked from accessing any of the OTT services.

V. Ukraine

Legal Liability for Online Intermediaries

As USTR observed in the previous NTE, Ukraine adopted a law — "On State Support of Cinematography in Ukraine" — in March 2017 which established a notice and takedown system for copyright enforcement.[378] However, the final law goes beyond what the notice and takedown system under Section 512 of the DMCA requires in the United States and in the many U.S. trading partners who have adopted similar systems for FTA compliance.

The legislation revised 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 is inconsistent with the "expeditious" standard under U.S. copyright law.[379] The law also effectively imposed 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. USTR noted the obligations and responsibilities are too ambiguous and onerous in the 2018 NTE and CCIA reiterates that these concerns should be included in the 2019 NTE.[380]

W. United Arab Emirates

Undue Restrictions on Over-The-Top Services

The UAE's main telecommunications providers, Etisalat and du, began blocking the majority of OTT video and messaging services in 2017. This discriminatory practice provides telecommunications providers an unfair competitive advantage as it allows them to restrict access to new and innovative technologies. USTR should encourage the UAE regulators to consider revising its regulatory framework to prevent the operators from blocking such services.

---

[378] 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).

[379] 17 U.S.C. § 512(1)(C).

[380] *2018 NTE, supra note* 4, at 472.

X. Vietnam

Data Localization

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

Vietnam is also using cybersecurity policies as a means to further impose localization mandates. The National Assembly passed the Law on Cybersecurity in June 2018 and it will take effect on January 1, 2019. The lack of clarity around obligations regarding commercial presence and data localization[381] is concerning. While the law removed concerning provision from the draft that specifically mandated server localization, the law still imposes localization requirements that will place significant burdens on U.S. exporters and discourage investment.[382] The law also mandates that service providers develop mechanisms to monitor and remove content within 24 hours after a request from government authorities regarding prohibited content.[383]

Legal Liability for Online Intermediaries

Vietnam's Decree No. 55 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."[384] This prohibited content includes behaviors that are, in the law's words,

---

[381] Article 26.3 provides that "Domestic and foreign enterprises providing services on telecommunication networks or the internet or value-added services in cyberspace in Vietnam with activities of collecting, exploiting, analyzing, and processing personal information data, data on the relationships of service users, or data generated by service users in Vietnam must store such data in Vietnam for the period prescribed by the government.", https://www.lexology.com/library/detail.aspx?g=d9c3ec0d-500c-4f6c-aed1-dfb0a20e1f62

[382] *Updates to the Draft Cybersecurity Law*, BAKER MCKENZIE (Mar. 2018), https://www.bakermckenzie.com/en/insight/publications/2018/03/updates-draft-cybersecurity-law.

[383] *Vietnam's Controversial New Cybersecurity Law Raises Questions*, LEXOLOGY (Aug. 28, 2018), https://www.lexology.com/library/detail.aspx?g=d9c3ec0d-500c-4f6c-aed1-dfb0a20e1f62.

[384] 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.

"seditious, libelous, defamatory, obscene and violent, and those that constitute hate speech or disclose State secrets."[385]

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.[386] 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 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,[387] Internet 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.[388]

---

[385] *Id*. at 3.

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

[387] *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.

[388] *See 2018 Key Barriers to Digital Trade*, *supra* note 5.