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

In re Request for Comments to Compile the National Trade Estimate Report on Foreign Trade Barriers	Docket No. USTR-2019-0012

COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION
REGARDING FOREIGN TRADE BARRIERS TO U.S. EXPORTS
FOR 2020 REPORTING

October 31, 2019

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 84 Fed. Reg. 46,079 (Sept. 3, 2019), the Computer & Communications Industry Association (CCIA)[1] submits the following comments for consideration as USTR composes its annual National Trade Estimate Report on Foreign Trade Barriers (NTE).

CCIA welcomes USTR's continued focus and renewed commitments to reducing barriers to digital trade. The Internet remains an integral component to international trade in both goods and services and is also a key driver to development, enabling SMEs to reach new markets and serve customers around the world. In 2017, the digital economy accounted for 6.9% of GDP, $1.35 trillion, in the United States.[2]

These gains are facing growing threats from countries who continue to adopt laws and regulations that hinder growth and cross-border delivery of Internet services. Under the guise of promoting domestic champions, protecting national security, and upholding privacy, countries are adopting discriminatory policies that disadvantage, and often target, U.S. technology companies and pose significant barriers to the delivery of Internet-centric products and 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.

For the 2020 National Trade Estimate report, CCIA identifies barriers to trade facing U.S. Internet and digital exporters that relate to the following: (1) restrictions on cross-border data flows and data and infrastructure localization mandates, (2) government-imposed restrictions on Internet content and related access barriers, (3) digital taxation, (4) market-based platform regulation, (5) copyright liability regimes for online intermediaries, (6) imbalanced copyright laws and "link taxes", (7) extraterritorial regulations and judgments, (8) customs duties on electronic transmissions, (9) backdoor access to secure technologies, and (10) market access barriers for communications providers. 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] CCIA represents technology products and services providers of all sizes, including computer hardware and software, electronic commerce, and telecommunications and Internet products and services. A list of CCIA members is available at https://www.ccianet.org/members.

[2] BUREAU OF ECONOMIC ANALYSIS, Measuring the Digital Economy: An Update Incorporating Data from the 2018 Comprehensive Update of the Industry Economic Accounts (2019), *available at* https://www.bea.gov/system/files/2019-04/digital-economy-report-update-april-2019_1.pdf; BUREAU OF ECONOMIC ANALYSIS, Digital Economy Accounted for 6.9 Percent of GDP in 2017 (Apr. 4, 2019), https://www.bea.gov/news/blog/2019-04-04/digital-economy-accounted-69-percent-gdp-2017.

Table of Contents

I. INTRODUCTION

The United States is a world leader in high-tech innovation and Internet technology — a central component of cross-border trade in both goods and services.[3] The removal of foreign obstacles to Internet-enabled international commerce and export of Internet-enabled products and services is thus increasingly critical to the growth of the American economy. Internet-enabled commerce represents a significant, yet still growing, sector of the global economy. Since 1998, the digital economy grew at an annual rate of 9.9%, compared to 2.3% overall economic growth.[4] In 2017, the digital economy accounted for 6.9% of GDP, or $1.35 trillion, in the United States.[5]

This sector is a key driver to international trade in an increasingly digitalized global economy. As a McKinsey report observed, "virtually every type of cross-border transaction now has a digital component".[6] Internet-enabled trade also is critical for development, and presents new opportunities to grow local economies.[7] The Internet also empowers small platforms to reach new markets. Research conducted by eBay shows that 97% of eBay-enabled small businesses export abroad, compared to only 1% of traditional businesses.[8] This is widespread,

---

[3] 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).

[4] BUREAU OF ECONOMIC ANALYSIS, Measuring the Digital Economy: An Update Incorporating Data from the 2018 Comprehensive Update of the Industry Economic Accounts (2019), *available at* https://www.bea.gov/system/files/2019-04/digital-economy-report-update-april-2019_1.pdf; BUREAU OF ECONOMIC ANALYSIS, Digital Economy Accounted for 6.9 Percent of GDP in 2017 (Apr. 4, 2019), https://www.bea.gov/news/blog/2019-04-04/digital-economy-accounted-69-percent-gdp-2017.

[5] *Id*. *See also* INTERNET ASSOCIATION, Measuring the U.S. Internet Sector 2019, *available at* https://internetassociation.org/wp-content/uploads/2019/09/IA_Measuring-The-US-Internet-Sector-2019.pdf (using Bureau of Economic Analysis data to calculate that the "internet sector" contributed to $2.1 trillion to the U.S economy in 2018, created 6 million direct jobs to the U.S. economy, and that the "internet sector" invested over $60 billion into the U.S. economy in 2018).

[6] MCKINSEY INSTITUTE, Digital Globalization The New Era of Global Flows (Feb. 2016), *available at* https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.

[7] WORLD TRADE ORGANIZATION, World Trade Report 2019 (2019), *available at* https://www.wto.org/english/res_e/booksp_e/00_wtr19_e.pdf ("Digital technologies can be a driver of inclusivity in services trade, by dramatically cutting costs and lowering barriers to entry. This is true for developing countries, and it is true for smaller businesses. Micro, small and medium-sized enterprises (MSMEs) that offer services are on average two years younger when they start exporting as compared to manufacturing MSMEs. New technologies have facilitated this faster access to international markets as MSMEs' participation in services trade is frequently in digitizable services, such as professional and scientific activities."). *See also* Joshua Meltzer, A Digital Trade Policy for Latin America and the Caribbean (Aug. 2018), *available at* https://publications.iadb.org/en/digital-trade-policy-latin-america-and-caribbean.

[8] eBay Main Street, Global Trade At a Glance, https://www.ebaymainstreet.com/issues/global-trade (last visited Oct. 31, 2019).

with 61% of these small sellers reaching customers on four or more continents. It is not merely e-commerce services that serve as a facilitating role in promoting trade. Data collected through the Future of Business Survey, a project between Facebook, the OECD, and the World Bank, shows how social media platforms enable exports.[9] The Survey data was collected through businesses' responses to their interactions on Facebook and perspectives on trade issues that affect their ability to export.[10] A recent industry report shows that small businesses are exporting at an increasing rate, and 92% of those SMEs surveys reported that they use digital tools such as online payment processing tools, online productivity tools, e-commerce websites, and online marketing.[11]

The global Internet penetration rate reached 51% in 2018, and it is critical that the Internet remains an open platform for users across the world.[12] International markets continue to present the most significant growth opportunities for major U.S. companies, even as international competition has grown. 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.

The United States should 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,

---

[9] OECD, The Future of Business Survey, http://www.oecd.org/sdd/business-stats/the-future-of-business-survey.htm (last visited Oct. 31, 2019).

[10] Utilizing this data, the Mercatus Center has a series of policy briefs breaking down these numbers and highlighting that firms using Facebook have a higher propensity to export. The data shows that businesses, particularly small businesses, utilizing online platforms have a higher propensity to engage in international trade than traditional firms. 6.75 percent of U.S. small and medium-sized businesses (SMBs) on Facebook engage in international trade, compared to 4.33 percent of SMBs not on Facebook. In other reporting countries, the share of businesses who were engaged in trade was up to 30.9 percent (Bangladesh), with other high shares reported in businesses located in Nigeria, Egypt, Portugal, Pakistan, and the Czech Republic. *See* Mercatus Center, Businesses on Facebook and Propensity to Export: The United States (Feb. 2019), https://www.mercatus.org/system/files/mcdaniel_and_parks_-_policy_brief_-_digital_platforms_small-_and_medium-sized_businesses_-_v1_0.pdf.

[11] Additionally, 61 percent of all small businesses surveyed believe that technology is key to overcoming top barriers to trade including foreign regulations. *See* U.S. Chamber of Commerce Technology Engagement Center and Google, *Growing Small Business Exports: How Technology Strengthens American Trade* (2019), available at https://americaninnovators.com/wp-content/uploads/2019/10/CTEC_GoogleReport_v7-DIGITAL-opt.pdf.

[12] Internet Trends 2019 Report, https://www.bondcap.com/report/itr19/#view/9 at 9.

provide, or rely on Internet technologies. To fully realize this goal, the United States should pursue a trade agenda and craft agreements that will reflect our global digital economy and set the stage for all future trade agreements. The United States set the gold standard for digital trade rules in the negotiations of the U.S.-Mexico-Canada Agreement (USMCA), which also serves as the basis of the U.S.-Japan Digital Trade Agreement. Industry is also strongly encouraged by reports that the United States is pursuing this gold standard at the WTO in the context of ongoing e-commerce discussions which is a key opportunity for global agreement on digital trade rules.[13]

Continued U.S. leadership on digital trade rules is critical for the continued growth of the U.S. digital economy, and the NTE is a beneficial tool to identify regions where this leadership is most needed. CCIA thanks USTR for highlighting digital trade as a key priority for the Administration in the 2019 National Trade Estimate Report, 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.[14]

II. PROMINENT DIGITAL TRADE-RELATED BARRIERS

This section provides an overview of the predominant barriers to digital trade that are identified in countries included in CCIA's comments. Other barriers, in addition to the ten outlined in this section below, are also included in country profiles in Section III such as customs and shipments requirements, regulations on "over-the-top" (OTT) services, and asymmetric competition policies.

1. Restrictions on Cross-border Data Flows and Data and Infrastructure Localization Mandates

Open data flows are critical for continued global economic growth.[15] As CCIA has noted in previous NTE filings, a number of countries continue to pursue data localization policies, including mandated server localization and data storage. In a 2017 report, the USITC included

[13] Bryce Baschuk, *U.S. WTO E-Commerce Offer Reflects USMCA Digital Trade Chapter*, BLOOMBERG LAW (May 6, 2019), https://news.bloomberglaw.com/international-trade/u-s-wto-e-commerce-offer-reflects-usmca-digital-trade-chapter.

[14] OFFICE OF THE U.S. TRADE REP., National Trade Estimate Report 2019, *available at* https://ustr.gov/about-us/policy-offices/press-office/press-releases/2019/march/ustr-releases-2019-national-trade [hereinafter "2019 NTE Report"].

[15] MCKINSEY GLOBAL INSTITUTE, *The Ascendancy of International Data Flows* (Jan. 9, 2017) (estimating that the global flows of goods, services, finance, and people increased world gross domestic product by at least 10% in the past decade).

estimates that such localization measures have doubled in the last six years.[16] Since that time, countries continue to pursue policy and regulatory frameworks that restrict the free flow of information across borders.

Citing domestic privacy protections, defense against foreign espionage, law enforcement needs, and the promotion of local economic development, foreign governments are pursuing these policies at an increasing rate. While rarely the stated intention, many of these policies have the effect of inhibiting foreign competitors from entering 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.[17] Data localization rules often centralize information in hotbeds for digital criminal activity, working against data security best practices that emphasize decentralization over single points of failure. 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.[18]

Rather than promote domestic industry, data localization policies are likely to hinder economic development and restrict domestic economic activity,[19] and impede global

---

[16] 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"].

[17] 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.

[18] 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.

[19] *See* Nigel Cory, *The False Appeal of Data Nationalism: Why the Value of Data Comes from How It's Used, Not Where It's Stored*, INFORMATION TECHNOLOGY & INFORMATION FOUNDATION (2019), *available at* https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where ("[The] supposed benefits of data-localization policies, including the stimulus to jobs, are incorrect. One expected benefit is that forcing companies to store data inside a country's borders will produce a boom in domestic data center jobs. In fact, while data centers contain expensive hardware (which is usually imported) and create some temporary construction jobs, they employ relatively few staff. Data centers are typically highly automated, using artificial intelligence, which allows a small number of workers to operate a large facility."); Matthias Bauer, et al, *Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization*, GLOBAL COMMISSION ON INTERNET GOVERNANCE (May 2016), *available at* https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf; EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY, The Costs of Data Localisation: Friend Fire on Economic Recovery (2014), *available at* http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf at 2 ("The impact of recently proposed or enacted legislation on GDP is substantial in all seven countries: Brazil (-0.2%), China (-1.1%), EU (-0.4%), India (-0.1%), Indonesia (-0.5%), Korea (-0.4%) and Vietnam (-1.7%). These changes significantly affect post-crisis economic recovery and can undo the productivity increases from major trade agreements, while economic growth is often instrumental to social stability. . . If these countries would also introduce economy-wide data localisation

competitiveness.[20] Data localization policies also frequently violate international obligations, including GATS commitments. To remain compliant with international trade rules, measures that restrict trade in services must be necessary to achieve specific legitimate national security or public policy objectives, and must not be applied in a discriminatory manner or in a way that amounts to a disguised restriction on trade in services.[21] 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.[22]

In Latin America, there is a concerning trend where countries that are advancing legislation that will further restrict data transfer across borders.[23] Largely influenced by the EU's

---

requirements that apply across all sectors of the economy, GDP losses would be even higher: Brazil (-0.8%), the EU (-1.1%), India (-0.8%), Indonesia (-0.7%), Korea (-1.1%)."); 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).

[20] 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."); Nigel Cory, *Cross-Border Data Flows: What Are the Barriers, and What Do They Cost?* (May 2017), *available at* https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost 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.").

[21] Article XIV - XIV 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).

[22] See Chander & Lê, Data Nationalism, *supra* note 17; 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"].

[23] Panama, 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* Stacy Palker, *Data Privacy Law Across Latin America*, MONDAQ (Apr. 8, 2019), http://www.mondaq.com/brazil/x/797024/Data+Protection+Privacy/Data+privacy+laws+across+Latin+America; *Data Protection Regulation in Latin America and the Impact of the GDPR*, GARRIGUES (May 24, 2018), https://www.garrigues.com/en_GB/new/data-protection-regulation-latin-america-and-impact-gdpr; *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_Modelv2.pdf.

General Data Protection Regulation (GDPR), countries in this region are revising domestic privacy laws to further restrict data flows and trade within the region. In the Middle East, industry reports persistent data localization measures across the region, exacerbated by recent geopolitical tensions. For example, in the UAE, banks and insurance companies are required to keep data within the country. In Saudi Arabia, industry reports that the Communications and Information Technology Commission is pressuring cloud customers to roll back non-domestic deployments.

Further concerning is that some countries are using data localization policies as a means to advance domestic industries and as a tool for development. The UN Conference on Trade and Development (UNCTAD) released a concerning document in 2018,[24] echoing similar arguments made by countries that have pursued strict data localization measures. These countries have also tried to use the ongoing WTO e-commerce negotiation process to advocate for these restrictions and undermine the process to achieve global rules.[25] Continued opposition from U.S. and like-minded allies is needed at the multilateral stage in light of these growing trends.[26]

2. Government-Imposed Content Restrictions and Related Access Barriers

i. Online Content Regulations

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. While ostensibly in pursuit of legitimate and valid goals to address illegal content online, many of the proposals are expansive in scope and will conflict with U.S. law and free expression values. Another concerning trend in recent years is authoritarian governments pursuing content regulations to fight "fake news" that have the effect of targeting dissidents and political opposition.[27]

---

[24] UNCTAD, *Trade and Development Report 2018 Power, Platforms, and the Free Trade Delusion*, *available at* https://unctad.org/en/PublicationsLibrary/tdr2018_en.pdf.

[25] Kumar Uttam & Rezaul H. Laskar, *India Won't Back Down on Its Plan for Mandatory Data Localisation*, HINDUSTAN TIMES (July 5, 2019), https://www.hindustantimes.com/india-news/india-firm-on-its-proposal-for-mandatory-data-localisation/story-xILV14GhqxTmMAd1IoW0zL.html.

[26] Industry supports these negotiations and recently released a position paper outlining priorities for the discussions. *See* Global Industry Position Paper on the WTO E-Commerce Initiative, *available at* https://www.itic.org/dotAsset/f2de6c22-e286-47d2-aca7-ba34830e462c.pdf (Oct. 2019).

[27] *See North Korea's KCNA, Russian TASS News Agency Hope to Fights 'Fake News'*, BBC (Oct. 9, 2019) https://monitoring.bbc.co.uk/product/c20157yl; *Fake News, Data Collection, and the Challenges to Democracy* (2018), FREEDOM HOUSE, Freedom on the Net 2018 Report (2018), *available at* https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism#fotn18-section-citing-fake-news-governments-curb-online-dissent [hereinafter "2018 Freedom on the Net Report"] ("Like "terrorism," the

Internet services recognize the importance of ensuring user trust in their platforms. In recent years, companies have significantly increased resources to ensure their services remain spaces for free expression, users comply with their terms of service, and that illegal content is identified and removed from their platform. These measures include initiatives on combating online misinformation,[28] quickly detecting and removing terrorist and extremist content,[29] and working with brand owners and rightsholders to remove counterfeit products from their services.[30] Continued collaboration with stakeholders is key to build upon these measures.

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. When Internet services exit a market, local small and medium-sized enterprises are denied Internet-enabled access to the global marketplace, similarly discouraging investment in and growth of domestic startups. While U.S. Internet businesses have thrived domestically under carefully crafted legal frameworks, international asymmetries in liability rules frequently favor domestic plaintiffs.

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

---

term "fake news" has been co-opted by authoritarian leaders to justify crackdowns on dissent. Deliberately falsified or misleading content is a genuine problem, but some governments are using it as a pretext to consolidate their control over information. In the past year, at least 17 countries approved or proposed laws that would restrict online media in the name of fighting "fake news" and online manipulation.").

[28] *See*, *e.g.*, Danielle Abril, *Google Introduces New Tools to Help Journalists Fight Fake News*, Fortune (Mar. 20, 2019), https://fortune.com/2019/03/20/google-new-tools-fight-fake-news/; Henry Silverman, *The Next Phase in Fighting Misinformation*, FACEBOOK NEWSROOM (Apr. 10, 2019), https://newsroom.fb.com/news/2019/04/tackling-more-false-news-more-quickly/; Katharina Borchert, *The Mozilla Information Trust Initiative: Building a movement to fight misinformation online*, THE MOZILLA BLOG (Aug. 8,2017), https://blog.mozilla.org/blog/2017/08/08/mozilla-information-trust-initiative-building-movement-fight-misinformation-online/.

[29] *See* Global Internet Forum to Counter Terrorism, https://gifct.org/ (last visited Oct. 31, 2019).

[30] CCIA Comments to Dep't Of Commerce, *In re* Comments Request: Report on the State of Counterfeit and Pirated Goods Trafficking and Recommendations, filed July 29, 2019, at 2-5, *available at* http://www.ccianet.org/wp-content/uploads/2019/07/DOC-2019-0003-0001-CCIA-Comments-Counterfeiting-Pirated-Goods-Trafficking-Report.pdf (detailing industry practices to address counterfeits online).

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.[31]

ii. Censorship and Internet Shutdowns

Among the most explicit barriers to digital trade are the outright filtering and blocking of U.S. Internet platforms and online content, a trend that continues to grow. As the Washington Post Editorial Board recently observed, more governments are shutting down the Internet with disastrous consequences.[32] In its most recent annual report, Freedom House determined that "global internet freedom declined for the eighth consecutive year in 2018.[33] Internet shutdowns are also costly, with one study finding that countries lose $23.6 million (per 10 million in population) for every day that the Internet is shut down.[34] 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.

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 Brookings Institution study estimated the global loss of intermittent

---

[31] Jonathan Band, *Keeping the DMCA's Grand Bargain in NAFTA*, DISRUPTIVE COMPETITION PROJECT (Oct. 2, 2017), https://www.project-disco.org/intellectual-property/100217-keeping-dmcas-grand-bargain-nafta (noting that intermediary protections regarding copyright content have been included in free trade agreements with Australia, Bahrain, Chile, Central America (Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras and Nicaragua), Morocco, Oman, and Singapore, Colombia, Korea, and Panama, as well as the Trans-Pacific Partnership Agreement). For why intermediary protections are needed in trade agreements, *see* Rachael Stelly, *Setting the Digital Standard for U.S. Trade Agreements*, DISRUPTIVE COMPETITION PROJECT (Aug. 9, 2019), http://www.project-disco.org/21st-century-trade/080919-setting-the-digital-standard-for-u-s-trade-agreements.

[32] *More Governments are Shutting Down the Internet. The harm is Far-Reaching*, WASH. POST (Sept. 7, 2019), https://www.washingtonpost.com/opinions/more-governments-are-shutting-down-the-internet-the-harm-is-far-reaching/2019/09/06/ace6f200-d018-11e9-8c1c-7c8ee785b855_story.html. *See also* ACCESS NOW, Fighting Internet Shutdowns Around the World (2018), https://www.accessnow.org/cms/assets/uploads/2018/06/KeepItOn-Digital-Pamphlet.pdf.

[33] FREEDOM HOUSE, The Rise of Digital Authoritarianism (Oct. 2018), https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

[34] 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-InternetConnectivity-Deloitte.pdf.

blackouts at no less than $2.4 billion in one year.[35] 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.[36]

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.[37] As CCIA has previously stated in its NTE comments,[38] 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, minimal restrictiveness, and due process to affected parties.

3. Digital Taxation

An alarming trend among foreign countries is the singling out of the U.S. digital economy for additional taxation.[39] To date, the following countries have introduced, or signaled that they will introduce, direct taxes on the digital economy: Austria, Belgium, Canada, Czech Republic, Denmark, Egypt, Greece, Hungary, India, Indonesia, Italy, Kenya, Mexico, Pakistan,

---

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

[36] WORLD ECONOMIC FORUM, Internet Fragmentation: An Overview at 35-36 (2016), http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

[37] Alexander Chipman Koty, *China's Great Firewall: Business Implications*, CHINA BRIEFING (June 1, 2017), https://www.china-briefing.com/news/chinas-great-firewall-implications-businesses/.

[38] CCIA Comments to USTR, *In re Request for Public Comments to Compile the National Trade Estimates Report on Foreign Trade Barriers*, filed Oct. 30, 2018 *available at* https://www.ccianet.org/wp-content/uploads/2018/10/CCIA-Comments-to-USTR-for-2019-NTE.pdf [hereinafter "CCIA 2018 NTE Comments"].

[39] *See* Parliament of Australia, France's Digital Services Tax, https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2019/August/Digital_Services_Taxation.

Poland, Russia,[40] Spain, Turkey, and the UK.[41] Many others are currently holding consultations on the issue of digital taxation.[42] Often based on inaccurate estimates, some countries assert that digital services fail to pay adequate taxes and should be subject to additional taxation.[43] These proposals that have 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. To that end, CCIA strongly supports the Section 301 investigation against France regarding its Digital Services Tax passed into law this summer.[44]

Changes to international taxation may be warranted in the increasingly globalized economy, but these changes should not be carried out unilaterally, or 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, a multilateral, 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 2018 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.[45] The OECD also cautioned in October that "uncoordinated unilateral tax measures, including measures that tax gross revenues . . . would undermine the relevance and sustainability of the international tax framework, and would damage global investment and growth."[46] To that

---

[40] Elke Asen, *Announced, Proposed, and Implemented Digital Services Taxes in Europe*, TAX FOUNDATION (July 18, 2019), https://taxfoundation.org/digital-taxes-europe-2019/.

[41] *See* KPMG, Taxation of the Digitalized Economy Developments Summary, https://tax.kpmg.us/content/dam/tax/en/pdfs/2019/digitalized-economy-taxation-developments-summary.pdf (updated Oct. 15, 2019).

[42] *See, e.g.,* New Zealand section of these comments, *infra* p. 75.

[43] 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/.

[44] *See* Submission of CCIA In Re Section 301 Investigation of French Digital Services Tax Docket No. USTR 2019-0009 (filed Aug. 19, 2019), *available at* http://www.ccianet.org/wp-content/uploads/2019/08/USTR-2019-0009-CCIA-Written-Comments-on-French-Digital-Tax.pdf.

[45] OECD, TAX CHALLENGES ARISING FROM DIGITILISATION – Interim Report 2018, http://www.oecd.org/tax/taxchallenges-arising-from-digitalisation-interim-report-9789264293083-en.htm.

[46] OECD Public Consultation Document, Secretariat Proposal for a "Unified Approach" Under Pillar One, *available at* https://www.oecd.org/tax/beps/public-consultation-document-secretariat-proposal-unified-approach-pillar-one.pdf.

end, CCIA strongly supports the efforts of the OECD in its ongoing process to reach consensus on multilateral rules for taxation in light of digitalization. The OECD is making significant progress, evidenced by the draft framework released in October 2019, and countries should let the process continue under the current timeframe to deliver a solution by 2020 before imposing national taxes that undermine this progress.[47]

4. Market-based Platform Regulation

The idea of "platform regulation" is spurring measures around the world, including the EU,[48] Japan,[49] and Australia.[50] In some cases, platform regulation serves as a backdoor for outcome-oriented competition policy and often targets leading U.S. Internet services. The effectiveness of such proposals has been called into question to the extent it serves the purposes of promoting innovation in the tech sector.[51]

5. Copyright Liability Regimes for Online Intermediaries

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 on intermediaries that have had no role in the development of objectionable content. 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. Another concerning trend is the

---

[47] This was reaffirmed by the G20 Finance Ministers following meetings on October 18-19. Press Release, G20 Press Release on International Taxation, Japan Ministry of Finance, https://www.mof.go.jp/english/international_policy/convention/g20/g20_191018it.htm ("We reaffirm our full support for a consensus-based solution with a final report to be delivered by the end of 2020. With a view to meeting this ambitious timeline, we stress the importance of the Inclusive Framework on BEPS agreeing to the outlines of the architecture by January 2020. The outlines will include a determination of the nature of, and the interaction between, both Pillars. We welcome the OECD Secretariat's efforts for the proposed unified approach under Pillar 1.").

[48] See discussion on the EU Platform to Business Regulation in Section III.

[49] *Japan Likely to Seek More Transparency From Digital Platform Businesses*, WHITE & CASE (June 6, 2019), https://www.whitecase.com/publications/alert/japan-likely-seek-more-transparency-digital-platform-businesses.

[50] *Australia Considers More Regulation of Google and Facebook*, CNBC (July 26, 2019), https://www.cnbc.com/2019/07/26/australia-considers-more-regulation-of-google-and-facebook.html.

[51] Mark MacCarthy, *To Regulate Digital Platforms, Focus on Specific Business Sectors*, BROOKINGS (Oct. 22, 2019), *available at* https://www.brookings.edu/blog/techtank/2019/10/22/to-regulate-digital-platforms-focus-on-specific-business-sectors/ ("[Various platform proposals] each seek to define the scope of a new regulatory regime based on the standard conception of digital platforms as digital companies that provide service to two different groups of customers and experience strong indirect network effects. The bad news is that this conception will not work. It is either too inclusive and covers vast swaths of U.S. industry, or so porous that it allows companies to escape regulation at their own discretion by changing their mode of business operation.").

failure of current U.S. trading partners to fully implement existing carefully negotiated intermediary protections in free trade agreements.[52] This is illustrated by Australia and Colombia's continued lack of compliance.

As discussed in the EU section of these comments, the recent EU Copyright Directive poses an immediate threat to Internet services and the obligations set out in the final text depart significantly from global norms. Laws made pursuant to the Directive will deter Internet service exports into the EU market due to significant costs of compliance.

6. Imbalanced Copyright Laws and "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.[53] 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.[54] 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.[55] 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.

Balanced copyright provisions are also a defining aspect of U.S. trade policy. Beginning with free trade agreements with Chile and Singapore in 2003, every modern U.S. trade agreement has ensured some measure of copyright balance, at least through the inclusion of intermediary protections.[56] USTR also stated in 2017 its commitment to seek "the commitment

---

[52] *See also* Comments of the Computer & Commc'ns Indus. Ass'n, In re Request for Public Comment for 2019 Special 301 Review, Dkt No. 2018-0037, filed Feb. 7, 2019, *available at* https://www.ccianet.org/wp-content/uploads/2019/02/CCIA_2019-Special-301_Review_Comment-2.pdf [hereinafter "CCIA 2019 Special 301 Comments"].

[53] 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.

[54] 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.

[55] *Id*. at 6.

[56] *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

of our free trade agreement partners to continuously seek to achieve an appropriate balance in their copyright systems, including through copyright exceptions and limitations."[57] 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.[58] 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.

CCIA reiterates concerns with the threat of new publisher subsidies styled as so-called "neighboring rights" — related to copyright — that may be invoked against online news search and aggregation services and, as USTR notes, raise concerns from a trade perspective.[59] A USITC report also observed that these laws tend to have "generated unintended consequences" to small online publishers.[60] Service providers of online search, news aggregation, and social media platforms are compelled to pay for the "privilege" of quoting from news publications. This is often referred to as a "snippet tax." It is also at times formally described as "ancillary

---

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, U.S.-Mexico-Canada Agreement, 2018 (to be implemented).

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

[58] 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/intellectualproperty/100217-keeping-dmcas-grand-bargain-nafta/ ("The balanced structure of the DMCA has been reflected in our trade agreements for the purpose of benefiting 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.").

[59] *2019 NTE Report*, *supra* note 14, 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-sheetkey-barriers-digital.

[60] *2017 Global Digital Trade I*, *supra* note 16, 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.").

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.[61] As explained in the EU section of these comments, the EU Copyright Directive creates an EU-wide version of this right.

7. Extraterritorial Regulations and Judgments

Using trade policy to promote appropriate intermediary liability frameworks is important since courts are attempting to enforce judgments on intermediaries not only within their borders, but worldwide.[62] Enforcing extraterritorial judgments on U.S. services not only imposes significant compliance costs, but also opens up intermediaries to greater degrees of liability in countries with competing laws. Important domestic policy choices pertaining to intermediaries are threatened when U.S. courts are asked to enforce foreign judgments that conflict with U.S. law. There are also significant technical difficulties to enforcing these judgments in effectively all countries of operation. While intermediaries make a concerted effort to identify and remove content regarding illegal content and copyright infringement, pinpointing and effectively removing this material is challenging. Recent decisions by the European Court of Justice make extraterritoriality concerns an immediate threat to Internet services.[63]

Balancing different countries' laws is already difficult for online intermediaries which operate hundreds of country specific domains. Complications arise when governments attempt to apply domestic laws to Internet activities that occur outside their borders without considering the equities of stakeholders outside their jurisdictions. Requiring sites to implement countries' often contradictory laws at an international scale would be all but impossible and, consequently, expose intermediaries to further liability if they fall short. It would be even harder for small businesses and startups to effectively navigate and implement these policies, limiting

[61] 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.

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

[63] *Infra* notes 182, 183.

competition and harming users. Facing heightened liability, huge fines, and a complex, inconsistent legal system could discourage new businesses from forming and force current ones to curb their services. As countries continue to propose and implement new laws on content regulation at an increasingy rate, remedies that apply extraterritorially will have far-reaching consequences.

8. Customs Duties on Electronic Transmissions

The 2nd Ministerial Conference of the World Trade Organization in 1998 produced the Declaration of Global Electronic Commerce which called for (1) the establishment of a work program on e-commerce and (2) a moratorium on customs duties on electronic transmission.[64] The moratorium has been renewed at every Ministerial since that time.

The moratorium has been key to the development of global digital trade and shows the international consensus with respect to the digital economy, reflected in the number of commitments made in free trade agreements among multiple leading digital economies. Permanent bans on the imposition of customs duties on electronic transmissions are also a frequent item in trade agreements around the world. This includes, but is not limited to, Article 14.3 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP),[65] Article 19.3 of the U.S.- Mexico-Canada Agreement (USMCA),[66] and Article 8.72 of the EU-Japan Economic Partnership Agreement.[67]

Imposing customs requirements on purely digital transactions will also impose significant and unnecessary compliance burdens on nearly every enterprise, including small and medium-sized enterprises (SMEs). There would need to be a number of requirements created that would accompany such an approach, many of which would be extremely difficult to comply with. For instance, data points required for compliance include the description of underlying electronic transfer, end-destination of the transmission, value of transmission, and the country of origin of

[64] The Geneva Ministerial Declaration on Global Electronic Commerce, May 18-20, 1998 https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm.

[65] Final Text of Comprehensive and Progressive Agreement for Trans-Pacific Partnership, signed Mar. 8, 2018, https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf.

[66] Final Text of U.S.-Mexico-Canada Agreement, signed Nov. 30, 2018, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf [hereinafter "USMCA"].

[67] Final Text of Agreement Between EU and Japan for Economic Partnership, http://trade.ec.europa.eu/doclib/docs/2018/august/tradoc_157228.pdf#page=185.

the transmission — all of which do not exist for most electronic transmissions, especially in the cloud services market.

The moratorium is facing threats within the WTO by pressure from primarily India, South Africa, and Indonesia, who seek authority to impose these duties as a way to recoup perceived lost revenue.[68] Analysis on duties on electronic transmissions for economic development shows that this is not supported.[69] The United States should continue to advocate for the permanent extension of the moratorium at the WTO and discourage countries from including electronic transmission in their domestic tariff codes.

9. 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 to exploit that information.

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. There is growing international hostility to encryption.[70] Countries that are considering or have recently implemented anti-encryption laws include Australia, Brazil, China, France, Germany, India, and

[68] *India, South Africa: WTO E-Commerce Moratorium Too Costly for Developing Members*, INSIDE U.S. TRADE (June 5, 2019), https://insidetrade.com/daily-news/india-south-africa-wto-e-commerce-moratorium-too-costly-developing-members; *India, SA Asks WTO To Review Moratorium on E-Commerce Customs Duties*, BUSINESS STANDARD (June 4, 2019), https://www.business-standard.com/article/pti-stories/india-south-africa-asks-wto-to-revisit-moratorium-on-customs-duties-on-e-commerce-trade-119060401401_1.html.

[69] ECIPE, The Economic Losses From Ending the WTO Moratorium on Electronic Transmission (Aug. 2019), https://ecipe.org/publications/moratorium/. *See also* Nigel Cory, *Explainer: Understanding Digital Trade*, REALCLEAR POLICY (Mar. 13, 2019), https://www.realclearpolicy.com/articles/2019/03/13/explainer_understanding_digital_trade_111113.html; Nigel Cory, *The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018*, ITIF, Jan. 2019, at 24, *available at* www2.itif.org/2019-worst-mercantilist-policies.pdf.

[70] Press Release, CCIA Dismayed by AG Opposition to Stronger Consumer Encryption Options, Oct. 3, 2019, http://www.ccianet.org/2019/10/ccia-dismayed-by-ag-opposition-to-stronger-consumer-encryption-options/.

the United Kingdom.[71] Russia has already imposed this requirement on companies operating in its jurisdiction through its "Yarovaya" laws.[72]

These exceptional access regimes run contrary to the consensus assessments of security technologists because they are technically and economically infeasible to develop and implement.[73] Companies already operating in countries that have or are considering anti-encryption laws will be required to alter global platforms or design region-specific devices, or face fines and shutdowns for noncompliance. Companies that might have otherwise expanded to these markets will likely find the anti-encryption requirements to be barriers to entry. Further, given that technology is sold and used on a global basis, introduction of vulnerabilities as required by a number of these regulations risks the privacy and security of users worldwide. 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.

10. Market Access for Communication Providers

Communications providers rely on fair and transparent public procurement regimes. They also rely on consistent, pro-competitive regulation of business-grade whole access and nondiscrimination by major suppliers. For example, even in the United States there is no adequate regulation on bottlenecks in access layers, particularly in the business data service market. Markets abroad, such as the UK, have seen greater competition, with regulation and legal separation requiring the main national operator to provide wholesale/leased access and treat all of its customers equally. Furthermore, the regulator is legally required to carry out detailed market reviews regularly and to impose regulatory remedies where the biggest national operator is found to have significant market power. To ensure this, trade agreements should include

[71] 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.

[72] 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.

[73] 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.

strong language regarding forbearance in trade agreements, to ensure that the regulator's decisions on forbearance are based on evidence-based analysis.[74]

III. COUNTRY-SPECIFIC CONSIDERATIONS

1. Argentina

Additional E-Commerce Barriers

Import policies continue to serve as a trade barrier in Argentina. Industry has encountered difficulties with Argentina's reformed import policies set out in the Comprehensive Import Monitoring System.[75] 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.[76] 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 unlevel 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.

2. Australia

Backdoor Access to Secure Technologies

The Australian Parliament passed the Telecommunications (Assistance and Access) Act at the end of 2018, granting the country's national security and law enforcement agencies

[74] *See* CETA Telecommunications Chapter, Art. 15.41, https://ec.europa.eu/trade/policy/in-focus/ceta/ceta-chapter-by-chapter/.

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

[76] 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.

additional powers when dealing with encrypted communications and devices.[77] The legislation authorizes the Australian government to use three new tools to compel assistance from technology companies in accessing information within electronic communications. These tools are technical assistance requests (TARs), which seek voluntary assistance from communications providers; and technical assistance notices (TANs) and technical capability notices (TCNs). These tools 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 undermine encryption through other technical means with little oversight. Over the past year, technology companies have called for amendments to the bill citing the broad language and failure to address concerns during the drafting process.[78]

Copyright Liability Regimes for Online Intermediaries

Failure to implement obligations under existing trade agreements serves as a barrier to trade.[79] The U.S.-Australia Free Trade Agreement 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. The consequence of this limitation is that intermediary protection is largely limited to Australia's domestic broadband providers. Online service providers engaged in the export of information services into the Australian market remain in a precarious legal situation. This unduly narrow construction violates Australia's trade obligations under Article 17.11.29 of the FTA. This article makes clear that the protections envisioned should be available to all online service providers, not merely carriage service providers. Although Australian authorities documented this implementation flaw years ago, no legislation

[77] Telecommunications (Assistance and Access) Bill 2018, Parliament of Australia, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195.

[78] Josh Taylor, *Australia's Anti-Encryption Laws Being Used to Bypass Journalist Protections, Expert Says*, THE GUARDIAN (July 8, 2019), https://www.theguardian.com/australia-news/2019/jul/08/australias-anti-encryption-laws-being-used-to-bypass-journalist-protections-expert-says; Paul Karp, *Tech Companies Not 'Comfortable' Storing Data in Australia*, THE GUARDIAN (Mar. 27, 2019), https://www.theguardian.com/technology/2019/mar/27/tech-companies-not-comfortable-storing-data-in-australia-microsoft-warns.

[79] CCIA has raised this concern with USTR in the context of the Special 301 Report. *CCIA 2019 Special 301 Comments*, *supra* note 52 at 13-14.

has been enacted to remedy it.[80] This oversight was not addressed by recent passage of amendments to Australia's Copyright Act, which expanded intermediary protections to some public organizations but pointedly excluded commercial service providers including online platforms.[81] These amendments specifically exclude U.S. digital services and platforms from the operation of the framework. 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.

Digital Taxation

In March 2019, the Australian Government announced that, following a consultation, they would not pursue an interim tax and continue engagement at the OECD on a multilateral solution.[82] This was based on "overwhelming" support for the multilateral process. CCIA supports Australia's decision to not proceed with a national digital tax.

Government-Imposed Content Restrictions and Related Access Barriers

Australia amended its Criminal Code in April to establish new penalties for Internet and hosting services who fail to provide law enforcement authorities with details of "abhorrent violent material" within a reasonable time, or fail to "expeditiously" remove and cease hosting this material.[83] Criticism for the legislation was widespread, with particular concern about the rushed nature of the drafting and legislative process.[84] The legislation applies to a broad range of technology and Internet services, including U.S.-based social media platforms, user-generated

---

[80] 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.

[81] 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-australiancopyright-law-thumbs-nose-at-u-s-trade-commitments/.

[82] Government Response to the Digital Economy Consultation, Mar. 20, 2019, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A"media%2Fpressrel%2F6568787" ("Many stakeholders raised significant concerns about the potential impact of an Australian interim measure across a wide range of Australian businesses and consumers, including discouraging innovation and competition, adversely affecting start-ups and low-margin businesses, and the potential for double taxation. Given this feedback and recent international developments, the Government has decided to continue to focus our efforts on engaging in a multilateral process and not to proceed with an interim measure, such as a digital services tax, at this time.").

[83] Criminal Code Amendments (Sharing of Abhorrent Violent Material) Bill 2019, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1201.

[84] *See* Evelyn Douek, *Australia's New Social Media Law is a Mess*, LAWFARE (Apr. 10, 2019), https://www.lawfareblog.com/australias-new-social-media-law-mess.

content and live streaming services, and hosting services. However, the law does not take into account the varying business models of these services in scope of the law and their varying capabilities or roles in facilitating user-generated content. CCIA encourages governments to enact policies affecting online content only after consultation by all stakeholders.[85] Australian officials have also indicated that the country will soon block access to Internet domains hosting terrorist material and will pursue additional legislation that will impose new content requirements on digital services.[86]

Market-based Platform Regulation

Following a lengthy consultation and inquiry on "digital platforms", the Australian Competition and Consumer Commission released a final report in July.[87] Among the 23 recommendations outlined in the report, there are proposals to amend competition laws, create new codes of conduct mandating transparency requirements among businesses, require implementation of "choice screens", establish industry codes of conduct to govern the handling of "fake news" online, and establish new prohibitions on "unfair" trading practices. Many of these recommendations are strongly inconsistent with global best practices on competition issues and may represent market access barriers if implemented.

Additional Barriers to E-Commerce

The Treasury Laws Amendment (GST Low Value Goods) Act 2017 took effect in 2018 and directs the Australian government to start collecting goods and service tax (GST) on all goods including those purchased online from overseas, previously only applied to goods over $1,000 AUD.[88] Companies with over $75,000 AUD in sales to Australian customers are required to register and lodge returns with the Australian Tax Office.

---

[85] *See* Lucie Krahulcova & Brett Solomon, *Australia's Plans for Internet Regulation: Aimed at Terrorist, But Harming Human Rights*, ACCESS NOW (Mar. 26, 2019), https://www.accessnow.org/australias-plans-to-regulate-social-media-bound-to-boomerang/ ("Writing sound policy to address challenges linked to online speech (even "terrorist" content) requires a carefully considered, measured, and proportionate approach. . . Progress requires inclusive, open dialogues and evidence-based policy solutions geared toward a healthier environment that would reflect Australian democratic values of respect for human rights, whether online or off.").

[86] *Australia to Block Internet Domains Hosting Extremist Content During Terror Attacks*, REUTERS (Aug. 25, 2019), https://www.reuters.com/article/us-australia-security-internet/australia-to-block-internet-domains-hosting-extremist-content-during-terror-attacks-idUSKCN1VF05G.

[87] Australian Competition & Consumer Commission, Digital Platforms Inquiry - Final Report (July 26, 2019), *available at* https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report. CCIA's comments to the ACCC are available here: http://www.ccianet.org/wp-content/uploads/2019/08/CCIA-ACCC-Comments-2.15.19-Final-.pdf.

[88] Treasury Laws Amendments (GST Low Value Goods) Act 2017, No. 77, 2017, *available at* https://www.legislation.gov.au/Details/C2017A00077.

3. Austria

Digital Taxation

In April 2019, Austria published a draft bill introducing a 5% tax on digital advertising revenues (an increase from the 3% in previous proposals).[89] Then-Chancellor Kurz announced that "Austria will now introduce a national tax on digital giants like Google or Facebook to ensure that they also pay their fair share of taxes."[90] Like other national tax proposals identified in these comments, a revenue threshold ensures that only large U.S. companies fall within the scope of the proposed tax. The tax received a favorable vote[91] from Austria's Federal Council on October 10 and may be applied starting January 1, 2020.[92]

4. Brazil

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates

In 2018, Brazil passed a privacy law, *Lei Geral de Proteção de Dados* (LGPD), which is set to go into effect in February 2020.[93] The law is closely modeled after the EU's General Data Protection Regulation (GDPR) and has extraterritorial scope. However, the LGPD lacks a number of provisions in the GDPR designed to lessen the burden on smaller firms.[94] Further, the LGPD does not permit cross-border data transfers based on the controller's legitimate interests, but rather lists ten instances in which cross-border data transfer under the LGPD is permitted.[95] In addition, the national authority is tasked with determining whether a foreign government or

---

[89] Alison Bevege, *Austria Increases Size of Planned Digital Tax to 5 Percent of Ad Revenue*, REUTERS (Apr. 3, 2019), https://www.reuters.com/article/austria-economy-digital-tax/update-1-austria-increases-size-of-planned-digital-tax-to-5-pct-of-ad-revenue-idUSL8N21L0KL.

[90] Sebastian Kurz (@sebastiankurz), TWITTER (Apr. 3, 2019, 1:44 AM), https://twitter.com/sebastiankurz/status/1113361541938778112.

[91] Hamza Ali, *Austria's Federal Council Approves 5 Percent Tax on Digital Ad Revenue*, BLOOMBERG TAX (Oct. 10, 2019), https://news.bloombergtax.com/daily-tax-report-international/austrias-federal-council-approves-5-tax-on-digital-ad-revenue.

[92] Hamza Ali, *Austria Pushes Forward With 5% Digital Tax Bill*, BLOOMBERG TAX (July 8, 2019), https://news.bloombergtax.com/daily-tax-report-international/austria-pushes-forward-with-5-digital-tax-bill.

[93] Available at http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm [Portuguese]; *see also* Erin Locker & David Navetta, *Brazil's New Data Protection Law: The LGPD*, COOLEY POLICY & LEGISLATION (Sept. 18, 2018), https://cdp.cooley.com/brazils-new-data-protection-law-the-lgpd.

[94] *Id* (comparing the LGPD with provisions in the GDPR).

[95] Chris Brook, *Breaking Down LGPD, Brazil's New Data Protection Law*, DATAINSIDER (June 10, 2019), https://www.digitalguardian.com/blog/breaking-down-lgpd-brazils-new-data-protection-law (noting that the instances where cross-border data transfer is allowable is found in articles 33-36 of the LGPD).

international organization has a sufficient data protection scheme in place before any data is authorized to be transferred to the government or organization.[96]

Other localization barriers reported include tax incentives for locally sourced information and communication technology (ICT) goods and equipment,[97] government procurement preferences for local ICT hardware and software,[98] and non-recognition of the results of conformity assessment procedures performed outside of Brazil for equipment connected to telecommunications networks.[99] Industry reports that cloud services are also required to have some types of government data localized under recent revisions to the Institutional Security Office cloud guidelines.

Copyright Liability Regimes for Online Intermediaries

The Ministry of Citizenship is currently reviewing Brazil's Copyright Law.[100] Industry reports that they are considering what approach to take with respect to intermediary liability protections, which do not currently exist within the existing statute for copyrighted content. The *Marco Civil da Internet*, Federal Law No. 12965/2014, granted limited intermediary protections that do not include copyrighted content. CCIA encourages Brazil to adopt an approach consistent with DMCA notice-and-takedown provisions that will allow legal certainty for Internet services in Brazil.

Additional E-Commerce Barriers

Brazil's *de minimis* threshold for duty-free importation remains at USD $50, which is applicable only to consumer-to-consumer transactions sent through post. 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.[101] 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

[96] Erin Locker & David Navetta, *Brazil's New Data Protection Law: The LGPD*, COOLEY, LLP (Sept. 18, 2018), https://www.cdp.cooley.com/brazils-new-data-protection-law-the-lgpd/.

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

[98] 2014 Decrees 8184, 8185, 8186, 8194, and 2013 Decree 7903.

[99] ANATEL's Resolution 323.

[100] Ministerio da Cidadania abre Consulta public sobre reforma da Lei de Direitos Autorais (June 28, 2019), http://cultura.gov.br/ministerio-da-cidadania-abre-consulta-publica-sobre-reforma-da-lei-de-direitos-autorais/.

[101] 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-ExpressDelivery.

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. Current legislation allows for an increase of the threshold to USD $100 without the need for Congressional approval. To compare, the average *de minimis* threshold among OECD members is USD $70 for taxes and USD $194 for duties.[102]

5. Belgium

Asymmetry in Competition Frameworks

The Belgian, Dutch, and Luxembourg competition authorities have proposed amendments to their competition regimes allowing for the imposition of remedies without proving harm to consumers for digital companies.[103] This will increase legal uncertainty and open a path to use competition to slow down successful U.S. companies operating in these regions.

6. Cambodia

Government-Imposed Content Restrictions and Related Access Barriers

Pursuant to a directive passed in July 2018, the country requires all websites to register with the Ministry of Information which can impose jail sentences for spreading fake news online.[104] Reports of censorship and mandated Internet filtering and blocking also continue to rise.[105]

7. Canada

Additional Barriers to E-Commerce

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.[106] This *de minimis*

---

[102] For an overview of *de minimis* values worldwide, *see* Global Express Association, Overview of de minimis value regimes open to express shipments worldwide (Mar. 9, 2018), https://global-express.org/assets/files/Customs%20Committee/deminimis/GEA%20overview%20on%20de%20minimis_9%20March%202018.pdf.

[103] Press Release, Joint Memorandum of the Belgian, Dutch and Luxembourg Competition Authorities on Challenges Faced by Competition Authorities in a Digital World, Oct. 10, 2019, https://www.belgiancompetition.be/sites/default/files/content/download/files/20191010_press_release_33_bma_acm_cdlcl.pdf.

[104] *2018 Freedom on the Net Report*, supra note 27, at 11.

[105] Freedom on the Net 2018 Country Report: Cambodia, https://freedomhouse.org/report/freedom-net/2018/cambodia (last visited Oct. 31, 2019).

[106] eBay Main Street, Canadian De Minimis, https://www.ebaymainstreet.com/issues/canadian-de-minimis (last visited Oct. 31, 2019).

level — the lowest among major U.S. trading partners[107] — includes shipped goods, which has a huge effect on digital trade. Industry was encouraged to see that the USMCA commits Canada to raise the *de minimis level* to $40 CAD.[108] 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.[109] 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. However, industry strongly discourages the United States from setting reciprocal *de minimis* levels, and using the implementing legislation of the USMCA to derogate authority away from Congress to set *de minimis* levels.[110]

Other barriers for digital services include broadcasting regulations that discriminate against foreign competitors. An expert legislative panel is currently reviewing Canada's Broadcasting Act and Telecommunications Act and a final report with panel recommendations is expected in January 2020.[111] Industry expects the panel to recommend that foreign digital video services be regulated under the Canadian Radio-television Telecommunications Commission Content rules.[112] These regulations could include Canadian content quotas, requirements to grant preferential treatment to Canadian content in online display menus and algorithms, and mandatory spending on Canadian content or contributions to the Canadian Media Fund.[113] These requirements would impose an unfair burden on foreign digital services, who do not benefit from

---

[107] *2017 Global Digital Trade I, supra* note 16, at 310.

[108] USMCA, *supra* note 66 art. 7.8.

[109] *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/Ebrief_Rights%20of%20Passage_June16.pdf (stating "we find that lifting the threshold would have a net economic benefit of up to C$648 million.").

[110] Tech Industry Association Letter to Congress, Sept. 9, 2019, http://www.ccianet.org/wp-content/uploads/2019/09/Tech-Association-USMCA-Fall-2019-Letter.pdf ("However, in order to gain these benefits, it will also be important to ensure that the Administration does not receive the authority to unilaterally amend the U.S. de minimis threshold through the USMCA implementing bill. The current threshold was set by Congress and continues to benefit U.S. small businesses.").

[111] *See* Innovation, Science and Economic Development Canada, Broadcasting and Telecommunications Legislative Review, https://www.ic.gc.ca/eic/site/110.nsf/eng/home.

[112] *See* Innovation, Science and Economic Development Canada, "What We Heard Report", https://www.ic.gc.ca/eic/site/110.nsf/eng/00011.html#s51
(last modified June 26, 2019).

[113] *Id*.

various market protections granted to domestic competitors. CCIA supports a user-driven approach to content creation and cultivation rather than by government quotas or mandates.

Digital Taxation

Ahead of the Canadian election cycle, Prime Minister Justin Trudeau's Liberal Party released its full policy platform outlining priorities for the next government.[114] Among other discouraging positions,[115] the platform includes a promise to pursue a digital tax on foreign tech companies. With the Liberal Party's success in the recent elections, industry is monitoring whether the government will act on these plans.[116] This appears to depart from Canada's previous position on support for the OECD multilateral process rather than a unilateral measure at the national level. According to Canada's Office of the Parliamentary Budget Officer, the tax would "replicate" the French Digital Services Tax and impose a 3% DST on advertising services and digital intermediation services companies that meet similar revenue thresholds. In the lead-up to USMCA passage, it is critical that USTR send a strong and clear signal to trading partners such as Canada that unilateral DST measures are unacceptable.

Extraterritorial Regulations and Judgments

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

[114] Liberal Party, Forward A Real Plan for the Middle Class, *available at* https://2019.liberal.ca/our-platform/ ("We will . . . make sure that multinational tech giants pay corporate tax on the revenue they generate in Canada. We will also work to achieve the standard set by the Organisation for Economic Co-operation and Development (OECD) to ensure that international digital corporations whose products are consumed in Canada collect and remit the same level of sales taxation as Canadian digital corporations.").

[115] Michael Geist, *Opinion: From Innovation to Regulation*, THE GLOBE AND MAIL (Oct. 1, 2019), https://www.theglobeandmail.com/business/commentary/article-from-innovation-to-regulation-why-the-liberals-have-lost-their-way-on/ "[T]he 2019 Liberal party platform does not include a single mention of innovation or AI. Instead, it is relying heavily on ill-fitting European policies to turn the Canadian digital space into one of the most heavily regulated in the world. Rather than positioning itself as the party of innovation, the Liberals are now the party of digital regulation with plans for new taxes, content regulation, takedown requirements, labour rules and a new layer of enforcement commissioners.").

[116] Stephanie Soong Johnston, *Canadian Digital Tax Likely as Trudeau Hangs On to Power*, TAX NOTES (Oct. 22, 2019), https://www.taxnotes.com/featured-news/canadian-digital-tax-likely-trudeau-hangs-power/2019/10/22/2b20t; Michael Geist, *What Comes Next for Canadian Digital Policy Under a Liberal Minority Government?* (Oct. 23, 2019), http://www.michaelgeist.ca/2019/10/what-comes-next-for-canadian-digital-policy-under-a-liberal-minority-government/.

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.[117]

Following two unsuccessful Canadian appeals, Google successfully obtained permanent injunctive relief in the United States District Court for 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. While an injunction was granted, the principle that Canadian courts can dictate to Americans what they can read online is itself a trade barrier. Further, the *Equustek* decision has since been cited by other foreign courts to justify world-wide injunctions for online content.[118]

Restrictions on Cross-Border Data Flows

The Office of the Privacy Commissioner (OPC) of Canada launched a consultation in early 2019[119] on the revisitation of its official policy position on cross-border data flows under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[120] The proposed view of the OPC was that under PIPEDA's accountability principles, an organization must obtain consent for a transfer to a third party for processing, including for cross-border transfers. This is a change from the 2009 guidelines that state: "Assuming the information is being used for the purpose it was originally collected, additional consent for the transfer is not required."

Following significant concerns raised by a number of stakeholders regarding the abrupt change in position, threats to business operations in the U.S. and Canada, and potential conflicts with existing trade obligations,[121] the OPC determined that it would not amend the guidelines.[122] Rather, they intend to direct lawmakers to reevaluate existing law and determine whether legislative changes are needed. Industry is closely following these proceedings. There is a risk that abrupt changes to procedures that enable data transfer between the U.S. and Canada would

---

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

[118] Swami Ramdev & Anr. v. Facebook, Inc., High Court of Delhi at New Delhi, Oct. 23, 2019, *available at* http://lobis.nic.in/ddir/dhc/PMS/judgement/23-10-2019/PMS23102019S272019.pdf, *infra* note 274.

[119] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, Consultation on Transborder Dataflows, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/.

[120] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, Processing Personal Data Across Borders Guidelines, *available at* https://www.priv.gc.ca/media/1992/gl_dab_090127_e.pdf.

[121] Comments of CCIA to the Office of the Privacy Commissioner of Canada, filed Aug. 6, 2019, *available at* https://www.ccianet.org/wp-content/uploads/2019/10/CCIA-Comments-Regarding-the-Consultation-on-Transfers-for-Processing.pdf.

[122] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, Commissioner Concludes Consultation on Transfer for Processing (Sept. 23, 2019), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190923/.

conflict with provisions in the Digital Trade Chapter of USMCA and Canada's commitments under CPTPP, which both contain commitments for all parties to enable cross-border data flows.

8. Chile

Digital Taxation

In previous comments, CCIA raised concerns with a bill that included a digital tax for services provided by foreign companies to Chilean individuals set at 10%.[123] However, it has been reported that Chile is now considering a 19% tax on multinational e-commerce firms.[124] However, it has been reported that Chile has proposed an updated bill that would replace the digital services tax with a value-added tax, which appears to be a positive development.

Data Localization Mandates

Chapter 20-7 of the Comisión para el Mercado Financiero's compilation of updated rules, Recopilación Actualizada de Normas Bancos, requires that "significant" or "strategic" outsourcing data be held in Chile.[125] The same requirement is outlined in Circular No. 2, which is addressed to non-banking payment cards issuers and operators. In effect, these regulations can apply to any confidential records. In the case of the international transfer of such data, transfer may occur but duplicate copies of such records must be held in Chile.

9. China

The Chinese market continues to be hostile to foreign competitors, and 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. The Administration recognizes the concerns of the U.S. Internet and technology community with respect to China, as evidenced by the initiation of a Section 301 investigation to determine whether the policies of the Chinese government relating to technology transfer, intellectual property, and innovation are actionable under the Trade Act. CCIA asks USTR to remain vigilant and discourage policies restricting foreign companies'

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

[124] Marion Giraldo, *Chile Considers New 19 Percent Tax on Multinational E-Commerce Firms*, REUTERS (Jan. 10, 2019), https://www.reuters.com/article/us-chile-economy-ecommerce/chile-considers-new-19-percent-tax-on-multinational-e-commerce-firms-idUSKCN1P42A4.

[125] Recopilación Actualizada de Normas Bancos (RAN), *available at* https://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=3.1.2&LNAN=1 (last visited on Oct. 31, 2019).

ability to enter the Chinese technology sector, and to promote policies focused on allowing free and open competition within China's borders.

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization 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]

Similarly, discriminatory practices are also prevalent in Chinese information technology industries. As USTR has previously noted, foreign companies providing cloud computing services are forced to enter into joint partnerships with Chinese firms if they wish to conduct business within China,[128] 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.

China seeks to further restrain foreign cloud service operators, in concert with its national plan to promote the Chinese cloud computing industry.[129] U.S. cloud service providers (CSPs) are worldwide[130] leaders and are strong U.S exporters.[131] China has adopted discriminatory

---

[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] 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.

[129] 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.

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

[131] CCIA has discussed these restrictions in previous submissions to the USTR. *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.

practices against U.S. cloud service providers with increasing frequency in recent years. A draft regulation (*Regulating Business Operation in Cloud Services Market (2016*)), yet to be finalized, threatens to significantly disadvantage U.S. providers issued by the Ministry of Industry and Information Technology (MIIT). The proposal, 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.[132] These measures are fundamentally protectionist and anticompetitive, threaten to further discourage foreign investment, and are contrary to China's WTO commitments and separate commitments to the United States.[133] Foreign access to the cloud computing market is also restricted under the guise of strengthening cybersecurity.[134]

In 2016, China passed three pieces of anticompetitive legislation concerning data localization with negative implications to cloud computing: (1) a "counterterrorism" law that requires Internet and telecommunication companies to create methods for monitoring content for terror threats;[135] (2) an online publishing law that requires that all servers used for online publications and press be located within China; and (3) the long-awaited Cybersecurity Law which came into effect in 2017.[136]

Subsequent standards and draft measures made pursuant to the Cybersecurity Law signal continued concerns. On June 13, 2019, new draft *Measures of Security Assessment of the Cross-border Transfer of Personal Information* were released by the Cyberspace Administration China for public comment. This draft focuses on cross-border transfer of "personal information."

---

[132] 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.

[133] In commitments made in September 2015 and June 16, China agreed that its cybersecurity measures in the commercial sector would not disadvantage foreign providers and would not include nationality-based restrictions.

[134] 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.

[135] 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.

[136] David Barboza & Paul Mozer, *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.

Article 2 of the draft measures subjects any transfer of covered data outside China to strict and comprehensive security assessments.[137] There is confusion regarding how this draft affects prior draft legislation on cross-border data and localization mandates issued pursuant to the Cybersecurity Act.[138]

On May 28, 2019, draft *Measures for Data Security Management* were released that set out requirements for the treatment of "important" information which was not clearly defined in the Cybersecurity Law.[139] "Important data" is defined as "data that, if leaked, may directly affect China's national security, economic security, social stability, or public health and security."[140] Draft amendments were also published in 2019 to amend the Personal Information Protection Standard, which became effective in 2018 and sets out best practices regarding enforcement of the data protection rules outlined in the Cybersecurity Law.[141] The draft amendments released on February 1, 2019 set out the following: enhanced notice and consent requirements, new requirements on personalized recommendations and target advertising, requirements on access by third parties and data integration, revised notification requirements for incident response, and requirements to maintain data processing records.[142]

Additional regulations issued pursuant to the Cybersecurity Act granted Ministry of Public Security officials additional inspection powers. Under these new rules, which took effect in November 2018, companies doing business in China must submit to in-person inspections of

---

[137] Yan Luo, Nicholas Shepherd & Zhijing Yu, *China Seeks Public Comments on Draft Measures Related to the Cross-border Transfer of Personal Information*, COVINGTON INSIDE PRIVACY (June 13, 2019), https://www.insideprivacy.com/international/china/china-seeks-public-comments-on-draft-measures-on-security-assessment-for-the-cross-border-transfer-of-personal-information/

[138] Samm Sacks & Graham Webster, *Five Big Questions Raised by China's New Draft Cross-Border Data Rules*, NEW AMERICA (June 13, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/five-big-questions-raised-chinas-new-draft-cross-border-data-ruless/ (noting conflict with 2017 draft measuring on "personal information and important data outbound transfer security assessment").

[139] Yan Luo, Nicholas Shepherd & Zhijing Yu, *China Releases Draft Measures for Data Security Management,* COVINGTON INSIDE PRIVACY (May 28, 2019), https://www.insideprivacy.com/uncategorized/china-releases-draft-measures-for-the-administration-of-data-security/.

[140] *Id*.

[141] Yan Luo & Phil Bradley-Schmieg, *China Issues New Personal Information Protection Standard*, COVINGTON INSIDE PRIVACY (Jan. 25, 2018) https://www.insideprivacy.com/international/china/china-issues-new-personal-information-protection-standard/

[142] Yan Luo, *China Releases Draft Amendments to the Personal Information Protection Standard*, COVINGTON INSIDE PRIVACY (Feb. 11, 2019), https://www.insideprivacy.com/international/china/china-releases-draft-amendments-to-the-personal-information-protection-standard/.

their networked computer systems.[143] The Chinese government is allowed to enter almost any company area related to networked units in order to check computer systems for network security compliance. This includes viewing, searching, and copying any information related to the inspection such as all user information, technical measures for the network, information security protection, hosting, domain name information, and any content distribution the organization may be conducting.[144] Additionally, if any content or information found during the inspection is censored by the Chinese government, the companies hosting that content can be subject to prosecution under the Cybersecurity law.[145]

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.[146] 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.[147]

Government-Imposed Content Restrictions and Related Access Barriers

As CCIA explained to the U.S.-China Economic and Security Review Commission in 2015,[148] barriers to digital trade in China continue to present significant challenges to U.S. exporters. USTR acknowledged these challenges in the 2019 NTE Report, highlighting the burdens that China's filtering of cross-border Internet traffic has imposed, and recognizing that outright blocking of websites has worsened. High-profile examples of targeted blocking of whole services have included China's blocking of major U.S. services including Facebook, Picasa, Twitter, Tumblr, Google Search, Foursquare, Hulu, YouTube, Dropbox, LinkedIn, and

---

[143] Regulations on Internet Security Supervision and Inspection by Public Security Organs (公安机关互联网安全监督检查规定) (2018). *See also* Catalin Cimpanu, *China's cybersecurity law updates lets state agencies 'pen-test' local companies*, ZDNET (Feb. 9, 2019), https://www.zdnet.com/article/chinas-cybersecurity-law-update-lets-state-agencies-pen-test-local-companies.

[144] Insikt Group, *China's New Cybersecurity Measures Allow State Police to Remotely Access Company Systems*, RECORDED FUTURE (Feb. 8, 2019), https://www.recordedfuture.com/china-cybersecurity-measures.

[145] *Id*.

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

[147] *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.

[148] *Commercial Espionage and Barriers to Digital Trade in China: Before the U.S.-China Economic and Security Review Commission*, 114th Cong. (2015) (Testimony of Matthew Schruers, Chief Operating Officer, Computer & Communications Industry Association).

Slideshare.[149] In June 2017, China shut down over 60 news outlets and social media accounts under the new Cybersecurity Law.[150] Informal estimates suggest that this blocking has easily cost American firms billions of dollars as they are pushed out of the market.[151]

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.[152]

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. Industry remains concerned about China's ban on the use of "unauthorized" VPNs that reportedly went into effect in March 2018.[153] 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.[154] Additionally in 2015, China had cracked down on

---

[149] *2014 Digital Trade in the U.S. and Global Economies, Part 2*, *supra* note 22, at 98.

[150] 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/.

[151] *China's Internet Censorship Should be Lifted for the Sake of the Economy and Innovators*, SOUTH CHINA MORNING POST (Apr. 15, 2018), https://www.scmp.com/comment/letters/article/2141626/chinas-internet-censorship-should-be-lifted-sake-economy-and; 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.

[152] Graeme Burton, *China Government Starts Issuing Fines for VPN Use,* THE INQUIRER (Jan. 8, 2019), https://www.theinquirer.net/inquirer/news/3068962/chinas-government-starts-issuing-fines-for-vpn-use; 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/.

[153] 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. Industry supports U.S. efforts to oppose this measure at the WTO.

[154] Calum MacLeod & Elizabeth Weise, *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/.

special software tools hosted on GitHub, a website popular with open source enthusiasts,[155] by launching distributed denial of service attacks against the site.

Additional Barriers to E-commerce

China passed its first law regulating "e-commerce" in August 2018 which took effect in January 2019.[156] 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."[157] Requirements include the need to obtain a business license 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 (PBOC) 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.

Industry also encourages China to expedite the review of its Copyright Law to ensure that there exist legal remedies, consistent with global copyright enforcement norms, for e-commerce sellers of e-books and software to combat infringement in the Chinese market.

10. Colombia

Digital Taxation

Colombia's Tax Authority has announced that a proposed financing bill will include a permanent establishment obligation for foreign companies that "have significant economic activities in the country."[158] 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.

---

[155] 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-militaryparade.html.

[156] Cyrus Lee, *Law Regulating Online Shopping Activities Enforced in China*, ZDNET (Jan. 2, 2019), https://www.zdnet.com/article/law-regulating-online-shopping-activities-enforced-in-china/.

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

[158] Laura Duran, *VAT on Digital Services in Colombia*, BAKER MCKENZIE (Feb. 28, 2019), https://www.lexology.com/library/detail.aspx?g=6803a06d-da3b-472c-a25b-0074cf0026ed.

Copyright Liability Regimes for Online Intermediaries

Colombia has failed to comply with its obligations under the 2006 U.S.-Colombia Free Trade Agreement to provide protections for Internet service providers.[159] Recently passed legislation that sought to implement the U.S.-Colombia FTA copyright chapter includes no language on online intermediaries.[160] 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. The recent legislation 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.

Additional E-Commerce Barriers

Colombia remains out of compliance with the U.S.-Colombia Trade Promotion Agreement (CTPA) by failing to implement the USD $200 *de minimis* threshold. A new customs regime was established under Decree 1165 of 2019 in July.[161] The Decree combined all relevant regulations over recent years, but failed to include Decree 349 which provides for a timeline for CTPA compliance on *de minimis*. Colombia has also failed to implement necessary reforms on trade facilitation that would permit firms to submit electronic invoices in place of physical copies.

11. Czech Republic

Digital Taxation

The Prime Minister has announced a 7% digital tax with a scope similar to the EU Digital Services Tax and the following thresholds: worldwide revenues of €750M and national revenues of 50M Czk (2M EUR) in taxable turnover.[162] The tax would apply starting in 2020. Some reports suggest that the Ministry of Finance might consider placing the digital services tax bill on hold in light of the OECD process.

---

[159] *See* U.S.-Colum. Free Trade Agreement, Nov. 22, 2006, art. 16.11, para. 29.

[160] 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/.

[161] Text available at: https://boletin-diario.icdt.co/wp-content/BOLETINDIARIO/2019/JULIO/3JULIO/DeMINHACIENDA1165_19.pdf.

[162] *Czech Republic: Update on Digital Services Tax*, KPMG (July 8, 2019), https://home.kpmg/us/en/home/insights/2019/07/tnf-czech-republic-update-on-digital-services-tax.html.

12. European Union[163]

As part of the ambitious Digital Single Market strategy under the previous European Commission, the EU finalized a number of regulations and policies affecting digital imports over the past year. Many of these policies will have a lasting impact on the state of innovation within the EU and industry is closely monitoring implementation of these new regulations. CCIA once again agrees with USTR's fear expressed in previous NTEs that the EU's pursuit of "well-intention goals 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."[164]

CCIA's concerns remain with the new Commission based on proposed plans for further regulating the digital economy in the name of "technology sovereignty". According to the stated priorities of President-elect Ursula von der Leyen, officials will look to develop a regulatory framework for artificial intelligence, create a new "Digital Services Act" that will change existing liability regimes for digital services, and act on a EU-wide strategy to favor and grow EU competitors.[165] All initiatives will work towards achieving European "technical sovereignty".[166] Reports indicate that the Commission's entire digital agenda is very expansive, and industry encourages USTR to closely monitor developments in the region and engage when warranted.

---

[163] This section covers regulations and legislation pursed at the EU-level. Other sections of these comments focus on national laws that represent barriers to trade within the EU.

[164] *2019 NTE Report*, *supra* note 14, at 207.

[165] Political Guidelines for the Next European Commission 2019-2024, *available at* https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

[166] Mission Letter to Commissioner-designate for Internal Market (Sept. 10, 2019), https://ec.europa.eu/commission/sites/beta-political/files/mission-letter-sylvie-goulard_en.pdf ("I want you to contribute to the work on enhancing Europe's technological sovereignty . . . I also want you to lead the Commission's reflections on issues such as Europe's technological sovereignty in key value chains, including in the defence and space sectors, common standards and future trends."); Natasha Lomas, *Europe's Antitrust Chief, Margrethe Vestager, Set for Expanded Role in Next Commission*, TECHCRUNCH (Sept. 10, 2019), https://techcrunch.com/2019/09/10/europes-antitrust-chief-margrethe-vestager-set-for-expanded-role-in-next-commission/ (quoting von Der Leyen remarks at a press conference saying the following: "We have to make more out of the field of artificial intelligence. We have to make our single market a digital single market. We have to use way more the big data that is out there but we don't make enough out of it. What innovation and startups are concerned. It's not only need to know but it's need to share big data. We have to improve on cyber security. *We have to work hard on our technological sovereignty* just to name a few issues in these broad topics."[emphasis added]).

Market-based Platform Regulation

A political agreement on the EU's Platform-to-Business Regulation, introduced in 2017, was reached in February of this year, and the final text was adopted on June 20, 2019.[167] While changes to the regulations were made to address a number of concerns industry had raised in previous comments,[168] industry will continue to monitor the following: the operation of the exception for trade secret protection in Article 5; transparency requirements regarding algorithms but also vertical integration practices; the use of most favored nation clauses; the reference to "operating systems" that could result in expansion of regulatory scope in some contexts; the inclusion of monetary penalties in addition to injunctive relief; and prescriptive mechanisms for handling business complaints. The Commission is currently working on guidance on Article 5 and Article 8. USTR should also closely monitor its implementation to ensure that compliance does not have the effect of undermining market access.

Digital Taxation

The European Commission presented a package of two digital tax proposals in March 2018.[169] 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) was to be set at 3% of companies' gross revenues from making available advertisement space, intermediation services, and transmission of user data.[170] Industry applauds the EU for deciding not to move forward with the tax, and its support for the multilateral process at the OECD.

However, on a national level, Member States have used the EU proposal to move forward with their own national taxes with even more explicit carve-outs for domestic competitors, making the tax discriminatory towards U.S. technology firms. To date, Austria, Belgium, Czech Republic, Denmark, Hungary, Italy, Poland, Spain, and the UK have all announced or implemented digital taxes. The EU has indicated that a priority of the next Commission will be

---

[167] Press Release, European Commission, EU Negotiators Agree to Set Up New European Rules to Improve Fairness of Online Platforms' Trading Practices (Feb. 14, 2019), http://europa.eu/rapid/press-release_IP-19-1168_en.htm. Press Release, CCIA, EU Negotiators Reach Agreement on Platform Regulation Proposal (Feb. 14, 2019), http://www.ccianet.org/2019/02/eu-negotiators-reach-agreement-on-platform-regulation-proposal/.

[168] *CCIA 2018 NTE Comments*, *supra* note 38, at 38.

[169] *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.

[170] *See CCIA 2018 NTE Comments*, *supra* note 38, for full criticism of the EU's DST.

to once again pursue a digital tax in Q3 2020 if the OECD does not reach an agreement by 2020.[171]

Government-Imposed Content Restrictions and Related Access Barriers

The EU is currently negotiating over a Regulation pertaining to violent and extremist content which includes filtering requirements and a shot-clock deadline for content removal, aimed principally at U.S. firms, not all of which have the capacity to meet such a burden. This initiative regulating terrorist content could also increase the burden on service providers to monitor and filter content.[172] The proposal could 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 online services "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 dissemination" on each platform; and impose strong financial penalties of up to 4% of global turnover in case of "systematic failures to remove such content following removal orders". The current scope of the legislation would also extend to cloud infrastructure providers who lack the technical measures necessary to perform these obligations as drafted.

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. CCIA calls for a clear definition of "terrorist content" to avoid any legal uncertainty which could limit the freedom of speech. 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. Further, this regulation will apply to small firms in addition to larger players. Most do not have

[171] Bjarke Smith-Meyer, *Digital Tax Back-Up Plan in the Works for 2020, Antiloni Says*, POLITICO (Oct. 3, 2019), https://www.politico.eu/pro/digital-tax-back-up-plan-in-the-works-for-2020-gentiloni-says/; Francesco Guarascio, *In Blow to U.S., EU Pledges Quick Move on Tax for Polluting Firms*, Reuters (Oct. 3, 2019), https://www.reuters.com/article/us-eu-commission-gentiloni/in-blow-to-u-s-eu-pledges-quick-move-on-tax-for-polluting-firms-idUSKBN1WI0K1 ("[European Economy Commissioner-designate Gentiloni] reiterated the EU should move alone on an EU-wide tax on digital corporations if no deal was reached at global level in 2020. He said he was confident, although "not fully optimistic", about an international agreement by that deadline.").

[172] *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.

the required resources to comply with this timeline, which could force many out of the EU market. While policy-makers have global platforms in mind, this new law could put news burdens on small and medium-sized players. Many might not have the resources needed to comply which could force them out the EU market.

As mentioned above, the incoming Commission President has announced a forthcoming "Digital Services Act," which will further depart from trans-Atlantic norms on liability for online services. Several Commissioner-designates mentioned during their European Parliament hearings their intention to make online platforms more liable for the content they are hosting. This new initiative might target all kinds of platforms, regardless of where they are established (inside or outside the EU). New "binding rules" could be considered for hate speech, disinformation, political advertising, or product safety. The Commission is considering having a horizontal proposal associated with sectoral approaches. Regulatory options will be considered mid-2020, and a proposal is expected at the end of 2020 or early 2021.

Internet services are also experiencing concerning developments across EU Member States, as explained in other sections of these comments.

Copyright Liability Regimes for Online Intermediaries

On May 17, 2019, the Copyright Directive was published in the Official Journal of the European Union.[173] The Member States will have until June 7, 2021 to implement this new EU law. Articles 15 and 17 represent a departure from global IP norms and international commitments and will have significant consequences for online services and users. These rules diverge sharply from provisions in the U.S.-Mexico-Canada Agreement and U.S. law, and will place unreasonable and technically impractical obligations on a wide range of service providers, resulting in a loss of market access by U.S. firms.

Online services must implement filtering technologies in order to comply with the requirements under Article 17. While Article 17 avoids the word "filter", practically speaking content-based filtering will be required if a service is to have any hope of achieving compliance. This upends longstanding global norms on intermediary liability. Absent obtaining a license from all relevant rightsholders, online services would be directly liable unless they did all of the following: (1) made best efforts to obtain a license, (2) made best efforts to "ensure the

[173] 2019 J.O. (L130) 55, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:130:FULL&from=EN.

unavailability of specific works and other subject matter" for which the rightsholders have provided to the online service, and (3) "in any event" acted expeditiously to remove content once notified by rightsholders and made best efforts to prevent their future uploads. The last requirement effectively creates an EU-wide 'notice-and-staydown' obligation. The other requirements are not mitigated by the inclusion of a "best efforts" standard, in part because "best efforts" is a subjective but still mandatory standard open to abuse and inconsistent interpretations at the Member State level.

Despite claims from EU officials, lawful user activities will be severely restricted. EU officials are claiming that the new requirements would not affect lawful user activity such as sharing memes, alluding to the exceptions and limitations on quotation, criticism, review, and parody outlined in the text. This is a disingenuous argument for two reasons. First, while the text itself does not explicitly "ban memes," the action online services would have to take to avoid direct liability is the restriction of lawful content. Algorithms used to monitor content on platforms cannot contextualize to determine whether the content was lawfully uploaded under one of the exceptions listed. Second, under the final text of Article 17, the exceptions and limitations provided for only apply to users, not the sharing services themselves (¶ 5: "Member States shall ensure that users in all Member States are able to rely on the following existing exceptions and limitations when uploaded and making available content generated by users"). This makes the exceptions largely meaningless if the services used to take advantage of this exception do not also receive the same rights.

Member States are currently working on implementation and a number have already launched public consultations to develop national legislation to implement the Directive.[174] As Member States draft implementation legislation, CCIA emphasizes that a service provider which is made primarily liable for copyright infringements must be able to take steps to discharge this liability, otherwise this will ultimately lead to the demise of user-generated content services based in Europe — as it is materially impossible for any service to license all the works in the world and rightsholders are entitled to refuse to grant a license or to license only certain uses. Accordingly, CCIA believes that mitigation measures are absolutely necessary in order to make Article 17 workable. Moreover, any measures taken by a service provider under Article 17

[174] *See Capitals Special Edition: The Copyright Directive*, EURACTIV (Oct. 2, 2019), https://www.euractiv.com/section/politics/news/capitals-special-edition-the-copyright-directive/.

should be based on the notification of infringing uses of works, not just notification of works. A functional copyright system requires cooperation between information society service providers and rightsholders. Rightsholders should provide robust and detailed rights information (using standard formats and fingerprint technology where applicable) to facilitate efforts to limit the availability of potentially infringing content.

Imbalanced Copyright Laws and "Link Taxes"

CCIA also remains concerned with Article 15 of the Copyright Directive and the creation of a press publishers' right. Contrary to U.S. law and current commercial practices, Article 15 will require search engines, news aggregators, applications, and platforms to enter into commercial licenses before including snippets of content in search results, news listings, and other formats. The exception for "short excerpts" and single words is highly unlikely to provide any real certainty for Internet services who wish to continue operating aggregation services, and conflicts with the current practice of many U.S. providers who offer such services.[175]

The 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.[176] The beneficiaries of this exception are limited to "research organizations," excluding individual researchers and startups.

As explained in the France section in these comments, France has already started to implement this provision of the EU Copyright Directive as it created a new right for press publishers which entered into force in October.[177] French press publishers can now request payment from platforms when they display short previews or snippets of their content online in ways that would be treated as fair use under U.S. law. Following this development, Google

---

[175] Directive 2019/790, of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC, 2019 O.J. (L 130) 15:

> 1. Member States shall provide publishers of press publications established in a Member State with the rights provided for in Article 2 and Article 3(2) of directive 2001/29/EC for the online use of their press publications by information society service provider. The rights provided for in the first subparagraph shall not apply to private or non-commercial uses of press publications by individual users. The protection granted under the first subparagraph shall not apply to acts of hyperlinking. The rights provided for in the first subparagraph shall not apply in respect of the use of individual words or very short extract of a press publication.

[176] *Id*. at Article 3(2).

[177] Loi 2019-775 du 24 juillet 2019 à créer un droit vosin au profit des agencies de presse et des éditeurs de presse [Law 2019-775 of July 24, 2019 Law creating a neighboring right for press publishers and news editors], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE] [OFFICIAL GAZETTE OF FRANCE], Oct. 5, 2019.

announced on September 25 that it would stop showing preview content in France for European news publications.[178] On October 2, the French competition authority decided to open a preliminary investigation into Google in relation to conduct aimed at complying with the French law.[179]

Extraterritorial Regulations and Judgments

In September 2019, the EU Court of Justice ruled that removed or delisted URLs from search engines should not apply worldwide.[180] The ruling honors EU residents' "right to be forgotten" (RTBF). The decision concludes that a service provider subject to the RTBF is not obligated to de-index outside of the EU.[181] However, the decision does leave the possibility for a data protection authority or a national court to ask, on a case-by-case basis, for the delisting of all versions of the search engine, even outside the EU.[182] Further, a subsequent decision issued in October authorizing national courts to issue global content takedown injunctions regarding defamatory content indicates that EU courts may be moving in a direction that would conflict directly with the U.S. 2010 SPEECH Act, which was designed to combat libel tourism abroad.[183]

---

[178] Richard Gingras, *How Google Invests in News*, GOOGLE BLOG (Sept. 25, 2019), https://www.blog.google/perspectives/richard-gingras/how-google-invests-news/.

[179] David Meyer, *French Publishers Have Gone to War With Google. They Are Not Likely to Win*, FORTUNE (Oct. 25, 2019), https://www.fortune.com/2019/10/25/french-publishers-google-copyright-competition/.

[180] Case C-507/17 Google LLC v. CNIL, http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1092623

[181] "On a proper construction of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and of Article 17(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 (General Data Protection Regulation), where a search engine operator grants a request for de-referencing pursuant to those provisions, *that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States*, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request." (emphasis added).

[182] Case C-507/17 Google LLC v. CNIL, Paragraph 72.

[183] Eva Glawischnig-Piesczek v. Facebook Ireland Ltd., Case C-18/18, dec. Oct. 3, 2019, *available at* http://curia.europa.eu/juris/document/document_print.jsf?docid=218621&text=&dir=&doclang=EN&part=1&occ=first&mode=req&pageIndex=0&cid=1986464 (interpreting the EU E-Commerce Directive prohibition on general monitoring provisions not to preclude a court of a Member State from (1) ordering an online service from removing content worldwide, within the framework of relevant international law, and (2) as well as ordering the removal of content that is "equivalent" or "conveys a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality"). *See also* Press Release, EU Court Ruling on Worldwide Take Down of Defamatory Content Raises Freedom of Speech Concerns, Oct. 3, 2019,

The General Data Protection Regulation (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.[184] Under the GDPR, the fine for noncompliance with these and other provisions can be up to 4% of a company's global operating costs. Putting the onus on companies to respond to all requests in compliance with the "right to be forgotten" ruling and Article 17 of the GDPR is administratively burdensome. For example, popular U.S. services have fielded millions of requests since the policy went into effect.[185] 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.

Restrictions on Cross-Border Data Flows

The EU's approach to privacy protections presents barriers for some U.S. exporters. The aforementioned GDPR was adopted on April 27, 2016, and went into effect on May 25, 2018.[186] 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. Since taking effect, a number of small businesses and online services have ceased serving customers in the EU market due to compliance costs and uncertainty over obligations.[187]

The EU also has been working on amending the existing e-Privacy Directive and proposed the "ePrivacy Regulation" in 2017.[188] The proposal seeks to expand the existing

---

http://www.ccianet.org/2019/10/915157/&sa=D&ust=1570634473237000&usg=AFQjCNH8WVAjVBQJcbK_Iz5aM_ecyIN34w.

[184] GDPR art. 17.

[185] Adam Satariano, *Right to Be Forgotten' Privacy Rule is Limited by Europe's Top Court*, N.Y. TIMES (Sept. 24, 2019), https://www.nytimes.com/2019/09/24/technology/europe-google-right-to-be-forgotten.html.

[186] 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"].

[187] Hannah Kuchler, *US Small Businesses Drop EU Customers Over New Data Rule*, FINANCIAL TIMES (May 24, 2018), https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04.

[188] 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"].

Directive, which currently only applies to telecommunication services, to all "electronic communication services" including over-the-top services.[189] Rules that were originally created for traditional telecommunication services would apply to a variety of online applications, from those that provide communications and messaging services to personalized advertising and the Internet of Things. The Commission justifies this expansion in scope by observing that since the enactment of the e-Privacy Directive, services entered the market that "from a consumer perspective are substitutable to traditional services, but do not have to comply with the same set of rules."[190] This is based on a flawed understanding of the services at issue and a failure to recognize that the Internet has flourished largely due to *not* treating over-the-top services like traditional telecommunications providers.

Recognizing that the EU's approach to the protection of user privacy differs from that of the U.S., there must be valid mechanisms in place that allow for the interoperability of privacy regimes and enable cross-border data flows. The EU-U.S. Privacy Shield framework has been in place since 2016. In October, the European Commission issued its third annual report recommending the continuation of the agreement on the transfer of commercial data between the EU and the United States.[191] To date, close to 5,000 companies are now certified under the Privacy Shield. Its existence may be threatened by court challenges or modifications made during future annual reviews.[192] 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. While one challenge was dismissed for lack of standing,[193] the other remains pending.

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

---

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

[190] *Id*. at recital 6.

[191] Press Release, EU-U.S. Privacy Shield: Third Review Progress While Identifying Steps for Improvement, European Commission, Oct. 22, 2019, https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6134.

[192] 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.

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

parties that allege such clauses are inadequate on grounds similar to those used to invalidate the Privacy Shield's predecessor, the Safe Harbor.[194] 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.[195]

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.[196]

Data Localization

As CCIA raised in previous NTE comments, there have been attempts to establish an EU-wide cloud that would localize data within EU borders.[197] The latest push for a European-only cloud appears once again to be driven by German lawmakers and industry,[198] as well as French

---

[194] 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.").

[195] Melissa Baustein, *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/.

[196] 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/europeanunion/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 "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.").

[197] *CCIA 2018 NTE Comments*, *supra* note 38.

[198] *CCIA 2018 NTE Comments*, *supra* note 38 (discussing Germany's attempts to telecommunication service providers and Internet service providers to store data in Germany for a period of 10 weeks. Under the draft law, data needing to be stored includes phone numbers, times called, IP addresses, and the international identifiers of mobile users for both ends of a call. Furthermore, user location data in the context of mobile phone services would have to be retained for a period of four weeks. The German Bundestag approved the bill in October 2015. While

industry and policymakers. The Germany Economy Minister announced this year that they were working on a plan to create Europe's own cloud services, titled "Gaia-X".[199] At the same time, the French Economy Minister has characterized the U.S. CLOUD Act as an overstep into France's sovereignty and is helping local industry players exclude U.S. industry from public procurements.[200] More recently, Thierry Breton, who has long advocated for data localization measures[201] in his tenure as CEO and Chairman of Atos, has been put forward as Commissioner-designate responsible for EU's digital policies. Mr. Breton has previously called for an "EU data schengen area" and similar measures to that effect.[202] Atos has also been involved in the set-up of the Gaia-X project.[203]

Following a rise in data localization measures across EU Member States,[204] 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.[205] The regulation aims to remove national mandated data localization laws within Member States and is yet to be tested. In principle, CCIA welcomes the new rules as they seek to limit forced data localization in EU Member States

---

policymakers might reasonably impose certain security-related limits to some sets of secure data, centralization and streamlining efforts may effectively result in the application of localization mandates to all government services)

[199] Sourav D, *Germany Economy Minister Plans a European Cloud Services "Gaia-X"*, FINANCIAL WORLD (Aug. 25, 2019), https://www.financial-world.org/news/news/economy/3046/german-economy-minister-plans-a-european-cloud-service-gaiax/; Barbara Gillmann, *Europa-Cloud Gaia-X Startet Im Oktober*, HANDELSBLATT (Sept. 3, 2019), https://www.handelsblatt.com/politik/deutschland/datenplattform-europa-cloud-gaia-x-startet-im-oktober/24974718.html?ticket=ST-17113409-EQBXZiVMUtkUvXJtASJt-ap5.

[200] *France Recruits Dassault Systemes, OVH for alternative to U.S. cloud firms*, REUTERS (Oct. 3, 2019), https://www.reuters.com/article/us-france-dataprotection/france-recruits-dassault-systemes-ovh-for-alternative-to-u-s-cloud-firms-idUSKBN1WI189.

[201] *See* EU COMMISSION, *Cloud Computing Must Tackle the Security Challenges* (Sep. 25, 2013) (detailing Mr Breton's comments at a 'European Cloud Partnership' meeting in 2013); Thierry Breton: *« La France est entrée dans l'ère de la cyberguerre »*, LES ECHOS (July 5, 2019), https://www.lesechos.fr/tech-medias/hightech/thierry-breton-la-france-est-entree-dans-lere-de-la-cyberguerre-1035834.

[202] M. Breton has long pushed for a European cybersecurity Cloud label, which first shaped a French Cloud cybersecurity certification and more recently, a Franco-German cybersecurity certification. *See Secnumcloud Évolue et Passe À L'heure due RGPD*, ANSSI, https://www.ssi.gouv.fr/actualite/secnumcloud-evolue-et-passe-a-lheure-du-rgpd/; European Secure Cloud Label, Federal Office for Information Security [Germany], https://www.bsi.bund.de/EN/Topics/CloudComputing/ESCloudLabel/ESCloudLabel_node.html. The latter excludes data storage outside the EU. See ES Clous Computing Principles, *available at* https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ESCloud_Label/Annex_B_Core_Principles.pdf;jsessionid=E810205C403D41E71F2BD624E0F7C0A2.1_cid341?__blob=publicationFile&v=3.

[203] See Tweet of Atos Deutschland, Oct. 29, 2019 https://twitter.com/Atos_DE/status/1189222053909585925.

[204] 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.

[205] Press Release, 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.

and provide legal clarity for companies and users.[206] However, in early 2019, the European Commission published non-binding interpretative guidance which unfortunately provides Member States more leeway to restrict the free flow of data when both personal and non-personal data are involved.[207] Furthermore, 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.[208]

Cybersecurity Certifications

The EU is currently implementing a new regulation (the "Cybersecurity Act") which introduces a pan-European framework to develop cybersecurity certifications for any kind of ICT products launched in the EU market.[209] The Regulation mandates the EU Cybersecurity Agency (ENISA) and Member States to develop voluntary certification schemes for most ICT products, as well as mandatory certification schemes for ICT products "requiring a high level of assurance". To this date, 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.[210] Market players, especially smaller ones, may face increased entry costs if the outcome of the final negotiations disregards the possibility of self-

---

[206] 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/.

[207] Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, 29 May 2019, COM(2019) 250, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0250&from=EN.

[208] 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.").

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

[210] *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 (Sept. 13, 2017), https://eurlex.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.

conformity assessments — as the Council text[211] 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.

EU Value-Added Tax

The EU Value Added Tax (VAT) system for e-commerce has consistently been identified as a non-tariff trade barrier, even within the EU Single Market.[212] Industry reports difficulties with the registration system that is fragmented across the EU, complex, and particularly costly for SMEs. The European Commission has proposed a number of reforms to the VAT processes to provide more legal certainty for exporters in the region, but non-EU merchants are poised to remain disadvantaged due to high costs of compliance.[213]

Goods Package

Last December, the Commission 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)[214] which is aimed at increasing enforcement of existing EU product legislation and advancing customer safety. However, industry and U.S. offices have expressed concerns that the Regulation will do little to improve overall customer safety and have unintended effects.[215]

The final Regulation on market surveillance and product compliance entered into law on July 15, 2019, and the majority of the provisions will take effect on July 16, 2021.[216] The final text includes a number of ambiguities. Article 4 requires that sellers of goods in the EU have a dedicated "responsible person" based in the EU that is responsible for maintaining compliance documentation and cooperating with market surveillance authorities to furnish information as

---

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

[212] 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.

[213] *See* Press Release, *VAT: New Details on Rules for E-commerce Presented*, Dec. 11, 2018, https://europa.eu/rapid/press-release_IP-18-6732_en.htm; Press Release, *European Commission Proposed Far-Reaching Reform of the EU VAT System*, Oct. 4, 2017, https://europa.eu/rapid/press-release_IP-17-3443_en.htm.

[214] 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.

[215] Press Release, *Industry Groups Express Concerns with EU 'Goods Package'*, Feb. 7, 2019, http://www.ccianet.org/2019/02/industry-groups-express-concerns-with-eu-goods-package/; Tweet of U.S. Ambassador to EU, Feb. 7, 2019, https://twitter.com/USAmbEU/status/1093472353844191234.

[216] Press Release, *EU Adopts Regulation to Keep Unsafe Products Off the Market*, June 14, 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/06/14/eu-adopts-regulation-to-keep-unsafe-products-off-the-market/.

required. The Regulation does not offer sufficient clarity regarding the responsibilities and possible liability for the "responsible person" as it pertains to different fulfilment service providers. There are concerns that this 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. Additional guidance is needed for exporters who wish to sell goods in the EU market, as well as to confirm that the new Regulation is consistent with the EU's obligations under the WTO Technical Barriers to Trade Agreement on conformity assessment measures.[217]

Extended Producer Responsibility (EPR) Regulations

Industry reports issues when moving goods cross-border within the EU pursuant to a number of customs regulations under EU environmental legislation.[218] Under EPR legislation, the "producer", understood to be the seller of record, must register, report, and pay for certain products or materials that the producer ships to an EU jurisdiction. However, requirements are not harmonized across EU Member States, and a seller shipping into all EU countries is required to comply with 28 different regimes. Industry reports that countries have adopted varying EPR fees for different types of products, and require registration with various so called "compliance schemes" (*e.g.* organizations in charge of the collection of recycling fees) at national level, and filing of complex reports in thousands of different categories which do not align between countries, when selling goods to the market. Industry has estimated that compliance costs amount to 5,000 € per country, per seller.

According to industry reports, online marketplaces are not allowed to remit fees on behalf of their sellers, unless they become a so-called "authorized representative" which requires lengthy and costly contractual setup between Marketplace and seller and still requires detailed product and material level reporting, hence not enabling the seller (often an SME) to benefit from the single market. Furthermore, under the current regime, sellers on online marketplaces are often faced with a double payments issue where the vendor pays the relevant EPR fee in the country where it places the goods on the market originally ('Country A'), and the seller is then

[217] Agreement on Technical Barriers to Trade (TBT), 1868 U.N.T.S. 120.

[218] This includes the Waster Electrical & Electronic Equipment Directive, Batteries and Packaging Directive, and "Extended Producer Responsibility" legislation.

asked to pay the relevant EPR fee in the country of destination, if the goods are exported to another country ('Country B'). Some countries allow for the reimbursement of fees; however the documentary evidence is substantial and often discourages SMEs. Instead of these complex, and inconsistent regulations, the EU should introduce a simplified flat fee payment, based on average product information rather than actual detailed data, on the basis of which a marketplace will be allowed to remit recycling fees on behalf of its sellers.

13. Egypt

Government-Imposed Content Restrictions and Related Access Barriers

In 2018, Egypt passed a new law that requires all social media users with more than 5,000 followers to procure a license from the Higher Council for Media Regulation.[219] Reports continue to show the government's increased use of censorship and mandated content filtering.[220]

Additional E-Commerce Barriers

Industry reports a number of inconsistencies, subjectivity, and lack of clarity regarding import process that pose a barrier to shipping in the region. For example, valuation during import processes is highly inconsistent, even after declaring the value of goods and following official processes. Further, firms that wish to import products into Egypt must register, but are required to have a permanent establishment in the region to registered. This largely restricts smaller e-commerce sellers from expanding in the market.

14. France

Copyright Liability Regimes for Online Intermediaries

France proposed legislation in October 2019 intending to implement the EU Copyright Directive, through the ongoing audiovisual reform.[221] Previously, French officials indicated that filters would be required under implementing legislation.[222] The proposals appear to also insufficiently provide for the exception outlined under the Directive as it pertains to the filtering

[219] *2018 Freedom on Net Report*, *supra* note 27, at 13.

[220] Freedom on the Net 2018 Country Report: Egypt, https://freedomhouse.org/report/freedom-net/2018/egypt (last visited Oct. 31, 2019).

[221] Available at http://electronlibre.info/wp-content/uploads/2019/10/2019-09-30-PJL-audio-complet.pdf [France].

[222] Mike Masnick, *After Insisting That EU Copyright Directive Didn't Require Filters, France Immediately Starts Promoting Filters*, TECHDIRT (Mar. 28, 2019), https://www.techdirt.com/articles/20190327/17141241885/after-insisting-that-eu-copyright-directive-didnt-require-filters-france-immediately-starts-promoting-filters.shtml.

requirement. Specifically, the proposal replaces the prohibition on removal of safeguards that allow users to rely on exceptions granted in Article 17(7) of the Directive. Instead, there is only an obligation to inform users about relevant exceptions in terms and conditions.

Imbalanced Copyright Laws and "Link Taxes"

France has already started to implement this provision of the EU Copyright Directive as it created a new right for press publishers which entered into force in October.[223] French press publishers may now request payment from platforms when they display a short preview of snippets of their content online in ways that would be treated as fair use under U.S. law. Following this development, Google announced on September 25 that it would stop showing preview content in France for European news publications.[224] On October 2, the French competition authority decided to open a preliminary investigation into Google in relation to conduct aimed at complying with the French law.[225]

Digital Services Tax

On July 24, French legislation implemented a 3% tax on revenue generated in France derived from digital intermediary services and digital advertising services.[226] The tax is applied retroactive to January 1, 2019, with the first pay date in November 2019. The tax carries a high revenue threshold, effectively targeting leading U.S technology firms operating in France while carving out most French firms that offer the same services. French Finance Minister Bruno Le Maire has regularly referred to the tax as a "GAFA tax" and stated that the goal is to target the "American tech giants" for special taxation.[227] French Government sites and representatives of the French National Assembly and Senate refer to the French DST as a "GAFA" tax and cite specific American companies in reports.[228] Based on French officials' own admission, the

---

[223] Loi 2019-775 du 24 juillet 2019 à créer un droit vosin au profit des agencies de presse et des éditeurs de presse [Law 2019-775 of July 24, 2019 Law creating a neighboring right for press publishers and news editors], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE] [OFFICIAL GAZETTE OF FRANCE], Oct. 5, 2019.

[224] Richard Gingras, *How Google Invests in News*, GOOGLE BLOG (Sept. 25, 2019), https://www.blog.google/perspectives/richard-gingras/how-google-invests-news/.

[225] David Meyer, *French Publishers Have Gone to War With Google. They Are Not Likely to Win*, FORTUNE (Oct. 25, 2019), http://www.fortune.com/2019/10/25/french-publishers-google-copyright-competition/.

[226] LOI n° 2019-759 du 24 juillet 2019 portant création d'une taxe sur les services numériques et modification de la trajectoire de baisse de l'impôt sur les sociétés [Fr.] [hereinafter "Law on the Creation of a Tax on Digital Services"].

[227] *See* Submission of CCIA *In Re Section 301 Investigation of French Digital Services Tax* Docket No. USTR 2019-0009 (filed Aug. 19, 2019), *available at* http://www.ccianet.org/wp-content/uploads/2019/08/USTR-2019-0009-CCIA-Written-Comments-on-French-Digital-Tax.pdf at 6-8.

[228] *See, e.g.*, Assemblée nationale, Projet de loi de finances pour 2019, http://www.assembleenationale.fr/15/cri/2018-2019/20190108.asp (representatives making multiple reference on the

majority of firms that will pay the tax will be American.[229] The legislation does not include a sunset clause and statements by French officials make it unclear whether France will withdraw the national tax after the OECD reaches a solution. CCIA supports USTR's decision to pursue a Section 301 Investigation under the Trade Act of 1974 regarding the French DST in order to discourage other countries from pursuing a similar tax.

Government-Imposed Content Restrictions and Related Access Barriers

France has pursued a number of content-based regulations over the past year, and also made it a focus of its presidency of the G7 for 2019. In March, the National Assembly proposed a very broad law on combating hate speech ("*Lutte contre la haine sur internet*").[230] Legislation regarding hate speech had been anticipated, but the new text expands to terrorist content and other harmful content. As currently drafted, the law would require designated Internet services to take down hateful comments reported by users within 24 hours. The law targets any hateful attack on someone's "dignity" on the basis of race, religion, sexual orientation, gender identity, or disability. If platforms in scope do not comply, they could face an administrative penalty of 4% of their global revenue and penalties could reach tens of millions of euros. The French Parliament approved the legislation in July, and it is expected that the Senate will debate and likely adopt this law later this year. France notified the European Commission regarding its intent to finalize legislation quickly, but the Commission rejected France's application for

---

intent of France to introduce a tax on GAFA and "ces géants du numérique souvent américains"); Remarks of M. Benoit Potterie, Assemblée nationale Commission des finances, de l'économie générale et du contrôle budgétaire, Apr. 2, 2019, http://www.assemblee-nationale.fr/15/cr-cfiab/18-19/c1819064.asp (citing the need to tax the digital giants ("des géants du numérique") and identifying the "GAFA (Google, Amazon, Facebook, Apple)"); "); Remarks of Mme Sabine Rubin, Assemblée nationale Commission des finances, de l'économie générale et du contrôle budgétaire, Apr. 2, 2019, http://www.assemblee-nationale.fr/15/cr-cfiab/18-19/c1819064.asp (stating that "Sur le fond, taxer davantage les grandes multinationales, en particulier les GAFA, est un souhait louable et partagé sur tous les bancs de cette commission et, je le suppose, de notre Assemblée." [Taxing more large multinationals, in particular the GAFA, is a laudable and shared wish by this commission and our Assembly.]).

[229] Boris Cassel and Séverine Cazes, «Taxer les géants du numérique, une question de justice fiscale», affirme Bruno Le Maire, LE PARISIEN (Mar. 2, 2019), http://www.leparisien.fr/economie/taxer-les-geants-du-numeriqueune-question-de-justice-fiscale-affirme-bruno-le-maire-02-03-2019-8023578.php ("Une trentaine de groupes seront touchés. Ils sont majoritairement américains, mais aussi chinois, allemands, espagnols ou encore britanniques. Il y aura également une entreprise française et plusieurs autres sociétés d'origine française, mais rachetées par des grands groupes étrangers.") [There will be 30 holdings affected. The majority of them are American, but also Chinese, German, Spanish, and British. There will be one French company and others whose origins are French, but owned by foreign entities.]

[230] Lutte contre la haine sure internet, Assemblee National, http://www.assemblee-nationale.fr/dyn/15/dossiers/lutte_contre_haine_internet.

emergency procedure (to allow for France to bypass the 3-month waiting period under EU law).[231]

Data Localization

France has indicated that they will direct resources to build a national "trusted cloud".[232] Updates on this initiative are expected in December 2019. This follows France's "Cloud First" policy adopted in 2018 and public statements of distrust of U.S. services. For example, the French Economy Minister has characterized the U.S. CLOUD Act as an overstep into France's sovereignty and is helping local industry players exclude U.S. industry from public procurements.[233] France and Germany released a joint statement on October 29, 2019 indicating their commitments to collaborate on a European data infrastructure.[234] This serves as a protectionist barrier for U.S. cloud service providers in the public sector in France.

15. Germany

Government-Imposed Content Restrictions and Related Access Barriers

Germany adopted the Act to Improve the Enforcement of Rights on Social Networks (the "Network Enforcement Law" or "NetzDG") in June 2017.[235] The NetzDG law mandates removal of "manifestly unlawful" content within 24 hours, and provides for penalties of up to 50 million euros.[236] Unlawful content under the law includes a wide range of content from hate speech to unlawful propaganda. The large fines and broad considerations of "manifestly

---

[231] Notification Detail to the European Commission "Law Aimed at Combating Hate Content on the Internet", *available at* https://ec.europa.eu/growth/tools-databases/tris/en/index.cfm/search/?trisaction=search.detail&year=2019&num=412&mLang=en&CFID=6924737&CFTOKEN=fefae3121f578503-A5B3C277-C150-D1EA-86D5B610B60318F9.

[232] Leigh Thomas, *France Recruits Dassault Systemes, OVH For Alternative to U.S. Cloud Firms*, REUTERS (Oct. 8, 2019), https://www.reuters.com/article/us-france-dataprotection/france-recruits-dassault-systemes-ovh-for-alternative-to-u-s-cloud-firms-idUSKBN1WI189 ("France has enlisted tech companies Dassault Systemes and OVH to come up with plans to break the dominance of U.S. companies in cloud computing, its finance minister said on Thursday. Paris is eager to build up a capacity to store sensitive data in France amid concerns the U.S. government can obtain data kept on the servers of U.S. companies such as Amazon and Microsoft.").

[233] Leigh Thomas, *France Recruits Dassault Systemes, OVH for alternative to U.S. cloud firms*, REUTERS (Oct. 3, 2019), https://www.reuters.com/article/us-france-dataprotection/france-recruits-dassault-systemes-ovh-for-alternative-to-u-s-cloud-firms-idUSKBN1WI189.

[234] Press Release, *Franco-German Common Work on a Secure and Trustworthy Data Infrastructure*, Oct. 29, 2019, https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=04A8A0E-2AD2-4469-BF93-FDC4B601988F&filename=1511%20%20%20Gemeinsame%20Pressemitteilung_%20Franco-German%20Collaboration%20on%20Data%20In.%20w%20logo_.pdf.

[235] 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-techcompanies-c352efbbb993.

[236] Id. § 3(2).

unlawful content"[237] have led to companies removing lawful content, erring on the side of caution in attempts to comply.[238] Since coming into force in January 2018, the law has already led to high profile cases of content removal and wrongful account suspensions. Companies have repeatedly raised concerns regarding the law's specificity and transparency requirements[239] and groups have expressed concerns about its threats to free expression.[240] The German government indicated that changes were needed to the law last year,[241] but there is now a more urgent push to amend the law.[242] On October 30, the German Federal Ministry of the Interior and the Federal Ministry of Justice released a legislative package on combating hate speech that includes changes to NetzDG and introduces new proactive reporting requirements for online services.[243] Industry is currently evaluating the proposal.

Further concerning is the potential domino effect of this policy on other regimes. Russia, Singapore, and the Philippines have cited this law as a positive example which policymakers

---

[237] 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 telemedia 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 G*ermany: 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-hostedcontent-under-facebook-act/.

[238] *See* CEPS, *Germany's NetzDG: A Key Test for Combatting Online Hate* (2018), *available at* https://www.ceps.eu/system/files/RR%20No2018-09_Germany%27s%20NetzDG.pdf.

[239] Thomas Escritt, *Germany Fines Facebook for Under-Reporting Complaints*, REUTERS (July 2, 2019), https://www.reuters.com/article/us-facebook-germany-fine/germany-fines-facebook-for-under-reporting-complaints-idUSKCN1TX1IC.

[240] 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.").

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

[242] Janosch Delcker, *German MP Push NetzDG Update*, POLITICO (Oct. 28, 2019), https://www.politico.eu/pro/politico-pro-morning-tech-merkels-government-talks-tech-in-dortmund-german-mps-push-netzdg-update-technological-sovereignty/.

[243] Maßnahmenpaket zur Bekämpfung des Rechtsextremismus und der Hasskriminalität [Measures to Combat Right-Wing Extremism and Hate Crime], *available at* https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2019/massnahmenpaket-bekaempfung-rechts-und-hasskrim.pdf?__blob=publicationFile&v=5; Press Release, *Against Right-Wing Extremism and Hate Crime*, Oct. 30, 2019, FEDERAL MINISTRY OF THE INTERIOR, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/10/kabinett-beschliesst-massnahmen-gg-rechtsextrem-u-hasskrim.html.

intend to copy in the future to regulate speech.[244] Cases arising under this law will also have implications on extraterritoriality.[245]

Asymmetry in Competition Frameworks

Germany is currently in the process of reforming its competition rules. Reports indicate that a central part of the reform will be to "move to a preventative level (*ex ante*) imposing precautionary antitrust responsibilities on companies rather than waiting for an abuse to take place before taking action."[246] German authorities have also proposed targeting online platforms and other companies supposedly "transcend" their dominance in a given market based on vertical integration concerns or access to sensitive data. Another proposed rule would shift the burden of proof away from competition authorities and towards targeted companies. Many of these proposals are starkly inconsistent with longstanding U.S. and global competition norms and, if adopted, could serve as trade barriers.

Data Localization

The Germany Economy Minister announced this year that they were working on a plan to create Europe's own cloud services, titled "Gaia-X".[247] This project would connect existing central and decentralized infrastructure solutions via open source applications and interoperable solutions.[248] France and Germany released a joint statement on October 29, 2019 indicating their commitments to collaborate on a European data infrastructure.[249] U.S. cloud service providers could be disadvantaged from operating in these markets as a result of these protectionist measures.

---

[244] *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.

[245] *See* EU Section of these comments.

[246] Simon Van Dorpe, *Germany Gets Touch on Silicon Valley*, POLITICO (Oct. 11, 2019), https://www.politico.eu/pro/germany-gets-tough-on-silicon-valley.

[247] Sourav D, *Germany Economy Minister Plans a European Cloud Services "Gaia-X"*, FINANCIAL WORLD (Aug. 25, 2019), https://www.financial-world.org/news/news/economy/3046/german-economy-minister-plans-a-european-cloud-service-gaiax/; Barbara Gillmann, *Europa-Cloud Gaia-X Startet Im Oktober*, HANDELSBLATT (Sept. 3, 2019), https://www.handelsblatt.com/politik/deutschland/datenplattform-europa-cloud-gaia-x-startet-im-oktober/24974718.html?ticket=ST-17113409-EQBXZiVMUtkUvXJtASJt-ap5.

[248] Further details are expected at the German Digital Summit in October 2019.

[249] Press Release, *Franco-German Common Work on a Secure and Trustworthy Data Infrastructure*, Oct. 29, 2019, https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=04A8A0E-2AD2-4469-BF93-FDC4B601988F&filename=1511%20%20%20Gemeinsame%20Pressemitteilung_%20Franco-German%20Collaboration%20on%20Data%20In.%20w%20logo_.pdf.

16. Greece

Copyright Liability Regimes for Online Intermediaries

Greece recently amended its copyright law to establish a new model of copyright enforcement by creating an administrative committee that can issue injunctions to remove or block potentially infringing content. Under this system, a rightsholder may now choose to apply to the "Commission for the notification of online copyright and related rights infringement" for the removal of infringing content in exchange for a fee.[250] As an extrajudicial process, there is a fear that government restriction of online speech will occur absent due process. The Commission issued its first decision in November 2018 under this new process.

17. India

India is a region of continued growing concern for U.S. Internet exporters. India has an increasingly vibrant e-commerce market, illustrated by the high value of digital exports and imports.[251] The Indian Government has set ambitious goals for the country's digital future. This is notable with India's improved ranking in the World Bank's Ease of Doing Business report for the third consecutive year.[252] However, the government has continued to pursue a digital agenda that undermines this growing potential. Proposed and new regulations restrict cross-border data flows, bolster domestic companies through protectionist measures, and ultimately hinder global

[250] Eleonora Rosati, *Greece New Notice and Takedown Administrative Mechanism for Online Copyright Cases Now in Force*, THE IP KAT (Mar. 5, 2018), http://ipkitten.blogspot.com/2018/03/greece-new-notice-and-take-down.html.

[251] WORLD TRADE ORGANIZATION, World Trade Statistical Review 2018 (2018), *available at* https://www.wto.org/english/res_e/statis_e/wts2018_e/wts2018_e.pdf at 166; MCKINSEY GLOBAL INSTITUTE, Digital India: Technology to Transform a Connected Nation (Mar. 2019), *available at* https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation ("India is one of the largest and fastest-growing markets for digital consumers, with 560 million internet subscribers in 2018, second only to China. Indian mobile data users consume 8.3 gigabits (GB) of data each month on average, compared with 5.5 GB for mobile users in China and somewhere in the range of 8.0 to 8.5 GB in South Korea, an advanced digital economy. Indians have 1.2 billion mobile phone subscriptions and downloaded more than 12 billion apps in 2018.").

[252] INVEST INDIA, *India's Hat Trick in World Bank's Doing Business Report* (Oct. 24, 2019), https://www.investindia.gov.in/team-india-blogs/indias-hat-trick-world-banks-doing-business-2020 (noting that India has recently moved up to #63 from #74 this year); WORLD BANK GROUP, Doing Business 2019: Training For Reform (2019), *available at* http://www.worldbank.org/content/dam/doingBusiness/media/Annual-Reports/English/DB2019-report_webversion.pdf. *See also* Arvind Gupta & Philip Auerswald, *The Ups and Downs of India's Digital Transformation*, HARVARD BUSINESS REVIEW (May 6, 2019), https://www.hbr.org/2019/05/the-ups-and-downs-of-indias-digital-transformation.

trade flows. CCIA strongly supports the efforts of the U.S. and India in discussions for a trade agreement that will foster digital trade between the two countries.[253]

Digital Taxation

India's recent changes to its taxation regime depart from global norms on taxation nexus and target the Internet economy. The new tax rules do so by introducing the concept of a digital permanent establishment, determining that a "significant economic presence" meets the standards of permanent establishment for taxation purposes.[254] Further guidelines and changes are contemplated.[255]

Customs Duties on Electronic Transmissions

India has also been critical of the World Trade Organization's moratorium on customs duties on electronic transmissions and believes that ending the moratorium will enable the growth of domestic businesses.[256] Any imposition of new duties on electronic transmission would be inconsistent with India's WTO commitments and would significantly impact an exporter's ability to operate in India's increasingly growing digital economy.

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates

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 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.

---

[253] Industry Letter to Ambassador Lighthizer on U.S.-India Trade, Sept. 20, 2019, http://www.ccianet.org/wp-content/uploads/2019/09/Letter-to-Amb-Lighthizer-on-India-Trade_9-20-2019.pdf.

[254] *"Users" May Be Basis for Attribution of Profits to Digital PE*, DELOITTE (May 8, 2019), https://www.taxathand.com/article/11572/India/2019/Users-may-be-basis-for-attribution-of-profits-to-digital-PE.

[255] The Ministry of Finance launched a consultation in 2019. *See* Ministry of Finance, Government of India, Public Consultation on the Proposal for Amendment of Rules for Profit Attribution to Permanent Establishment Reg. April 2019, *available at* https://www.incometaxindia.gov.in/Lists/Latest%20News/Attachments/306/Public_consultation_Notice_18_4_19.pdf.

[256] DEPT. FOR PROMOTION OF INDUSTRY AND INTERNAL TRADE, Draft National e-Commerce Policy (2019), *available at* https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf [hereinafter "India National E-Commerce Strategy"] at 10 ("By making the moratorium permanent, and with more and more products now traded digitally in the era of additive manufacturing and digital printing, the GATT schedule of countries will erode and will vanish ultimately. Assuming that all nonagriculture products can be traded electronically, then everything will be traded at zero duty. So, the protection that is available to India, for the nascent industries in the digital arena will disappear at once, and that is an immensely important issue which concerns public policy makers in the developing world.").

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.[257]

India's draft Personal Data Protection bill was released in July 2018, and as of 2019, remains under consideration.[258] The bill is expected to be tabled in Parliament in December. As drafted, the law presents a comprehensive national mandate for data localization and 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 India. Only limited exceptions are provided for both the transfer of "personal" and "critical" data.[259] 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 2011 changes 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

---

[257] Nigel Cory, *Opinion: The RBI's Misguided Digital Protectionism*, LIVE MINT (Aug. 23, 2018), https://www.livemint.com/Opinion/bHelcN7RR5rQ5r3hPxXGRP/Opinion--The-RBIs-misguided-digital-protectionism.html ("The Reserve Bank of India's (RBI's) proposal that digital payment companies store all user data in India by October is both unnecessary and misguided. If the RBI's underlying concern relates to ensuring the Indian government's access to data for regulatory oversight, that's simply no justification for such a data localization policy. Firms can readily use the convenience of modern information technologies (such as cloud computing) to facilitate such access with the click of a button. Where the data is stored is irrelevant in this scenario.").

[258] However, transparency concerns regarding the process and official timeline remain. *Future of India's Personal Data Protection Bill Shrouded in Secrecy*, IAPP (July 29, 2019), https://iapp.org/news/a/future-of-indias-personal-data-protection-bill-shrouded-in-secrecy/.

[259] Remarks made by Minister Ravi Shankar Prasad indicate that changes may be made to only require localization for 'critical personal data', but uncertainty remains until the final text is submitted. *See Sensitive, Super-Sensitive Data Must Remain in India, Says Union Minister Prasad*, HINDU BUSINESS LINE (Sept. 20, 2019), https://www.thehindubusinessline.com/info-tech/sensitive-super-sentitive-data-must-remain-in-india-says-union-minister-ravi-shankar-prasad/article29468552.ece.

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 the use of private services regardless of geographic origin.[260]

Industry reports that U.S. cloud computing services already face a number of 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. 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.[261] 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.

Across different ministries in India, localization requirements are also being added to a variety of new policies that will disrupt online services in India and discourage foreign direct investment. Earlier this year, the Department for Promotion of Industry and Internal Trade (DPIIT) launched a consultation on the Draft National e-Commerce policy that outlined a number of concerning policy proposals including further restrictions cross-border data flows and restrictions on foreign direct investment.[262] The development of the draft policy had significant process and representation concerns.[263] CCIA outlined concerns with the policy

---

[260] Chander & Lê, Data Nationalism, *supra* note 17, at 694-97.

[261] *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-wantslocalization-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.").

[262] *India National E-Commerce Strategy*, *supra* note 256.

[263] 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.

recommendations and contemplated regulatory strategies in comments filed with DPIIT.[264] India also released a "National Strategy for Artificial Intelligence" in June 2018 that proposes regulatory practices and guidelines.[265]

Digital Communications Policy Priorities

In 2018, the Department of Telecommunications released the "Indian Governments National Data Communications Plan (NDCP) 2018" laying out a good future framework for the Indian telecommunications sector.[266] India should prioritize and implement the key areas as soon as possible. This includes two areas where TRAI is currently in consultation: (1) restrictions around cloud technologies and platforms, and (2) "Other service providers" (OSP) Guidelines.

While India favors promoting cloud-based technologies, there are challenges in terms of Telecom Ministry (DoT) approval for implementing cloud services for local sites such as for contact center operations. Cloud services are important for economies of scale and for technological and business model innovation. CCIA supports light-touch regulation around cloud services and customers should be free to choose services irrespective of the technology or platform used. Any concerns around security and privacy can be covered in existing or developing DP and related regimes.

OSP Guidelines are outdated and are not in line with new technologies and should be liberalized and deregulated. OSP regulation is rare globally. The current definition of OSP is very broad and covers almost all services that utilize voice, data, and Internet services. This leads to interpretation issues among enforcement agencies and uncertainty for businesses.

On a general note, industry reports difficulties in obtaining written clarity on telecommunication policy interpretations due to the lack of a formal mechanism for a central source of interpretation. For instance, there can be different interpretations of policy and regulations but different agencies within the DoT throughout the country.

---

[264] *See* Comments of CCIA to India National E-Commerce Strategy, filed Mar. 2019, *available at* http://www.ccianet.org/wp-content/uploads/2019/03/CCIA-Comments-on-India-National-E-Commerce-Strategy.pdf.

[265] NITI Aayog, National Strategy for Artificial Intelligence (June 2018), https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf.

[266] DEP. OF TELECOMMUNICATIONS, National Digital Communications Policy 2018, *available at* http://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf.

Additional E-Commerce Barriers

In September, MeitY created a committee to deliberate on a data governance framework for non-personal data.[267] The committee is expected to recommend a framework that facilitates sharing of non-personal data, but "non-personal data" is not defined as of yet. Industry reports concerns on the extension of the framework to proprietary data, or data protected by trade secrets.

Changes were recently made to India's foreign direct investment rules for e-commerce providers and these rules became effective in 2019.[268] These rules further disadvantage foreign e-commerce sellers in the Indian retail market.

Online Content Regulations

MeitY held a consultation in 2019 seeking comments on a proposal to amend rules created pursuant to Section 79 of the Information Technology Act (IT Act), which provides liability protections for online intermediaries.[269] The Indian government recently informed the Supreme Court that the process of notifying the revised intermediary rules will conclude by January 15, 2020, likely without any additional consultation with industry. CCIA urges USTR to raise strong concerns about these new requirements.

---

[267] Ministry of Electronics & Information Technology, Constitutional Committee of Experts to Deliberate on Data Governance Framework, https://meity.gov.in/content/constitution-committee-experts-deliberate-data-governance-framework.

[268] *See Explainer: What Are India's New Foreign Direct Investment Rules for E-Commerce?*, REUTERS (Jan. 31, 2019), https://in.reuters.com/article/india-ecommerce-explainer/explainer-what-are-indias-new-foreign-direct-investment-rules-for-e-commerce-idINKCN1PP1XS. Similar changes were contemplated in a prior draft of the National E-Commerce Strategy CCIA identified in 2018 comments. *See 2018 CCIA Comments, supra note* 38 at 57 ("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 ecommerce 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 wasn't extended to companies with foreign equity and protects the interests of companies promoted by Indian entrepreneurs over foreign equity-held companies").

[269] See Comments of CCIA to India Ministry of Electronics and Information Technology, filed Jan. 31, 2019, available at https://www.ccianet.org/wp-content/uploads/2019/02/Comments-of-CCIA-to-MeitY-on-Draft-Intermediary-Guidelines-2018-1.pdf.

The draft amendments would replace the 2011 Information Technology (Intermediary Guidelines) Rules and introduce new obligations on online intermediaries. Under the proposal, intermediaries must remove content within 24 hours upon receipt of a court order or Government notification and deploy tools to proactively identify and remove unlawful content (Amendment 9, Amendment 8, and Amendment 3(5)). There are also concerning law enforcement assistance provisions, including a requirement for intermediaries to "enable tracing out of such originator of information on its platform" at the request of government officials (Amendment 3(5)), and local incorporation and local presence requirements (Amendment 7).

Filtering and 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."[270] Often the shutdowns are in response to or in preparation for actions that may cause disturbances or violence.[271] These shutdowns stand in stark contrast to India's recent efforts to expand Internet services across the country. 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.[272]

As CCIA has raised in previous NTE comments, India has also ordered a number of filtering and removal requirements on social media and other Internet communication platforms.[273] While hardly the only country whose authorities are demanding speech and content restrictions by intermediaries, it is discouraging that India, as a quickly emerging player in the global Internet economy, does not foster a regulatory environment that encourages innovation and free expression.

---

[270] 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.

[271] *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.

[272] Darrell M. West, Internet Shutdowns, *supra* note 35, at 7.

[273] *CCIA 2018 NTE Comments*, *supra* note 38, at 58-59.

Extraterritorial Regulations and Judgments

Concerns regarding intermediary frameworks and content regulations are exacerbated by court mandates for global takedowns. A recent decision by the Delhi High Court suggests that India will now follow Canada and the EU regarding global injunctions.[274]

18. Indonesia

Customs Duties on Electronic Transmissions

Indonesia issued Regulation No.17/PMK.010/2018 (Regulation 17) in 2018.[275] 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's commitment under the WTO's moratorium on customs duties on electronic transmissions, dating back to 1998[276] and most recently reaffirmed in December 2017.[277] 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, and as the renewal for the moratorium comes up at the end of this year. Indonesia must rescind Regulation 17 and remove Chapter 99 from its HTS.

Additional Barriers to E-Commerce

U.S. firms face additional barriers in Indonesia through the country's restrictions on foreign direct investment for e-commerce services. Foreign firms cannot directly retail many products through electronic services. Ownership for physical distribution, warehousing, and

---

[274] *See* Swami Ramdev & Anr. v. Facebook, Inc., High Court of Delhi at New Delhi, Oct. 23, 2019, *available at* http://lobis.nic.in/ddir/dhc/PMS/judgement/23-10-2019/PMS23102019S272019.pdf ("The interpretation of Section 79 as discussed hereinabove, leads this Court to the conclusion that the disabling and blocking of access has to be from the computer resource, and such resource includes a computer network, i.e., the whole network and not a mere (geographically) limited network. It is not disputed that this resource or network is controlled by the Defendants. When disabling is done by the Platforms on their own, in terms of their policies, the same is global. So, there is no reason as to why court orders ought not to be global. All offending material which has therefore, been uploaded from within India on to the Defendants‟ computer resource or computer network would have to be disabled and blocked on a global basis.").

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

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

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

further logistics is limited to 67%, provided that each of these services is not ancillary to the main business line. Reports suggest that Indonesia might ease these foreign ownership caps within the next year.[278]

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates

Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transaction imposed a localization regime for Indonesia.[279] Industry reports that the regime pursuant to this regulation is a significant barrier for digital trade and inhibits foreign firms' participation in Indonesia's financial services sector. There have been recent positive steps to reform its regime, including clarifications with respect to a data classification policy.[280] However, industry still reports a lack of clarity and no clear commitments to when the financial sector can store and process certain data offshore.

Market-Based Platform Regulation

In previous submissions, CCIA has identified Indonesia's developing legislation on regulation of over-the-top (OTT) services.[281] Industry reports that negotiations continue on this draft legislation and it has since evolved into a "digital platform" regulation. The regulation seeks to bolster domestic competitors in the platform space and may include requirements for foreign services to register locally, submit to content screening, and enable law enforcement access on their services, among other regulations.

Backdoor Access to Secure Technologies

Indonesia established a new cybersecurity agency in 2018 – the National Cyber and Encryption Agency – and is expect to move forward with Cybersecurity Legislation later this year. Industry has significant concerns with the draft legislation and regulatory proposal with respect to provisions on law enforcement access to data and the broad authority granted to the

[278] *Indonesia to Ease Foreign Ownership Caps*, BUSINESS TIMES (Aug. 16, 2019), https://www.businesstimes.com.sg/government-economy/indonesia-to-ease-foreign-ownership-caps.

[279] General Data Localization Requirements in Indonesia, BAKER MCKENZIE (July 2018), https://www.bakermckenzie.com/-/media/files/insight/publications/2018/07/al_generaldatalocalizationrequirements_july2018.pdf?la=en.

[280] *Indonesia – Changes to Data Localization Provisions for Electronic System Operator*, BAKER MCKENZIE (April 2018), https://www.lexology.com/library/detail.aspx?g=a3b371a0-1b95-4ebc-86a1-2cbcda491eda.

[281] *CCIA 2018 NTE Comments*, *supra* note 38, at 62-63.

new Agency.[282] The planned approach appears to follow authoritarian cybersecurity models such as those of China and Russia.

19. Italy

Copyright Liability Regimes for Online Intermediaries

CCIA continues to have concerns regarding Italy's copyright enforcement framework as it applies to online intermediaries. Since 2014, the Italian Communications Authority (AGCOM) has had the authority to order the removal of allegedly infringing content and block domains at the ISP level upon notice by rightsholders, independent of judicial process. In March 2017, the Regional Administrative Court of Lazio upheld AGCOM's authority to grant injunctions without a court order.[283]

Digital Taxation

Italy's 2019 Budget included a 3% digital services tax closely aligned with the EU's original proposal. The tax is expected to predominantly affect U.S. firms, as senior government officials, including Former Deputy Prime Minister Luigi Di Maio, directed that prior iterations of the tax be gerrymandered around large U.S. tech firms.[284] The new Italian government has also included the digital tax in its priorities.[285] The implementation of the tax is merely administrative and could happen at any moment. Italian Finance Minister Roberto Gualiteri recently indicated that the DST will take effect on January 1, 2020.[286]

---

[282] *See Indonesia Needs to Fix 'Authorities' Clauses in Bill on Cyber Security Before Passing it Into Law*, The Conversation (Sept. 4, 2019), http://theconversation.com/indonesia-needs-to-fix-authoritarian-clauses-in-bill-on-cyber-security-before-passing-it-into-law-122342 (providing an overview of the draft legislation and background of the process).

[283] *See* Gianluca Campus, *Italian Public Enforcement on Online Copyright Infringements*, KLUWER COPYRIGHT BLOG (June 16, 2017), http://copyrightblog.kluweriplaw.com/2017/06/16/italian-publicenforcementonline-copyright-infringements-agcom-regulation-held-valid-regional-administrative-court-lazio-stillroom-cjeu/.

[284] *Web Tax in Arrivo*, ADNKRONOS (Dec. 19, 2018), https://www.adnkronos.com/soldi/economia/2018/12/19/web-tax-arrivodi-maio-rassicura-solo-per-giganti-rete_JEfFksy3wkwzPPJaG7vxuI.html.

[285] *M5S Members Vote Overwhelmingly In Favour of Italy Coalition*, THE GUARDIAN (Sept. 3, 2019), https://www.theguardian.com/world/2019/sep/03/m5s-members-vote-overwhelmingly-in-favour-italy-coalition ("The programme also called for a web tax on multinationals and the creation of a public bank to help boost development in the south.").

[286] *Italy, Austria Push Ahead with Digital Taxes*, TAX NOTES (Oct. 11, 2019), https://www.taxnotes.com/tax-notes-today-international/digital-economy/italy-austria-push-ahead-unilateral-digital-taxes/2019/10/11/2b12s.

20. Japan

Market-based Platform Regulation

Following the EU's pursuit of sector-specific regulations regarding "platforms", a number of Japanese regulatory agencies have conducted studies on potential regulatory frameworks for the platform economy.[287] Early reports from the joint working groups reiterated some concerning tropes on data access and competition. In October, the Japan Fair Trade Commission (JFTC) released for public comment its proposed merger guidelines to address the challenges raised by digital platforms.[288] Industry is closely following these developments.

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates

The Japanese Ministry of Communications is considering changes to the Telecommunications Business Act (TBA) to extend notification and other requirements extraterritorially. Industry reports that these changes are expected to oblige foreign over-the-top (OTT) services using third-party facilitates (potentially including search, digital ads, and other services that intermediate two-party communications) to (1) assign a local representative to notify and register as a service provider, and (2) observe TBA obligations.[289] A bill is expected to be submitted in January 2020 in the next Diet.

The TBA changes threaten to prevent online service providers from using metadata and other content that is indispensable to the operation of different communications services. These requirements may also be in violation of GATS Article XVII, National Treatment requirements in Chapter 2 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), and prohibitions on local presence requirements under Article 14.13 of the CPTPP.[290]

---

[287] *Japan Likely to Seek More Transparency on Digital Platform Businesses,* WHITE & CASE (2019), https://www.whitecase.com/publications/alert/japan-likely-seek-more-transparency-digital-platform-businesses.

[288] JAPAN FAIR TRADE COMMISSION, Request for Public Comments on the revised "Guidelines for Application of the Antimonopoly Act Concerning Review of Business Combination" (draft) and the revised "Policies Concerning Procedures of Review of Business Combination", Oct. 4, 2019, https://www.jftc.go.jp/en/pressreleases/yearly-2019/October/191004.html.

[289] Obligations contemplated under these regulations include protecting the "secrecy of communications" (TBA Article 4), "duty to inform suspension/abolishment of telecom services to users," (TBA Article 26-4), and "duty to report to MIC unexpected disruption of telecom services" (TBA Article 28).

[290] GATS: 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); Final Text of Comprehensive and Progressive Agreement for Trans-Pacific Partnership, signed Mar. 8, 2018, https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf.

In light of the recent U.S.-Japan Digital Trade Agreement, it is unfortunate that Japan is pursuing a policy that is inconsistent with the promotion of cross-border data flows.

21. Republic of Korea

Extraterritorial Regulations and Judgments

On September 23, 2016, 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.[291] 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 law forces these firms to adjust the way they operate both in South Korea and globally.

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates

Localization measures continue to be a concern for exporters to South Korea.[292] 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. Proposed legislation 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."[293] Korea is further obligated under KORUS

---

[291] *South Korea Enacts Stricter Penalties for Data Protection Violations by Telecommunications and Online Service Providers*, SIDLEY AUSTIN DATA MATTERS (Apr. 22, 2016), http://datamatters.sidley.com/south-korea-enacts-stricter-penalties-for-data-protection-violationsby-telecommunications-and-online-services-providers/.

[292] *See South Korean Data Localization: Shaped By Conflict*, University of Washington School of International Studies (Feb. 28, 2018), https://jsis.washington.edu/news/south-korean-data-localization-shaped-conflict/.

[293] 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

Art. 15.8 to "refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[294]

Government-Imposed Content Restrictions and Related Access Barriers

New rules announced by the Korean Communications Commission will enable officials to filter online content and block websites based outside the country.[295] While in the pursuit of enforcing existing laws regarding illegal content, some have raised concern that it follows authoritarian models of Internet regulation.[296]

Additional E-Commerce Barriers

Korean regulators have focused resources on studying the concept of "reverse discrimination".[297] The Korea Fair Trade Commission (KFTC) is attempting to address alleged competition concerns through increases in network usage fees.[298] The KFTC initiated a study on this issue and is currently reviewing to determine whether regulation to increase network usage fees for global providers is warranted. This concept is also influencing taxation discussions. The

[294] 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.

[295] Press Release, Korean Communications Commission, 방통위, 불법정보를 유통하는 해외 인터넷사이트 차단 강화로 피해구제 확대 ["KCC Expands Relief Measures by Strengthening Blocking of Overseas Internet Sites that Distribute Illegal Information"], https://kcc.go.kr/user.do?mode=view&page=A05030000&dc=K05030000&boardId=1113&cp=1&boardSeq=46820

[296] *Analysis: South Korea's New Tool for Filtering Illegal Internet Content*, NEW AMERICA (Mar. 15, 2019), https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/analysis-south-koreas-sni-monitoring/; *Is South Korea Sliding Toward Digital Dictatorship?* FORBES (Feb. 25, 2019), https://www.forbes.com/sites/davidvolodzko/2019/02/25/is-south-korea-sliding-toward-digital-dictatorship/#1567e3a648e2.

[297] The term originated in 2017 pursuant to a taskforce study that examined whether local firms were at a disadvantage to compete with international firms due to disparate regulations, and is largely driven by a domestic competitor. The taskforce included the Ministry of Science, ICT and Future Planning, the Korea Communications Commission (KCC), Korea Fair Trade Commission, Ministry of Strategy and Finance, National Tax Service, and the Financial Services Commission. *See Naver, Google Clash over Reverse Discrimination against Domestic Firms*, BUSINESS KOREA (Nov. 3, 2017), http://www.businesskorea.co.kr/news/articleView.html?idxno=19703; *S. Korea Moves to Strengthen Regulation of Facebook, Google, Netflix*, INQUIRER.NET (Sept. 11, 2018), https://technology.inquirer.net/79232/s-korea-moves-strengthen-regulation-facebook-google-netflix ("A group of lawmakers have set out to strengthen the regulation of foreign internet companies operating here, responding to complaints that they are not bound by the same laws that apply to competing South Korean firms in the sector. Led by Rep Byun Jae-il of the ruling Democratic Party of Korea, 10 lawmakers recently proposed four bills aimed at "creating a level playing ground" and resolving the "reverse discrimination" problem in Korea's information and communication technology sector.").

[298] *Korea Technology Sector Legal Developments*, LEXOLOGY (Aug. 22, 2019), https://www.lexology.com/library/detail.aspx?g=23f55ced-3141-437d-bc1d-43f0ff9efd84.

Korean government reportedly is considering introducing a digital tax, coined as a "YouTube tax" on OTT media services.[299]

Industry also reports concerns over networking charges and the rising costs of Internet bandwidth each year in Korea.[300] The Korean Ministry of Science and ICT issued Guidelines on interconnection in 2016, which aimed to serve as a price cap for the rate charged by ISPs for Internet traffic. However, the three leading ISPs increased their rate to the highest permitted level.

Cloud services also report a number of protectionist barriers in Korea. In 2016, the Korea Internet and Security Agency created a new cloud security certification system for offering cloud services to the public sector. Industry reports that it is difficult to meet the components of the certification scheme and many are prevented from accessing the market.[301] It is recommended that this certification scheme be revised to allow Korean public sector institutions to adopt global cloud services.

22. Mexico

Digital Taxation

In 2019, a bill was proposed to amend existing national legal frameworks on taxation to capture U.S. Internet services.[302] The bill would amend the VAT rules to extend the scope of taxpayers to foreign companies that "provide services as intermediaries through technological platforms for electronic commerce purposes."[303] The bill would also amend the income tax laws to require foreign companies that "provide services through a technological platform to provider goods and services" to register a tax domicile in Mexico, making the entity subject to Mexican corporate income tax even if they do not have a taxable presence in Mexico currently.[304]

---

[299] *Tax Chiefs in Asia to Discuss Digital Tax*, YONHAP NEWS (Oct. 23, 2019), rhttps://en.yna.co.kr/view/AEN20191023006700320; *South Korea Government Considering Introducing YouTube Tax*, Business Korea (Aug. 16, 2019), http://www.businesskorea.co.kr/news/articleView.html?idxno=34967.

[300] *Google and Naver Call for Network Free System Improvement*, BUSINESS KOREA (Aug. 27, 2019), http://www.businesskorea.co.kr/news/articleView.html?idxno=35341.

[301] These components for certification include: (1) physical separation (including physical resources, access control systems, human resource support), (2) common criteria certification, (3) vulnerability scanning and penetration testing, and (4) use of local encryption algorithms.

[302] *Mexico Proposes New Rules to Tax Highly Digitalized Business*, MNE TAX (Sept. 2, 2019), https://mnetax.com/mexico-proposes-new-rules-to-tax-highly-digitalized-businesses-35519.

[303] *Id*.

[304] *Id*.

Additional E-Commerce Barriers

In 2018, Mexico passed a number of regulations including one that lowered the *de minimis* threshold for low-value postal imports from USD $300 to USD $50.[305] As of March 1, 2019, import taxes apply to goods with a declared value exceeding $50.[306]

23. New Zealand

Digital Taxation

New Zealand has indicated that it will move forward with a national digital services tax. In June, the Government released a discussion document outlining two options: (1) to apply a separate digital services tax to certain digital transactions, or (2) to change international income tax rules at the OECD.[307] The first option, the national DST, would be a 3% tax on gross turnover attributable to New Zealand of certain digital businesses. The businesses in scope include intermediation platforms, social media platforms, content sharing sites, search engines and sellers of user data. U.S. firms are specified throughout the discussion document of firms in the scope of the proposed tax. As with other DSTs, the tax may conflict with WTO commitments and, as proposed, could be considered a 'covered tax' under various double taxation treaties, including the agreement with the United States.

24. Pakistan

Government-Imposed Content Restrictions and Related Access Barriers

Pakistan continues to intermittently block Twitter, YouTube, and Facebook,[308] and social media sites are also routinely asked by the government to censor material deemed "blasphemous".[309] The popular blog platform WordPress was also temporarily blocked for several days in 2015 with little explanation from authorities. These blocks cost the local GDP an

[305] *Mexico to Lower De Minimis Threshold for Postal Shipments Effective March 1* (Jan. 29, 2019), http://economists-pick-research.hktdc.com/business-news/article/Regulatory-Alert-US/Mexico-to-Lower-De-Minimis-Threshold-for-Postal-Shipments-Effective-1-March/baus/en/1/1X000000/1X0AGE0U.htm.

[306] Country Conditions for Mailing-Mexico, USPA, https://pe.usps.com/text/imm/mo_012.htm (last visited Oct. 31, 2019).

[307] Options for Taxing the Digital Economy: A Government Discussion Document (2019), *available at* http://taxpolicy.ird.govt.nz/sites/default/files/2019-dd-digital-economy.pdf [New Zealand].

[308] *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.

[309] *PTA Asks Govt to Block Social Media Websites to Curb Blasphemous Content,* PAKISTAN TODAY (July 26, 2019), https://www.pakistantoday.com.pk/2019/07/26/pta-asks-govt-to-block-social-media-websites-to-curb-blasphemous-content/.

estimated $69 million dollars in 2017.[310] Passed in August 2016, the Prevention of Electronic Crimes Act also introduced stronger censorship powers for authorities.[311]

25. Peru

Copyright Liability Regimes for Online Intermediaries

Peru remains out of compliance with key provisions under the U.S.-Peru Trade Promotion Agreement (PTPA). Article 16.11, para. 29 of the PTPA requires certain protections for online intermediaries against copyright infringement claims arising out of user activities. USTR cited this discrepancy in its inclusion of Peru in the 2018 Special 301 report, and CCIA supports its inclusion in the 2020 NTE Report. CCIA urges USTR to engage with Peru and push for full implementation of the trade agreement and establish intermediary protections within the parameters of the PTPA.

26. Russia

Government-Imposed Content Restrictions and Related Access Barriers

In May, the Russian government enacted legislation that will extend Russia's authoritarian control of the Internet by taking steps to create a local Internet infrastructure. The new law will permit Russia to establish an alternative domain name system for Russia, disconnecting itself from the World Wide Web and centralizing control of all Internet traffic within the country.[312]

In March 2019, Russia passed two laws aimed at eliminating "fake news". The laws, *Federal Law on Amending Article 15-3 of the Federal Law on Information, Information Technologies and Protection of Information*[313] and the *Federal Law on Amending the Code of Administrative Violations*,[314] establish penalties for "knowingly spreading fake news" and established a framework for ISPs to block access to websites deemed to be spreading "fake news."[315]

---

[310] Darrell M. West, Internet Shutdowns, *supra* note 35, at 3.

[311] Freedom on the Net 2018 Country Profile: Pakistan (2018), https://freedomhouse.org/report/freedom-net/2018/pakistan (last visited Oct. 31, 2019).

[312] *Putin Signs 'Russian Internet Law' to Disconnect Russia From the World Wide Web*, FORBES (May 2, 2019), https://www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnect-the-country-from-the-world-wide-web/#1da8356c1bf1.

[313] *Available at* http://publication.pravo.gov.ru/Document/View/0001201903180031 [Russian].

[314] *Available at* http://publication.pravo.gov.ru/Document/View/0001201903180021 [Russian].

[315] LIBRARY OF CONGRESS LEGAL MONITOR, *Russia: Russian President Signs Anti-fake News Laws* (Apr. 11, 2019) http://www.loc.gov/law/foreign-news/article/russia-russian-president-signs-anti-fake-news-laws/.

Copyright Liability Regimes for Online Intermediaries

In 2017, Russia extended its strict copyright enforcement rules under the "Mirrors Law".[316] The new scheme requires search providers to delist website links within 24 hours of a removal request, including for so-called "mirror" websites that are "confusingly similar" to a previously blocked website.[317] The law came into effect on October 1, 2017.

Legislation has also been proposed this year that would order hosting providers to block "pirate sites" extrajudicially.[318]

27. Saudi Arabia

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates

The Communications and Information Technology Council of Saudi Arabia (CITC) issued the Cloud Computing Regulatory Framework in 2018.[319] 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 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.

Additional E-Commerce Barriers

In 2018, Saudi Arabia began enforcing a new product compliance regulation that imposes import barriers to the Saudi market.[320] The new regulations impose several additional requirements on international shipments, including registration requirements, additional documentation that must be uploaded to online portals,[321] obtaining prior authorization for

[316] 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.

[317] *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.

[318] *Russia Plans to Block Pirate Sites Without Trial & De-Anonymize Their Operators*, TORRENTFREAK (Mar. 15, 2019), https://torrentfreak.com/russia-plans-to-block-pirate-sites-without-trial-de-anonymize-operators-190315/.

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

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

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

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.[322]

28. Singapore

Government-Imposed Content Restrictions and Related Access Barriers

Two proposed bills were introduced this year, following hearings and a comprehensive report, targeted at combating misinformation online that would take unprecedented steps to regulate content online. The bills — *Protection from Online Falsehoods and Manipulation Bill*[323] and *Protection from Harassment (Amendment) Bill*[324] — require online services to remove content or carry 'corrections' on their platforms in response to claims from the government or from individuals that content is false or misleading.[325] These bills place too much power to determine falsehoods in the hands of the government without adequate and timely oversight processes, particularly by the judiciary. Instead of enhancing trust online, they could spread more misinformation while restricting platforms' ability to continue to address misinformation issues. The proposals also threaten to undermine security and privacy.[326]

The Protection from Online Falsehoods and Manipulation Bill was passed in Parliament on May 8, 2019, assented to by the President on June 3, and published on June 25 in national law. The law became effective starting on October 2.[327]

---

[322] 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.

[323] Bill No. 10/2019, Protection from Online Falsehoods and Manipulation Bill, *available at* https://www.parliament.gov.sg/docs/default-source/default-document-library/protection-from-online-falsehoods-and-manipulation-bill10-2019.pdf.

[324] Bill No. 11/2019, Protection from Harassment (Amendment) Bill, *available at https://www.parliament.gov.sg/docs/default-source/default-document-library/protection-from-harassment-(amendment)-bill11-2019.pdf*.

[325] *See* Rachael Stelly, *Singapore's Dangerous Response to Combating Misinformation Online*, DISRUPTIVE COMPETITION PROJECT (Apr. 25, 2019), http://www.project-disco.org/21st-century-trade/042519-singapores-dangerous-response-combating-misinformation-online/.

[326] *This 'Fake News' Law Threatens Free Speech. But It Doesn't Stop There*, N.Y. TIMES (May 30, 2019), https://www.nytimes.com/2019/05/30/opinion/hate-speech-law-singapore.html.

[327] Republic of Singapore, Protection from Online Falsehoods and Manipulation Act 2019, published on June 25, 2019, https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625.

29. Spain

Digital Taxation

A digital services tax of 3%, closely modeled after the abandoned EU proposal, was included in Spain's budget bill for 2019. Following the G7 Finance Ministers meeting in July, Spanish officials indicated the intention to start deliberations on the digital tax bill "as soon as there is a government."[328] Elections will take place in November 2019, and candidates running for the elections across the political spectrum have expressed the need to adopt fiscal changes to address the digital economy.

30. Sweden

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates

Industry reports that use of U.S. cloud service providers has decreased in recent months in Sweden. This is due to the uncertainty surrounding the use of U.S. cloud services and the impact of the U.S. CLOUD Act. In October 2018, eSamverkansprogrammet, a quasi-government organization, published an opinion that concluded, due to the U.S. CLOUD Act requirements, use of these services would conflict with EU and Swedish law.[329] Industry encourages the Swedish government to issues a clarification that public sector bodies are not prohibited from using U.S. cloud services under existing law.

31. Switzerland

Imbalanced Copyright Laws and "Link Taxes"

The Swiss government has been negotiating a copyright reform package. However, in February a proposal was tabled from the Science, Education and Culture Committee of the Council of States (SECC-S) that would introduce a press publishers' right that goes beyond what is envisioned in the EU Copyright Directive. According to SECC-S amendments, this new right would provide both a remuneration right to journalists and a right to media companies to make available content, explicitly not protected by copyright, for 10 years.[330] The amendments were reconsidered in April, and the SECC-S declined to pursue the amendments further. However, it

---

[328] *Spain to Push Ahead with Tax on American Tech Giants*, THE LOCAL ES (July 18, 2019), https://www.thelocal.es/20190718/spain-to-push-ahead-with-tax-on-american-tech-giants.

[329] *See* AmCham Sweden, *The Cloud Act: Its Meaning and Consequences* (June 17, 2019), https://www.amcham.se/newsarchive/2019/6/17/the-cloud-act-amp-its-implications-for-business.

[330] Parliamentary Deliberation, Revisions to Copyright Law, Swiss Federal Institute of Intellectual Property, https://www.ige.ch/en/law-and-policy/national-ip-law/copyright-law/revision-to-copyright-law/parliamentarydeliberations.html#c63032/.

did "recommend that the Federal Council examine the effectiveness of the revision with regard to copyright law developments within the EU" which should "include and pay special attention to the experiences of press publishers concerning the recently adopted related rights within the EU."[331]

32. Thailand

Government-Imposed Content Restrictions and Related Access Barriers

In December 2016, Thailand's National Legislative Assembly passed amendments to the 2007 Computer Crime Act.[332] 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.[333] 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.[334]

In 2019, Thailand passed a controversial Cybersecurity Law following amendments in 2018. Industry has criticized the law due to provisions that enable government surveillance.[335] Under the new law, officials are granted authority to "search and seize data and equipment in cases that are deemed issues of national emergency."[336] This could "enable internet traffic monitoring and access to private data, including communications, without a court order."[337]

---

[331] Parliamentary Deliberation, Revisions to Copyright Law, Swiss Federal Institute of Intellectual Property, https://www.ige.ch/en/law-and-policy/national-ip-law/copyright-law/revision-to-copyright-law/parliamentary-deliberations.html#c66169 (last visited Oct. 31, 2019).

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

[333] *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/fiveministerial-notifications/

[334] 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 significantly impacts 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/freedomnet/2017/thailand.

[335] *See* Asia Internet Coalition Statement, Feb. 28, 2019, https://aicasia.org/wp-content/uploads/2019/03/AIC-Statement_Thailand-Cybersecurity-Law_28-Feb-2019.pdf ("Protecting online security is a top priority, however the Law's ambiguously defined scope, vague language and lack of safeguards raises serious privacy concerns for both individuals and businesses, especially provisions that allow overreaching authority to search and seize data and electronic equipment without proper legal oversight. This would give the regime sweeping powers to monitor online traffic in the name of an emergency or as a preventive measure, potentially compromising private and corporate data.").

[336] *Thailand Passes Controversial Cybersecurity Law*, TECHCRUNCH (Feb. 28, 2019), https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/.

[337] *Id*.

33. Turkey

Government-Imposed Content Restrictions and Related Access Barriers

Turkey remains one of the most restrictive markets for Internet services.[338] CCIA has previously identified laws that preemptively block websites on vague grounds, and specific instances of blocking by Turkish authorities.[339] 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.[340]

Continued unrest in Syria has led to further government censorship from Turkey, with Turkish authorities censoring websites and Twitter accounts accused of spreading Kurdish propaganda, including journalism sites. During 2018 elections, Turkish authorities utilized a "rapid response team" to block "abnormal" content on social media and online platforms.[341] In 2019, regulations were passed that will increase regulatory oversight and censorship of news content delivered online.[342] The scope is broad, and expected to apply to a variety of online services.[343]

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates

On July 6, 2019, the Presidential Circular on Information and Communication Security Measures No. 2019/12 was published and introduces important security measures and obligations. Article 3 prohibits public institutions and organizations' data from being stored in

---

[338] Freedom on the Net 2018 Country Report: Turkey (2018), https://freedomhouse.org/report/freedom-net/2018/turkey (last visited Oct. 31, 2019).

[339] *CCIA 2018 NTE Comments*, *supra* note 38, at 74; *see 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; *Google, Others Blast Turkey Over Internet Clampdown*, WALL ST. J. (Apr. 1, 2014), http://online.wsj.com/articles/SB10001424052702303978304579473190997035788; *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/. *See also* Internet Access Disruption in Turkey 2016, https://labs.ripe.net/Members/emileaben/internet-access-disruption-in-turkey.

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

[341] *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-blockingjune-elections/.

[342] *Turkey Publishes Draft Regulation Regarding RTÜK Supervision of Internet Content*, BAKER MCKENZIE (Oct. 11, 2018), https://www.lexology.com/library/detail.aspx?g=f1baa621-528e-4f95-9489-c52b1bc13f53.

[343] *Censorship Feared Under Turkey's New Rules for Online Broadcasts*, VOICE OF AMERICA (Aug. 3, 2019), https://www.voanews.com/press-freedom/censorship-feared-under-turkeys-new-rules-online-broadcasts.

cloud storage services that are not under the control of public institutions. The Circular also requires that critical information[344] and sensitive data[345] be stored domestically. Draft regulation is expected that will also mandate localization of data produces by banks and financial services.[346]

Digital Services Tax

Industry reports that the Ministry of Finance and Treasury is planning to introduce a digital services tax of 7.5% to Parliament in 2019. The tax would apply to all companies that lack a permanent establishment in Turkey, but that provide services through the Internet. The proposed tax is expected to apply to the revenue of a wide range of digital services and officials are not expected to wait for OECD negotiations to conclude before enacted this tax.

34. Uganda

In 2018, the Ugandan government began collecting tax on over-the-top (OTT) services in 2018 which was expected to have a negative impact on local Internet services.[347] 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, 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. As predicted,[348] the tax has been shown to be detrimental to users and Internet access.[349]

---

[344] This will be defined by the Digital Transformation Office.

[345] Sensitive data includes health and communication regulation information and genetic and biometric data.

[346] The *Draft Regulation on the Information System of Banks and Electronic Banking Services* is being prepared by the Banking Regulation and Supervision Agency and is in final stages of review.

[347] *Uganda Imposes Tax on Social Media Use*, REUTERS (May 31, 2018), https://www.reuters.com/article/us-uganda-internet/uganda-imposes-tax-on-social-media-use-idUSKCN1IW2IK.

[348] *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-investmentexecutives-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.").

[349] *Uganda's Social Media Tax Has Led to a Drop in Internet and Mobile Money Users*, QUARTZ (Feb. 19, 2019), https://qz.com/africa/1553468/uganda-social-media-tax-decrease-internet-users-revenues/ ("the Uganda Communications Commission noted internet subscription declined by more than 2.5 million users, while the sum of taxpayers from over-the-top (OTT) media services decreased by more than 1.2 million users. The value of mobile money transactions also fell by 4.5 trillion Ugandan shillings ($1.2 million).").

35. 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.[350] 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.[351] 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. 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 and parallel FTA provisions. USTR noted the obligations and responsibilities are too ambiguous and onerous in the 2018 NTE[352] and CCIA encourages USTR to include these concerns in the 2020 NTE.

36. United Arab Emirates

The UAE's main telecommunications providers, Etisalat and du, began blocking the majority of OTT video and messaging services in 2017.[353] This discriminatory practice provides telecommunications providers an unfair competitive advantage as it allows them to restrict

---

[350] *2019 NTE Report*, *supra* note 14.

[351] 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).

[352] USTR, National Trade Estimates Report (2018), *available at* https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf at 472-3 ("Although the adoption of the Law on Cinematography in March 2017 was a sign of progress in the fight against rampant online piracy in Ukraine, the legislation has some shortcomings — for example, some stakeholders report that obligations and responsibilities are too ambiguous or too onerous to facilitate an efficient and effective response to online piracy and the law does not apply to literary or photographic works — and it has not yet demonstrated effectiveness.").

[353] A longer discussion of industry concerns with the rise of OTT regulation (referred to as regulation on "rich interaction applications" or "RIAs") is included in CCIA's previous NTE comments. *CCIA 2018 NTE Comments*, *supra* note 38, at 16-17.

access to new and innovative technologies.[354] USTR should encourage the UAE regulators to consider revising its regulatory framework to prevent the operators from blocking such services.

37. United Kingdom

As the U.S. looks to negotiate with the UK following its exit from the EU, it should consider a number of regulations and policies that deter U.S. digital exports.[355]

Government-Imposed Content Restrictions and Related Access Barriers

In April, the UK government presented the Online Harms White Paper ("White Paper") to Parliament that outlines an unprecedented approach to regulating content online.[356] The White Paper is incredibly wide-ranging, and includes a number of untested ideas. The "online harms" these new policies would target include both lawful and unlawful content, including everything from "serious violent" content to "interference with legal proceedings" and "inappropriate" content accessed by children.[357] The proposal not only has trade implications, but also free expression concerns, to the extent these rules would conflict with U.S. law. It also anticipates placing burdens on small businesses.[358] While it's suggested that the new regulatory regime would assist startups and SMEs in fulfilling their obligations under the new rules, and emphasizes the need for proportionality, the measures contemplated in the White Paper are significant and it is unclear whether the substantial burden will be offset by this assistance. The

[354] Freedom on the Net 2018 Country Report: UAE, https://freedomhouse.org/report/freedom-net/2018/united-arab-emirates (last visited Oct. 31, 2019) ("Most popular Voice-over-Internet-Protocol (VoIP) services are restricted over mobile connections. Etisalat and Du are the only operators licensed to provide paid VoIP services, while the free or low-cost over-the-top (OTT) voice calls services provided by WhatsApp, Skype, and others are only accessible through fixed-line or Wi-Fi connections. WhatsApp's voice feature was blocked shortly after it was introduced in March 2015, as was a similar feature offered by Facebook. Viber has been banned since 2013, along with FaceTime, a feature provided by Apple; in fact, Apple agreed to sell its iPhone products to UAE mobile phone companies without the Facetime application preinstalled, though FaceTime can be used on phones purchased outside the country. Discord, a chatting app used by gamers, had its VoIP feature blocked in March 2016; Snapchat voice servicers were blocked in 2016.").

[355] *See also* Comments of CCIA In Re Request for Comments and Notice of a Public Hearing on Negotiating Objectives for a U.S.-United Kingdom Trade Agreement, Docket No. USTR 2018-0036, filed Jan. 15, 2019, *available at* http://www.ccianet.org/wp-content/uploads/2019/01/CCIA-Comments-on-U.S.-UK-Trade-Priorities.pdf; Comments of CCIA In Re U.S. SME Exports: Trade Related Barriers Affecting Exports of U.S. Small- and Medium-Sized Enterprises to the United Kingdom, Investigation No. 332-569, filed Apr. 30, 2019, *available at* http://www.ccianet.org/wp-content/uploads/2019/05/CCIA-Comments-to-ITC-UK-SME-Trade-Barriers.pdf.

[356] SEC. OF STATE FOR DIGITAL, CULTURE, MEDIA & SPORT, AND THE SEC. OF STATE FOR THE HOME DEP'T, Online Harms White Paper (Apr. 2019), [hereinafter "Online Harms White Paper"], *available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

[357] *Online Harms White Paper* at 75-76.

[358] *Online Harms White Paper* at 49.

White Paper also presents vague and untested ideas regarding "duty of care". For example, it is suggested that platforms would have to determine 'foreseeable' harm and act accordingly. The penalties contemplated are concerning and include "disruption of business activities" that would allow the regulator to force other online services to block the targeted companies' availability or presence online, ISP blocking, and senior management liability extending to criminal liability.[359] Draft legislation for pre-legislative scrutiny is expected in the new Parliament.[360] The UK Office of Communications also released a report on regulating online platforms to address online harms.[361]

Digital Services Tax

The UK government announced it would introduce a new DST in April 2020, following a public consultation launched last November.[362] The tax was included in the Finance Bill 2019-20 presented on July 11.[363] The UK's DST would be a 2% tax on the UK revenues of digital businesses that are considered to derive significant value from user participation. Activities in scope include social media platforms, Internet search engines, and online marketplaces. With the revenue threshold set at £500 million, the scope is limited to only a few leading U.S. firms offering these designated services: Facebook, Google, and Amazon. UK officials estimate these three companies would pay £30 million each under this tax. The 2019 draft legislation does not include a sunset provision, contrary to claims made by UK officials in 2018.[364] It is uncertain whether the next UK government will pursue an identical text. This recent action builds on a unilateral Diverted Profits Tax that the government publicly labeled the "Google Tax" when enacted in 2015. The U.S. could push back against the tax as part of a possible U.S.-UK free trade agreement following the UK's exit from the EU.

---

[359] *Online Harms White Paper* at 60.

[360] Queen's Speech and Associated Background Briefing On the Occasion of the Opening of Parliament on Monday 14 October 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/839370/Queen_s_Speech_Lobby_Pack_2019_.pdf, at 59.

[361] OFFICE OF COMMUNICATIONS, Online Market Failures and Harms – An Economic Perspective on the Challenges and Opportunities in Regulating Online Services (Oct. 28, 2019), *available at* https://www.ofcom.org.uk/__data/assets/pdf_file/0025/174634/online-market-failures-and-harms.pdf.

[362] HM REVENUE & CUSTOMS, Introduction of the New Digital Services Tax, July 11, 2019, https://www.gov.uk/government/publications/introduction-of-the-new-digital-services-tax.

[363] HM TREASURY, HM REVENUE & CUSTOMS, Finance Bill 2019-20, https://www.gov.uk/government/collections/finance-bill-2019-20.

[364] *EU, UK Officials Emphasize Sunset Provisions in Digital Tax Proposals*, WORLD TRADE ONLINE (Nov. 8, 2019), https://insidetrade.com/daily-news/eu-uk-officials-emphasize-sunset-provisions-digital-tax-proposals.

Backdoor Access to Secure Technologies

The UK has pursued policies that undermine secured communications by mandating law enforcement access to encrypted communications. Passed in 2016, the Investigatory Powers Act allows for authorities to require removal of "electronic protections" applied to communications data.[365] The UK also recently joined the United States and Australia in a concerning request to Facebook regarding undermining the security of user communications.[366]

Restrictions on Cross-Border Data Flows

The EU's General Data Protection Regulation (GDPR) went into effect last year, and was implemented into UK law under the Data Protection Act 2018. Since that time, some U.S. services have stopped operating in the EU over uncertainties regarding compliance.[367] If the UK intends to maintain GDPR compliance following Brexit, as expected pursuant to the EU Withdrawal Act (2018),[368] it is critical that there remain clear rules for U.S. exporters offering services in the UK. It is also critical that there remains a valid mechanism for companies to legally transfer the data of UK citizens following the UK's exit from the EU in the same manner as the U.S.-EU Privacy Shield.

Market Access Barriers for Communication Providers

Telecommunications services of all sizes rely on fair and transparent public procurement regimes. They also rely on consistent, pro-competitive regulation of business-grade whole access and nondiscrimination by major suppliers. For example, even in the United States there is no adequate regulation on bottlenecks in access layers, particularly in the business data service market. The UK market has seen greater competition, with regulation and legal separation requiring the main national operator to provide wholesale/leased access and treat all of its customers equally. Furthermore, the regulator is legally required to carry out detailed market

[365] See Investigatory Powers Act 2016, https://www.legislation.gov.uk/ukpga/2016/25.

[366] Press Release, CCIA Dismayed by AG Opposition to Stronger Consumer Encryption Options, Oct. 3, 2019, http://www.ccianet.org/2019/10/ccia-dismayed-by-ag-opposition-to-stronger-consumer-encryption-options/.

[367] *To Save Thousands on GDPR Compliance Some Companies Are Blocking All EU Users*, TECH REPUBLIC (May 7, 2018), https://www.techrepublic.com/article/to-save-thousands-on-gdpr-compliance-somecompanies-are-blocking-all-eu-users/; *US Small Businesses Drop EU Customers Over New Data Rule*, FT (May 24, 2018), https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04.

[368] DEPT. FOR DIGITAL, CULTURE, MEDIA & SPORT, Guidance, Amendments to UK Data Protection Law in Event the UK Leaves the EU Without a Deal (updated Apr. 23, 2019), https://www.gov.uk/government/publications/dataprotection-law-eu-exit/amendments-to-uk-data-protection-law-in-the-event-the-uk-leaves-the-eu-without-a-deal-on29-march-2019.

reviews regularly and to impose regulatory remedies where the biggest national operator is found to have significant market power.

38. Vietnam

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates

Vietnam remains a country of concern for industry as it continues to pursue localization measures. Last year the legislature approved a new Law on Cybersecurity that took effect January 1, 2019 (though there are reports that the government may grant extensions for compliance). The law is expansive and includes both data localization mandates and content regulations. Under the law, covered service providers are required to store personal data of Vietnamese end users, data created by users, and data regarding the relationships of a user within the country for a certain period of time.[369] There are also local representation requirements for services that meet designated criteria.

The Ministry of Public Security has since issued draft versions of the Implementing Decree that provide detailed requirements for covered services.[370] Industry reports that the latest drafts include requirements for all companies to comply with data requests, content takedown, and domain name seizures. As a penalty for noncompliance, authorities could then serve companies with a "data localization" notice by the Ministry of Public Security. The requirement for data access and content takedowns may not be practical for all types of firms in the scope of the regulation who may not have the necessary visibility into data stored on their platform. As a general matter of policy, governments should not use localization mandates as a penalty for non-compliance.

Government-Imposed Content Restrictions and Related Access Barriers

The Law on Cybersecurity also includes concerning provisions on content regulation, requiring online services to monitor user-generated content and remove "prohibited" content within 24 hours upon notification from government offices. It also establishes procedures for the service provider to both terminate access for a user posting "prohibited" content and share information regarding the user. "Prohibited" content includes content that is critical or

[369] *Update: Vietnam's New Cybersecurity Law*, HOGAN LOVELLS CHRONICLE OF DATA PROTECTION (Nov. 18, 2018), https://www.hldataprotection.com/2018/11/articles/international-eu-privacy/update-vietnams-new-cybersecurity-law/.

[370] See *Vietnam: Updates to Draft Decree Detailing Certain Articles of Law on Cybersecurity*, GLOBAL COMPLIANCE NEWS (Oct. 18, 2019), https://globalcompliancenews.com/vietnam-updates-draft-decree-detailing-certain-articles-law-cybersecurity-20191008/.

disparaging of the Vietnamese government. Companies have already been fined under this provision.[371]

The Authority of Broadcasting and Electronic Information issued a draft regulation ("Decree 6") that aims to regulate video on-demand services in the same manner as broadcast television, departing from global norms on video-on demand regulations.[372] The draft defines "on-demand" content broadly, and could include a variety of online content including content uploaded by users. Requirements envisioned as a result of these changes include licensing requirements, local content quotas, local presence mandates, and translation requirements.

[371] *Vietnam Says Facebook Violated Controversial Cybersecurity Law*, REUTERS (Jan. 8, 2019), https://www.reuters.com/article/us-vietnam-facebook/vietnam-says-facebook-violated-controversial-cybersecurity-law-idUSKCN1P30AJ; *Vietnam Quick to Enforce New Cybersecurity Law*, HOGAN LOVELLS CHRONICLE OF DATA PROTECTION (Mar. 6, 2019), https://www.hldataprotection.com/2019/03/articles/international-eu-privacy/vietnam-quick-to-enforce-new-cybersecurity-law/.

[372] *Vietnam to Amend Decree on Broadcasting and TV Services to Regulate On-Demand Content*, LEXOLOGY (Jan. 23, 2019), https://www.lexology.com/library/detail.aspx?g=fec93a51-ce3c-4e5f-885f-8dcd31d5fb90.

IV. CONCLUSION

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 continued focus on barriers to digital trade and recommends that this focus be reflected in this year's NTE.