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-2020-0034

COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION
REGARDING FOREIGN TRADE BARRIERS TO U.S. EXPORTS
FOR 2021 REPORTING

October 29, 2020

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 85 Fed. Reg. 55,925 (Sept. 10, 2020), the Computer & Communications Industry Association (CCIA) submits the following comments for consideration as USTR composes its annual National Trade Estimate Report on Foreign Trade Barriers (NTE).

CCIA welcomes USTR's continued focus and 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. Over recent months as countries are dealing with the COVID-19 pandemic, digital technologies have enabled regular business activities in cross-border communication.

These gains are facing growing threats from countries who continue to adopt regulations that hinder growth and cross-border delivery of Internet services. Under the guise of promoting domestic champions, countries are adopting discriminatory policies that disadvantage, and often target, U.S. technology companies including digital services taxes, localization mandates, and restrictions on foreign investment. This risks fragmentation of the global digital economy. As the Internet is essential to international commerce, it is essential that such barriers are identified and quelled.

For the 2021 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 barriers access for communications providers. Finally, CCIA highlights countries whose current and proposed regimes pose a threat to digital trade and negatively affect foreign investment by U.S. technology companies.

Table of Contents

I. INTRODUCTION 5

II. PROMINENT DIGITAL TRADE-RELATED BARRIERS 6
A. Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates 6
B. Government-Imposed Restrictions on Internet Content and Related Access Barriers 8
1. Online Content Regulations 8
2. Censorship and Internet Shutdowns 9
C. Digital Taxation 10
D. Market-Based Platform Regulation 12
E. Copyright Liability Regimes for Online Intermediaries 12
F. Imbalanced Copyright Laws and "Link Taxes" 13
G. Extraterritorial Regulations and Judgments 15
H. Customs Duties on Electronic Transmissions 15
I. Backdoor Access to Secure Technologies 16
J. Market Barriers Access for Communications Providers 17

III. COUNTRY-SPECIFIC CONCERNS 17
A. Argentina 17
B. Australia 19
C. Austria 21
D. Belgium 22
E. Brazil 23
F. Cambodia 25
G. Canada 25
H. Chile 26
I. China 26
J. Colombia 30
K. Czech Republic 31
L. European Union 31
M. Egypt 43
N. France 43
O. Germany 46
P. India 48
Q. Indonesia 51
R. Italy 55
S. Japan 55
T. Kenya 56
U. Korea 57
V. Mexico 58
W. New Zealand 60
X. Peru 60
Y. Russia 61
Z. Saudi Arabia 62
AA. Singapore 63
BB. Spain 64

CC. Sweden 64
DD. Taiwan 64
EE. Thailand 65
FF. Turkey 65
GG. Ukraine 67
HH. United Kingdom 67
II. Vietnam 70
IV. CONCLUSION 72

I. INTRODUCTION

The United States remains a world leader in high-tech innovation and Internet technologies — a central component of cross-border trade in goods and services in the 21st century. The removal of foreign obstacles to Internet-enabled international commerce and export of Internet-enabled products and services is thus critical to the growth of the American economy. Internet-enabled commerce represents a significant sector of the global economy.

Since 1998, the digital economy grew at an annual rate of 9.9 percent, compared to 2.3 percent overall economic growth.[1] According to U.S. Department of Commerce estimates, the digital economy accounted for 9.0 percent ($1,849.3 billion) of current-dollar gross domestic product (GDP) ($20,580.2 billion) in 2018.[2] Further, the digital economy supported 8.8 million jobs, which accounted for 5.7 percent of total U.S. employment (154.7 million jobs) in 2018.[3] The digital economy supported more jobs than the construction industry and the industry made up of "other" services, except in government.[4]

This is ever more apparent in difficult times such as these due to the ongoing global pandemic. Internet services around the world have enabled communications across borders, and enabled business activity to continue remotely.[5]

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.

Trading partners' pursuit of "technological sovereignty", with protectionist features, is an alarming trend U.S. Internet and technology services have encountered over the past year. Regulatory frameworks and policy agendas imposed as part of this pursuit threaten to undermine U.S. leadership in the digital economy and the global nature of the free and open Internet.

---

[1] BUREAU OF ECONOMIC ANALYSIS, *Measuring the Digital Economy: An Update Incorporating Data from the 2018 Comprehensive Update of the Industry Economic Accounts* (2019), 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.

[2] Jessica R. Nicholson, *New Digital Economy Estimates*, BUREAU OF ECONOMIC ANALYSIS (Aug. 25, 2020), https://www.bea.gov/system/files/2020-08/New-Digital-Economy-Estimates-August-2020.pdf.

[3] *Id.*

[4] *Id.*

[5] *See* Dan Primack, *Exclusive: Mary Meeker's coronavirus trends report*, AXIOS (Apr. 17, 2020), https://www.axios.com/mary-meeker-coronavirus-trends-report-0690fc96-294f-47e6-9c57-573f829a6d7c.html; Aamer Baig, *et al*., *The COVID-19 recovery will be digital: A plan for the first 90 days*, MCKINSEY DIGITAL (May 14, 2020), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-covid-19-recovery-will-be-digital-a-plan-for-the-first-90-days.

In its 2020 *Freedom on the Net* report, Freedom House highlighted the rising "allure of cyber sovereignty".[6] The report observed that it is no longer regimes such as China and Russia that are pursuing an isolationist and protectionist digital environment, but also regions such as the European Union seeking to draw up digital borders. This risks unprecedented fragmentation of the open Internet and delivery of digital services.

The United States should pursue a trade agenda and craft agreements that will reflect the needs of the 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 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.

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 2020 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.

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 those outlined in this section below, are also included in country profiles in Section III such as regulations on over-the-top (OTT) services and asymmetric competition policies pursued through market-based regulations.

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

Cross-border data flows are critical for continued global economic growth across industries. As CCIA has noted in previous NTE filings, countries continue to pursue data localization policies including mandated service localization and data storage. In a 2017 report, the U.S. International Trade Commission (USITC) includes estimates that localization measures have doubled in the previous six years.[7] Since that time, industry continues to see countries pursue policy and regulatory frameworks that restrict the free flow of information across borders.

Governments often cite domestic privacy protections, defense against foreign espionage, law enforcement access needs, and local development as motivations for restricting cross-border data flows and mandating localization. Many of these policies have instead had the effect of

[6] Adrian Shahbaz & Allie Funk, *Freedom on the Net 2020: The Pandemic's Digital Shadow*, FREEDOM HOUSE (Oct. 2020), https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow.

[7] 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*"].

inhibiting foreign competitors from entering markets, and in recent years there has been an increasingly protectionist angle to these regulations in the pursuit of achieving "technological sovereignty" from mainly U.S. services. Further, rather than ensuring user privacy or data security, forced localization creates a host of new targets of opportunity for criminals and foreign intelligence agencies.[8] 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. These measures also undermine 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.[9]

Rather than promote domestic industry, data localization policies are likely to hinder economic development and restrict domestic economic activity,[10] and impede global competitiveness.[11]

---

[8] 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.

[9] 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.

[10] *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), https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-notwhere ("[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), 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), http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf at 2 ("The impact of recently proposed or enacted legislation on GDP is substantial in all seven countries: Brazil (-0.2%), China (-1.1%), EU (-0.4%), India (-0.1%), Indonesia (-0.5%), Korea (-0.4%) and Vietnam (-1.7%). These changes significantly affect post-crisis economic recovery and can undo the productivity increases from major trade agreements, while economic growth is often instrumental to social stability. . . If these countries would also introduce economy-wide data localisation requirements that apply across all sectors of the economy, GDP losses would be even higher: Brazil (-0.8%), the EU (-1.1%), India (-0.8%), Indonesia (-0.7%), Korea (-1.1%)."); 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 the country's borders") (emphasis in original).

[11] 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?*, INFORMATION TECHNOLOGY & INFORMATION FOUNDATION (May 2017), https://itif.org/publications/2017/05/01/crossborder-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

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.[12] 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.[13]

Data localization policies and similar restrictions are increasingly used to advance domestic industries. For instance, the UN Conference on Trade and Development (UNCTAD) released a document in 2018, echoing arguments made by countries that have pursued strict data localization measures as a tool for local development.[14] More recently, industry has tracked initiatives in the EU to establish an EU-wide cloud that would localize data within EU borders.[15]

Continued opposition from the U.S. and likeminded allies is needed at the multilateral stage in light of these growing trends.[16]

B. Government-Imposed Restrictions on Internet Content and Related Access Barriers

1. 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.[17]

---

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.").

[12] Article 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).

[13] *See* Chander & Lê, Data Nationalism, *supra* note 8; 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*"].

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

[15] *Infra* p. 31.

[16] 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* (Oct. 2019), https://www.itic.org/dotAsset/f2de6c22-e286-47d2-aca7-ba34830e462c.pdf.

[17] *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), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism [hereinafter "*2018 Freedom on the Net Report*"] ("Like "terrorism," the term

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,[18] quickly detecting and removing terrorist and extremist content,[19] and working with brand owners and rightsholders to remove counterfeit products from their services.[20] 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 should utilize trade agreements in order to remedy the barriers these legal asymmetries create.

2. 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 observed in 2019, more governments are shutting down the Internet with disastrous consequences.[21] Internet shutdowns are also costly, with one study finding that

---

"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.").

[18] *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/tacklingmore-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-fightmisinformation-online/.

[19] *See* Global Internet Forum to Counter Terrorism, https://gifct.org/.

[20] 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, 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).

[21] *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*

countries lose $23.6 million (per 10 million in population) for every day that the Internet is shut down.[22] 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 blackouts at no less than $2.4 billion in one year.[23] 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.[24] 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.[25]

As CCIA has previously stated in its NTE comments, 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.

C. Digital Taxation

Since CCIA began raising concerns with digital services taxes (DSTs) in its NTE comments in 2018, an alarming number of countries have moved forward with unilateral measures to tax U.S. digital firms around the world. Most recently, the African Tax Administration Forum announced

---

Internet Shutdowns Around the World (2018), https://www.accessnow.org/cms/assets/uploads/2018/06/KeepItOn-Digital-Pamphlet.pdf.

[22] DELOITTE, The Economic Impact of Disruptions to Internet Connectivity, A Report for Facebook, at 6 (Oct. 2016), http://globalnetworkinitiative.org/wp-content/uploads/2016/10/GNI-The-Economic-Impact-of-Disruptions-to-Internet-Connectivity.pdf.

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

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

[25] 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/.

efforts to guide African countries' development of national digital tax measures.[26] These comments document key DST proposals or implemented measures, but may not include all discriminatory digital tax measures at time of filing.[27]

Often based on inaccurate estimates, some countries assert that digital services fail to pay adequate taxes and should be subject to additional taxation.[28] 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 investigations against countries that have announced or implemented DSTs.

In the United States, officials and lawmakers across the spectrum have made clear their disapproval of countries pursuing unilateral digital taxes that discriminate against U.S. firms.[29] DSTs also represent a significant departure from international taxation norms, and undermine the ongoing process to reach an international tax solution to the challenges associated with the

---

[26] Hamza Ali, *African Countries Prep Digital Tax Plans if OECD Talks Stall*, BLOOMBERG TAX (Sept. 30, 2020), https://news.bloombergtax.com/daily-tax-report-international/african-countries-prep-digital-tax-plans-if-oecd-talks-stall.

[27] The following countries have proposed or enacted direct taxes on digital services: Austria, Belgium, Brazil, Canada, Costa Rica, Czech Republic, France, Greece Hungary, India, Indonesia, Israel, Italy, Kenya, Latvia, Malaysia, Mexico, Nigeria, Pakistan, Paraguay, Poland, Slovakia, Spain, Taiwan, Thailand, Tunisia, Turkey, United Kingdom, Uruguay, Vietnam, and Zimbabwe. *See* KPMG, *Taxation of the Digitalized Economy Developments Summary* (July 10, 2020), https://tax.kpmg.us/content/dam/tax/en/pdfs/2020/digitalized-economy-taxationdevelopments-summary.pdf [hereinafter "*KPMG Digital Taxation Report*"]. Further, while structurally different from a DST or other direct taxes, industry is also aware of a rise in indirect taxes on digital services including VATs. *See* TAXAMO, *Global VAT/GST Rules on Cross-Border Digital Sales*, https://blog.taxamo.com/insights/vat-gst-rules-on-digital-sales.

[28] 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), http://ecipe.org/publications/digital-companies-and-their-fair-share-of-taxes/.

[29] *See, e.g.*, Press Release, Grassley, Wyden Joint Statement (June 18, 2020), https://www.finance.senate.gov/chairmans-news/grassley-wyden-joint-statement-on-oecd-digital-economy-tax-negotiations; LaHood, DelBene Letter to White House, June 19, 2019, https://lahood.house.gov/sites/lahood.house.gov/files/6.19.19_Digital%20Tax%20Letter_Signed.pdf; Press Release, Portland Questions Treasury Nominees About France Digital Services Tax (July 24, 2019), https://www.portman.senate.gov/newsroom/press-releases/hearing-portman-questions-treasury-nominees-about-frances-digital-services; *Pompeo Urges France Not to Approve Digital Services Tax*, REUTERS (Apr. 4, 2019), https://www.reuters.com/article/us-usa-france-tax/pompeo-urges-france-not-to-approve-digital-services-taxidUSKCN1RG1TZ; OFFICE OF U.S. TRADE REP., Digital Trade Fact Sheet 2020, https://ustr.gov/index.php/about-us/policy-offices/press-office/fact-sheets/2020/march/fact-sheet-2020-national-trade-estimate-strong-binding-rules-advance-digital-trade; U.S. DEP'T OF TREASURY, Press Release, Secretary Mnuchin Statement on Digital Economy Taxation Efforts (Oct. 25, 2018), https://home.treasury.gov/news/press-releases/sm534; Press Release, House Ways and Means, Senate Finance Leaders' Statement on Unilateral Digital Services Taxes, OECD Negotiations to Address the Tax Challenges of the Digitalization of the Economy (Apr. 10, 2019), https://gop-waysandmeans.house.gov/house-ways-and-means-senate-finance-leaders-statement-on-unilateral-digital-services-taxes-oecd-negotiations-to-address-the-tax-challenges-of-the-digitalization-of-the-economy/; Letter to White House, House Ways & Means Committee Republicans (Apr. 3, 2019), https://lahood.house.gov/sites/lahood.house.gov/files/LaHood%20DST%20Letter%20-%20Final.pdf.

digitalization of the global economy. These taxes, wherever imposed, warrant a substantial, proportionate response from the United States.[30]

Changes to international taxation may be warranted in the increasingly digitized global economy. To this end, CCIA supports the efforts of the Organization for Economic Cooperation and Development (OECD) and the Group of 20 (G20) to negotiate a consensus-based solution to the tax challenges arising from the digitalization of the economy. A long-term, multilateral solution that does not discriminate against U.S. services remains the only path forward to provide certainty, and reduce trade tensions caused by countries' decisions to enact unilateral measures.

With the OECD's announcement that work will continue into 2021 on the proposed blueprints,[31] the United States should ensure that countries continue to pause collection under existing DSTs until the OECD process is concluded.

D. Market-Based Platform Regulation

The idea of "platform regulation" is spurring measures around the world, including the EU, Japan, and Australia. 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.[32]

E. 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 the 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 failure of current U.S. trading partners to fully implement existing carefully negotiated intermediary protections in

[30] Additional analysis of DSTs and their violation of international norms are available in CCIA's Section 301 Comments to USTR. *See* CCIA Comments to Office of the U.S. Trade Rep., In re Initiation of Section 301 Investigations of Digital Services Taxes, Docket No. USTR-2020-0022, filed July 14, 2020, https://www.ccianet.org/wp-content/uploads/2020/07/Comments-of-CCIA-USTR-2020-0022-Section-301-Digital-Services-Taxes-.pdf (hereinafter "CCIA DST Comments").

[31] OECD/G20 Inclusive Framework on BEPS invites public input on the Reports on Pillar One and Pillar Two Blueprints (Oct. 12, 2020), https://www.oecd.org/tax/beps/oecd-g20-inclusive-framework-on-beps-invites-public-input-on-the-reports-on-pillar-one-and-pillar-two-blueprints.htm.

[32] Mark MacCarthy, *To Regulate Digital Platforms, Focus on Specific Business Sectors*, BROOKINGS INSTITUTION (Oct. 22, 2019), 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.").

free trade agreements.[33] This is illustrated by Australia and Colombia's continued lack of compliance.

As discussed in the EU section of these comments, implementation of the EU Digital Single Market 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.

F. 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.[34] A CCIA study showed that in 2014 fair use industries accounted for 16 percent of the U.S. economy, employed 1 in 8 workers, and contributed $2.8 trillion to GDP. Driven by increases in service-sector exports, U.S. exports of goods and services related to fair use increased by 21 percent from $304 billion in 2010 to $368 billion in 2014.[35] 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.[36] USTR also stated in 2017 its commitment to seek "the commitment of our free trade agreement partners to continuously seek to achieve an appropriate balance in their copyright systems, including through copyright exceptions and limitations."[37] 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

[33] *See also* CCIA Comments, In re Request for Public Comment for 2020 Special 301 Review, Docket No. 2019-0023, filed Feb. 6, 2020, https://www.ccianet.org/wp-content/uploads/2020/03/CCIA_2020-Special-301_Review_Comments.pdf.

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

[35] 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.

[36] See U.S.-Austl. Free Trade Agreement, May 18, 2004, 43 I.L.M. 1248, art. 17.11, para. 29; U.S.-Bahr. Free Trade Agreement, Dec. 7, 2005, 44 I.L.M. 544, art. 14.10, para. 29; U.S.-Chile Free Trade Agreement, June 6, 2003, 42 I.L.M. 1026, art. 17.11, para. 23; U.S.-Colom. Free Trade Agreement, Nov. 22, 2006, art. 16.11, para. 29; U.S.-S. Kor. Free Trade Agreement, June. 30, 2007, art. 18.10, para. 30; U.S.-Morocco Free Trade Agreement, June 15, 2004, art. 15.11, para. 28; U.S.-Oman Free Trade Agreement, Jan. 19, 2006, art. 15.10, para. 29; U.S.-Pan. Trade Promotion Agreement, June 28, 2007, art. 15.11, para. 27; U.S.-Sing. Free Trade Agreement, May 6, 2003, 42 I.L.M. 1026, art. 16.9, para. 22, U.S.-Mexico-Canada Agreement, 2018.

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

are jeopardized by weak or nonexistent limitations and exceptions in the copyright laws of other countries.[38] 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.[39] A USITC report also observed that these laws tend to have "generated unintended consequences" to small online publishers.[40] 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 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.[41]

As explained in the EU section of these comments, the EU Digital Single Market Copyright Directive creates an EU-wide version of this right. Australia recently proposed a mandatory draft Code of Conduct on online news aggregators that assume a right to payment similar to ancillary rights. Similar proposals have been discussed in Canada.[42] These initiatives often are

[38] 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.projectdisco.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.").

[39] USTR, *2020 NTE Report*, https://ustr.gov/sites/default/files/2020_National_Trade_Estimate_Report.pdf.

[40] *2017 Global Digital Trade 1*, *supra* note 7, 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.").

[41] 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.

[42] Michael Geist, *How to pay for the future of journalism*, FINANCIAL POST (May 13, 2020), https://financialpost.com/opinion/michael-geist-how-to-pay-for-the-future-of-journalism.

based on flawed understanding of market dynamics between online news content and online aggregators, and especially in the case of Australia, narrowly targeted to apply to U.S. firms.[43]

G. 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.[44] 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.

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 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 increasing rate, remedies that apply extraterritorially will have far-reaching consequences.

H. 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.

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

[43] *Id.*

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

Progressive Agreement for Trans-Pacific Partnership (CPTPP),[45] Article 19.3 of the U.S.-Mexico-Canada Agreement (USMCA),[46] and Article 8.72 of the EU-Japan Economic Partnership Agreement.[47]

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 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.[48] Analysis on duties on electronic transmissions for economic development shows that this is not supported.[49] 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.

I. 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

[45] 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.

[46] 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"].

[47] 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.

[48] *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 ask 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.

[49] OECD, *Electronic transmissions and international trade – Shedding new light on the Moratorium Debate* (Nov. 4, 2019), https://one.oecd.org/document/TAD/TC/WP(2019)19/FINAL/en/pdf; 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*, REALCLEARPOLICY (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, http://www2.itif.org/2019-worst-mercantilist-policies.pdf.

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.[50]

These exceptional access regimes run contrary to the consensus assessments of security technologists because they are technically and economically infeasible to develop and implement.[51] 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.

J. Market Barriers Access for Communications 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 strong language regarding forbearance in trade agreements, to ensure that the regulator's decisions on forbearance are based on evidence-based analysis.[52]

III. COUNTRY-SPECIFIC CONCERNS

A. 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

[50] 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/.

[51] 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.

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

Monitoring System.[53] 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.[54] However, industry reports that there are still limits within the "express" regime that make it difficult to export to Argentina and some U.S. companies have had to stop exporting to the Argentinian market completely.

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

Capital Controls

The Argentine government has applied a series of capital controls and new tax measures to the consumption of imports over the past year that make it more challenging for Argentine citizens to import goods and services. On October 28, 2019, the Central Bank established a limit of $200 per month that citizens were able to access through their bank accounts, limiting the amount of money those citizens could use to import goods and services.[55] On December 23, 2019, the executive branch issued Decree 99/2019, implementing a temporary 30 percent tax ("PAIS tax") on the purchase of foreign currency and purchases made online invoiced in foreign currency, among other things.[56] Further on September 16, 2020 the Central Bank introduced a new 35 percent tax on foreign currency purchases, including on cross-border transactions made with credit cards, to "discourage the demand for foreign currency."[57] Combined, these controls and taxes are making it increasingly difficult, and at times impossible, for foreign companies to sell to Argentine customers.

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

[54] 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.

[55] *Argentine Central Bank Cuts Dollar Purchase Limit Sharply as Forex Reserves Tumble*, REUTERS (Oct. 28, 2019), https://www.reuters.com/article/us-argentina-cenbank/argentine-central-bank-cuts-dollar-purchase-limit-sharply-as-forex-reserves-tumble-idUSKBN1X708U.

[56] *Argentina: Argentina Introduces Major Tax Reform*, INTERNATIONAL TAX REVIEW (Feb. 3, 2020), https://www.internationaltaxreview.com/article/b1k41n6smqd3jy/argentina-argentina-introduces-major-tax-reform.

[57] *Central Bank Tightens Currency Controls as Peso Weakens*, BA TIMES (Sept. 16, 2020), https://www.batimes.com.ar/news/economy/central-bank-tightens-currency-controls-as-peso-weakens.phtml.

B. Australia

Market-Based Regulations

In August 2020, the Australian Government and the Australian Competition and Consumer Commission (ACCC) published a draft Code of Conduct that seeks to regulate commercial relationships between publishers and digital platforms. This followed an initial inquiry earlier in 2018 that contemplated a voluntary regime to encourage these entities to work together. However, the Concepts Paper released earlier in 2020 departed from this reasoning significantly in proposing a compulsory model governed by the ACCC.

Motivated by a desire to empower domestic news publishers, the new rules would dictate that online services negotiate and pay Australian news publishers for online content, and also disclose proprietary information related to private user data and algorithms. As drafted, the Australian Treasury would have the utmost discretion to determine which companies these mandates are applied to, and currently only two companies – both American – have been identified at this time. There are significant concerns from a procedural,[58] competition,[59] trade,[60] and intellectual property[61] perspective that USTR should pay close attention to.

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 additional powers when dealing with encrypted communications and devices.[62] 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

[58] Marianela Lopez-Galdos, *Australian Regulations Detrimental to the Digital Economy: Process (Part 1)*, DISRUPTIVE COMPETITION PROJECT (Aug. 6, 2020), https://www.project-disco.org/competition/080620-australian-regulations-detrimental-to-the-digital-economy-process/.

[59] Marianela Lopez-Galdos, *Australian Regulations Detrimental to the Digital Economy: Competition (Part 2)*, DISRUPTIVE COMPETITION PROJECT (Aug. 13, 2020), https://www.project-disco.org/competition/081320-australian-regulations-detrimental-to-the-digital-economy-competition/.

[60] Rachael Stelly, *Australian Regulations Detrimental to the Digital Economy: Trade (Part 3)*, DISRUPTIVE COMPETITION PROJECT (Sept. 4, 2020), https://www.project-disco.org/21st-century-trade/090420-australian-regulations-detrimental-to-the-digital-economy-trade-part-3/.

[61] Ali Sternburg, *Australian Regulations Detrimental to the Digital Economy: Intellectual Property (Part 4)*, DISRUPTIVE COMPETITION PROJECT (Oct. 9, 2020), https://www.project-disco.org/intellectual-property/100920-australian-regulations-detrimental-to-the-digital-economy-intellectual-property-part-4/.

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

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.[63]

Copyright Liability Regimes for Online Intermediaries

Failure to implement obligations under existing trade agreements serves as a barrier to trade.[64] 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 has been enacted to remedy it.[65] This oversight was not addressed by the 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.[66] 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.

Government-Imposed Content Restrictions and Related Access Barriers

Australia amended its Criminal Code in April 2019 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

---

[63] 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.

[64] *See* CCIA Comments to Office of the U.S. Trade Rep., In re Request for Public Comments and Notice of a Public Hearing Reading the 2020 Special 301 Review, Docket No. USTR-2019-0023, filed Feb. 6, 2020, https://www.ccianet.org/wp-content/uploads/2020/03/CCIA_2020-Special-301_Review_Comments.pdf.

[65] 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.

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

this material.[67] Criticism for the legislation was widespread, with particular concern about the rushed nature of the drafting and legislative process.[68] The legislation applies to a broad range of technology and Internet services, including U.S.-based social media platforms, user-generated 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.[69] 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.[70]

Additional E-Commerce Barriers

The Treasury Laws Amendment (GST Low Value Goods) Act 2017 took effect in 2018 and directs the Australian government to start collecting goods and services tax (GST) on all goods including those purchased online from overseas, previously only applied to goods over $1,000 AUD.[71] Companies with over $75,000 AUD in sales to Australian customers are required to register and lodge returns with the Australian Tax Office.

C. Austria

Digital Taxation

Austria implemented a 5 percent digital tax on revenues from digital advertising services provided domestically.[72] The global revenue threshold is 750 million euro, and domestic revenue threshold is 25 million euro. The tax, implemented in the Digital Tax Act 2020 (*Digitalsteuergesetz* 2020), became effective on January 1, 2020. "Online advertisement services" include advertisements placed on a digital interface, in particular in the form of banner advertising, search engine advertising and comparable advertising services.[73] Per officials, a covered service is deemed to have been provided domestically "if it is received on a user's

[67] 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.

[68] *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.

[69] *See* Lucie Krahulcova & Brett Solomon, *Australia's plans for internet regulation: aimed at terrorism, 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.").

[70] Alison Bevege, *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.

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

[72] Austria: Legislation Introducing Digital Services Tax, KPMG (Oct. 29, 2019), https://home.kpmg/us/en/home/insights/2019/10/tnf-austria-legislation-introducing-digital-services-tax.html.

[73] Federal Ministry Republic of Austria, Digital Tax Act 2020, https://www.bmf.gv.at/en/topics/taxation/digital-tax-act.html (last visited Oct. 29, 2020).

device having a domestic IP address and is addressed (also) to domestic users in terms of its content and design."[74] The tax also provides for the use of an IP address or other geolocation technologies to determine the location of the service.

The discriminatory motivations underlying this tax are clear, with U.S. companies being singled out as targets of this online advertising tax. Upon introduction, 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."[75]

D. 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. This will increase legal uncertainty and open a path to use competition to slow down successful U.S. companies operating in these regions.

Digital Taxation

After rejecting a similar proposal in 2019, Belgium reintroduced a DST in June 2020. The tax would be 3 percent and applies to revenue derived from the selling of user data. The newly elected government announced that they would wait for an OECD solution. Industry is monitoring political developments.[76]

---

[74] Id.

[75] Sebastian Kurz (@sebastiankurz), Twitter (Apr. 3, 2019, 1:44 AM), https://twitter.com/sebastiankurz/status/1113361541938778112. *See also* Parliamentary Correspondence No. 914, National Council: digital tax on online advertising sales decided, Aug. 20, 2019, *available at* https://www.parlament.gv.at/PAKT/PR/JAHR_2019/PK0914/ ("Internetgiganten wie Facebook oder Google müssen künftig Online-Werbeumsetze abführen. Um mehr Steuergerechtigkeit zu erreichen, soll nun auch die seit längerem in der Öffentlichkeit diskutierte Digitalsteuer umgesetzt werden; das dazu von ÖVP und FPÖ vorgelegte Abgabenänderungsgesetz 2020 hatte die nötige Stimmenmehrheit. Nunmehr müssen Internetgiganten wie Facebook, Google oder Amazon ab dem Jahr 2020 eine fünfprozentige Steuer auf Online-Werbeumsätze abführen haben. Konkret sind jene Unternehmen betroffen, die einen weltweiten Umsatz von 750 Mio. € bzw. einen jährlichen Umsatz aus Onlinewerbeleistungen von mindestens 25 Mio. € erzielen, soweit diese in Österreich gegen Entgelt erbracht werden. Aus den aus der Digitalsteuer resultierenden Einnahmen sollen jährlich 15 Mio. € an österreichische Medienunternehmen gehen." [Internet giants like Facebook or Google will have to pay for online advertising sales in the future. In order to achieve more tax justice, the digital tax that has long been discussed in public should now be implemented; the Tax Amendment Act 2020 presented by the ÖVP and FPÖ had the necessary majority of votes. Internet giants like Facebook, Google or Amazon must now pay a five percent tax on online advertising sales from 2020. Specifically, those companies are affected that achieve a worldwide turnover of € 750 million or an annual turnover from online advertising services of at least € 25 million, as far as these are rendered in Austria for a fee. From the income resulting from the digital tax, € 15 million should go to Austrian media companies every year.]).

[76] David Gaier, *INSIGHT: Belgium and Digital Taxation—Where do we Stand?*, BLOOMBERG TAX (Sept. 30, 2020), https://news.bloombergtax.com/daily-tax-report-international/insight-belgium-and-digital-taxation-where-do-we-stand.

E. 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). There has been confusion with respect to its effective date after a series of announced delays.[77]

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.[78] 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.[79] In addition, the national authority is tasked with determining whether a foreign government or international organization has a sufficient data protection scheme in place before any data is authorized to be transferred to the government or organization.[80]

On September 29, 2020, Bill 4723/2020 was introduced that would amend Brazils' Data Protection Law requiring all personal data to be stored within the country.[81] The bill also would forbid the use of cloud computing for any data processing when data is stored outside the country.

Other localization barriers reported include tax incentives for locally sourced information and communications technology (ICT) goods and equipment,[82] government procurement preferences for local ICT hardware and software,[83] and non-recognition of the results of conformity assessment procedures performed outside of Brazil for equipment connected to telecommunications networks.[84] 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.[85] These requirements disadvantage firms that provide services to the Brazil public sector but do not have the capacity to store data locally, and these guidelines set concerns precedents.

---

[77] Kate Black *et al*., *Brazil's Data Protection Law Will Be Effective After All, But Enforcement Provisions Delayed Until August 2021*, GREENBERGTRAURIG (Aug. 28, 2020), https://www.gtlaw.com/en/insights/2020/8/brazils-data-protection-law-effective-enforcement-provisions-delayed-august-2021.

[78] 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.

[79] Chris Brook, *Breaking Down LGPD, Brazil's New Data Protection Law*, DATA INSIDER (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 are found in articles 33-36 of the LGPD).

[80] *Brazil's New Data Protection Law: The LGPD*, *supra* note 78.

[81] Legislative text available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=FBFEDDCD86E43AC204C6E5AA41823F12.proposicoesWebExterno2?codteor=1932528&filename=Tramitacao-PL+4723/2020.

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

[83] 2014 Decrees 8184, 8185, 8186, 8194, and 2013 Decree 7903.

[84] ANATEL's Resolution 323.

[85] *Brazil's New Data Protection Law: The LGPD*, *supra* note 78.

Copyright Liability Regimes for Online Intermediaries

The Ministry of Citizenship held a consultation in 2019 on Brazil's Copyright Law.[86] Industry reports that officials 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.

Digital Taxation

Brazil is currently considering various digital tax initiatives, including the introduction of a DST through an expansion of its existing CIDE (*contribuição de intervenção no domínio econômico*) regime. The CIDE-Digital tax (PL 2,358/2020) would apply progressively from 1 percent to 5 percent on gross revenues derived from (1) digital advertising; (2) operating a digital service that permits users to interact with each other for the sale of goods and services; and (3) collection of user-generated data in the operation of a digital platform.[87] There is also pending legislation (PL 131/2020) to raise payments under the existing COFINS regime (*contribuição para o financiamento da seguridade social*) for companies in the digital sector.[88] Brazil should be discouraged from introducing new taxes that discriminate against a specific class of digital companies for specialized taxation.

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 sizes and serves as an e-commerce barrier. It also does not apply to business-to-consumer or business-to-business transactions.[89] The differential treatment and low *de minimis* threshold for consumer-to-consumer transactions create barriers to international trade by increasing transaction costs for Brazilian businesses while limiting consumer choice and competition amongst Brazilian businesses. Extending the *de minimis* threshold to business-to-consumer and business-to-business transactions and raising the *de minimis* threshold would help

[86] Ministério Do Turismo, Secretaria Especial da Cultura, Ministério da Cidadania abre consulta pública 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/.

[87] *Brazil Congressman Proposed Digital Services Tax*, EY (May 8, 2020), https://taxnews.ey.com/news/2020-1246-brazilian-congressman-proposes-digital-services-tax.

[88] *Brazil: Proposed COFINS Regime for Digital Sector Taxpayers*, KPMG (July 7, 2020), https://home.kpmg/us/en/home/insights/2020/07/tnf-brazil-proposed-cofins-regime-digital-sector-taxpayers.html ("The proposal (COFINS-Digital) would, if enacted, affect companies that operate in the digital sector and would focus on the gross monthly revenue earned in relation to digital services from: [1] Electronic communications and digital interface that allows interaction between users with regard to the delivery of goods or provision of services [and 2] Marketing to advertisers or agents for placing targeted advertising messages on a digital interface based on user data.").

[89] 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.

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.[90]

F. Cambodia

Government-Imposed Content Restrictions and Related Access Barriers

Reports of censorship and mandated Internet filtering and blocking continue to rise in Cambodia.[91] Legislation passed in April 2020 grants extensive authorities to the government to restrict information online if a state of emergency is imposed.[92]

G. Canada

Extraterritorial Regulations and Judgments

Rulings regarding intermediary liability that have extraterritorial effects present a significant barrier to trade by creating significant market uncertainty for companies seeking to host user content and communications on a global basis. In *Equustek Solutions v. Jack*, Google was compelled by the Supreme Court of British Columbia to remove—from all its domains worldwide—indexes and references to the website of Datalink, a competitor to Equustek that had been found to have violated Canadian trade secrets and consumer protection laws.[93]

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.[94]

Restrictions on Cross-Border Data Flows

In its 2019 comments CCIA raised concerns with the Office of Privacy Commission (OPC) consultation on the review of its official policy position on cross-border data flows under the

---

[90] 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/de-minimis/GEA%20overview%20on%20de%20minimis_9%20March%202018.pdf.

[91] *Freedom on the Net 2020: Cambodia* (2020), https://freedomhouse.org/country/cambodia/freedom-net/2020.

[92] *Id.* at C1, The Law on the Management of the Nation in a State of Emergency.

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

[94] 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.

Personal Information Protection and Electronic Documents Act.[95] After industry concerns, the OPC determined that it would not amend the guidelines.[96] Rather, it intends to direct lawmakers to reevaluate existing law and determine whether legislative changes are needed. The Government of Quebec has recently introduced new privacy legislation that, amongst other things, would make data transfers extraordinarily difficult.[97] Industry is following these proceedings. Abrupt changes to procedures that enable data transfer between the U.S. and Canada may 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.

H. Chile

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. The same requirement is outlined in Circular No. 2, which is addressed to non-banking payment card 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.

I. 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.

CCIA asks USTR to remain vigilant and discourage policies restricting foreign companies' ability to enter the Chinese technology sector, and to promote policies focused on allowing free and open competition within China's borders. This is increasingly critical as China's global dominance in technology services continues to rise.[98] U.S. policy should target unfair practices by foreign trade partners, while ensuring any U.S. offensive measures or regulations do not have the adverse effect of disadvantaging U.S. firms.

---

[95] CCIA Comments, In re Request for Public Comments To Compile the National Trade Estimate Report on Foreign Trade Barriers, Docket. No. 2019-0012, filed Oct. 31, 2019 at 33, *available at* https://www.ccianet.org/wp-content/uploads/2019/10/USTR-2019-CCIA-Comments-for-NTE.pdf [hereinafter "2019 CCIA NTE Comments"].

[96] 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/.

[97] *Quebec to introduce the most punitive privacy laws in Canada – with fines of up to $25 million*, LEXOLOGY (June 19, 2020), https://www.lexology.com/library/detail.aspx?g=a42e22b1-ec2d-4a79-a9d3-74519ef6a3e8.

[98] Richard Bowman, *Rise of China's Tech Giants – What to know when investing in Chinese tech companies*, CATANA CAPITAL (Aug. 3, 2020), https://catanacapital.com/blog/investing-chinese-tech-companies/.

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

As documented in previous CCIA NTE comments, China remains a very difficult market for Internet services to operate in due to a number of localization and protectionist measures.[99] This is a result of measures including restrictions on the transfer of personal information, extensive requirements on foreign cloud service providers to partner with local firms, and foreign investment restrictions. These regulations all are fundamentally protectionist and anticompetitive, and contrary to China's WTO commitments and separate commitments to the United States.[100]

Subsequent standards and draft measures made pursuant to the 2016 Cybersecurity Law pose continued concerns. Below are recent measures that industry is tracking.

On June 13, 2019, new draft Measures of Security Assessment of the Crossborder Transfer of Personal Information were released by the Cyberspace Administration of China for public comment. This draft focuses on cross-border transfer of "personal information." Article 2 of the draft measures subjects any transfer of covered data outside China to strict and comprehensive security assessments.[101] There is confusion regarding how this draft affects prior draft legislation on cross-border data and localization mandates issued pursuant to the Cybersecurity Act.[102]

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.[103] "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."[104]

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.[105] The draft amendments released

---

[99] 2019 CCIA NTE Comments, *supra* note 95 at 34-40.

[100] In commitments made in September 2015 and June 2016, China agreed that its cybersecurity measures in the commercial sector would not disadvantage foreign providers and would not include nationality-based restrictions.

[101] 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/.

[102] 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 measures on "personal information and important data outbound transfer security assessment").

[103] 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/.

[104] *Id.*

[105] 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/.

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.[106]

The two draft Measures above are reportedly being submitted for deliberation during the National People's Congress term ending in 2023.[107]

In July 2020, a draft Data Security Law was released for public comment. As drafted, the law would create new rules and liability for entities engaging in certain data activities including those that would harm the "national security, public interest, or lawful interests of citizens or organizations" in China.[108] The law also provides greater authority for the Chinese government to retaliate against foreign governments that impose restrictions on Chinese foreign investment or technologies.[109] The draft law further states China will establish a data security review mechanism, and data processers shall obtain licenses, cooperate with national security agencies and go through data review processes for various data related activities in China.

Industry reports that China has also released more measures regarding data security, lacking of necessary clarifications on key terms and procedures (e.g. clarification on important data and criteria for triggering a data security review), bringing more ambiguity and uncertainty, and increasing the already complex and uncertain compliance burdens on multinational companies.

Restrictions on Cloud Services

China seeks to further restrain foreign cloud service operators, in concert with its national plan to promote the Chinese cloud computing industry. As CCIA have noted in previous submissions, U.S. cloud service providers (CSPs) are worldwide leaders and strong U.S exporters, supporting tens of thousands of high-paying American jobs and making a strong contribution toward a positive balance of trade.[110] While U.S. CSPs have been at the forefront of the movement to the cloud in virtually every country in the world, China has blocked them.

Draft Chinese regulations combined with existing Chinese laws will force U.S. CSPs to transfer valuable U.S. intellectual property, surrender use of their brand names, and hand over operation and control of their business to a Chinese company in order to operate in the Chinese market.

---

[106] 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/.

[107] Graham Webster & Rogier Creemers, *A Chinese Scholar Outlines Stakes for New 'Personal Information' and 'Data Security' Laws (Translation)*, NEW AMERICA (May 28, 2020), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-scholar-outlines-stakes-new-personal-information-and-data-security-laws-translation/.

[108] Emma Rafaelof, *et al*., Translation: China's 'Data Security Law (Draft)', NEW AMERICA (July 2, 2020), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/.

[109] *Id.*

[110] 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-leadsmanaged-private-cloud.

Without immediate U.S. Government intervention, China is poised to implement fully these restrictions, effectively barring U.S. CSPs from operating or competing fairly in China.

China's Ministry of Industry and Information Technology (MIIT) proposed two draft notices – Regulating Business Operation in Cloud Services Market (2016) and Cleaning up and Regulating the Internet Access Service Market (2017). These measures, together with existing licensing and foreign direct investment restrictions on foreign CSPs operating in China under the Classification Catalogue of Telecommunications Services (2015) and the Cybersecurity Law (2016), would require foreign CSPs to turn over essentially all ownership and operations to a Chinese company, forcing the transfer of incredibly valuable U.S. intellectual property and know-how to China.[111]

Further, China's draft notices are inconsistent with its WTO commitments as well as specific commitments China has made to the U.S. Government in the past. In both September 2015 and June 2016, China agreed that measures it took to enhance cybersecurity in commercial sectors would be non-discriminatory and would not impose nationality-based conditions or restrictions.

The United States must secure a Chinese commitment to allow U.S. CSPs to compete in China under their own brand names, without foreign equity restrictions or licensing limitations, and to maintain control and ownership over their technology and services. Chinese CSPs remain free to operate and compete in the U.S. market, and U.S. CSPs should benefit from the same opportunity in China.

Export Controls

China finalized a new export law in October 2020 that is set to take effect December 1, 2020.[112] The law permits China to take reciprocal measures against "any country or region that abuses export control measures to endanger the national security and interest of the People's Republic of China." There are concerns that this law will be used to retaliate against U.S. services as a result of ongoing U.S.-China trade conflicts.

Intellectual Property Reforms

CCIA is tracking developments regarding the National People's Congress's 2020 amendments to the Chinese patent law. Changes to damages in Chinese patent law, in particular to enhanced damages and permitting the recovery of infringers' profits, are concerning. Industry encourages continued monitoring of the impact of these changes on U.S. industry.

[111] More specifically, these measures (1) prohibit licensing foreign CSPs for operations; (2) actively restrict direct foreign equity participation of foreign CSPs in Chinese companies; (3) prohibit foreign CSPs from signing contracts directly with Chinese customers; (4) prohibit foreign CSPs from independently using their brands and logos to market their services; (5) prohibit foreign CSPs from contracting with Chinese telecommunication carriers for Internet connectivity; (6) restrict foreign CSPs from broadcasting IP addresses within China; (7) prohibit foreign CSPs from providing customer support to Chinese customers; and (8) require any cooperation between foreign CSPs and Chinese companies be disclosed in detail to regulators. These measures are fundamentally protectionist and anti-competitive.

[112] Available at http://www.mofcom.gov.cn/article/zwgk/zcfb/202010/20201003008907.shtml.

Industry also supports the process to revise China's 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.

Additional E-Commerce Barriers

China passed its first law regulating "e-commerce" in August 2018 which took effect in January 2019.[113] The law is broadly written, applying new regulations and requirements on all ecommerce activities in China defined as the "sale of goods or services through the internet or any other information network."[114] Requirements include the need to obtain a business license to operate, which could place a burden on small businesses.

Electronic Payment Regulations

The People's Bank of China (PBOC) released Notification No.7 in March 2018 that restrict foreign institutions that intend to provide electronic payment services for domestic or cross-border transactions.[115] Notification No. 7 mandates service providers set up a Chinese entity and obtain a payments license. Industry reports that the PBOC has subsequently blocked foreign entities from obtaining payment license, by restricting the ability of acquiring existing licensed entities and by stopping foreign entities from applying for licenses, not approving new foreign entity applications, including for those already in the pipeline. The inconsistent interpretation has resulted in the blocking or delaying the launch and operation of new electronic payment services provided by U.S. companies.

J. Colombia

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.[116] Revision to the legislation in 2018 that sought to implement the U.S.-Colombia FTA copyright chapter includes no language on online intermediaries.[117] 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.

---

[113] 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/.

[114] *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.

[115] *PBOC opens the door for foreign payment institutions*, HOGAN LOVELLS (Mar. 23, 2018), https://www.hoganlovells.com/en/publications/pboc-opens-the-door-for-foreign-payment-institutions.

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

[117] 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-billcolombia-law-1915-2018/.

National Strategy on Artificial Intelligence

Colombia is currently considering a national strategy on AI. Some policymakers have taken positions on these initiatives that could lead to unique standards, onerous certification or localization requirements or other concerning regulations. Colombia should pursue a flexible and diversified regulatory approach that champions public-private collaboration. Additional, the facilitation of data sharing, advancement of structure and standardized AI research and development, support for STEM workforce development should all be encourage.

K. Czech Republic

Digital Taxation

Announced by the Ministry of Finance in July 2019,[118] the Czech Republic is currently finalizing its digital tax which was presented to Parliament in November 2019.[119] The tax would apply to revenues from (1) targeted advertising on digital interface, (2) the transmission of data about users and generated from users' activities on digital interfaces, and (3) making available to users a multi-sided digital interface to facilitate the provision of supplies of goods and services.[120] The proposed tax rate was 7 percent but there was recently an agreement to reduce it to 5 percent, in order to be consistent with other EU member measures.[121] The effective date is expected to be January 2021. Policymakers have cited the need to tax U.S. companies despite support for an OECD solution.

L. European Union

Under the current European Commission, the EU is pursuing an expansive agenda and new regulatory frameworks designed to bring the EU closer to achieving "technology sovereignty". European politicians have stated that the purpose of digital sovereignty is to create a "new empire" of European industrial powerhouses to resist American rivals.[122] This includes regulations on competition, artificial intelligence, platform liability, among other certification schemes. The pursuit of "technological sovereignty" will likely disadvantage U.S. exporters to the benefit of domestic competitors.

At a time when countries such as China are pursuing protectionist policies that threaten the open Internet and free trade, it is discouraging that the EU is heading down a similar path. Industry

---

[118] Press Release, The Ministry of Finance Sends Draft Law in Digital Tax to Comment Procedure (July 4, 2019), https://www.mfcr.cz/cs/aktualne/tiskove-zpravy/2019/mf-posila-do-pripominkoveho-rizeni-navrh-35609.

[119] *Czech Republic to Delay Proposed Digital Tax, Cut Rate to 5%*, BLOOMBERG TAX (June 10, 2020), https://news.bloombergtax.com/daily-tax-report-international/czech-republic-to-delay-proposed-digital-tax-cut-rate-to-5.

[120] *KPMG Digital Taxation Report*, *supra* note 27, at 7.

[121] *Coalition Agrees on Lower Rate for Forthcoming Digital Tax*, ČESKÉ NOVINY (June 10, 2020), https://www.ceskenoviny.cz/zpravy/koalice-se-shodla-na-nizsi-sazbe-pro-chystanou-digitalni-dan/1900867; *Czech Republic Agrees to Lower "GAFA Tax" on Digital Giants*, KAFKADESK (June 13, 2020), https://kafkadesk.org/2020/06/13/czech-republic-agrees-to-lower-gafa-tax-on-digital-giants/.

[122] Scott Fulton III, *After Brexit, will 5G survive the age of the European empire?*, ZDNET (Nov. 5, 2019), https://www.zdnet.com/article/after-brexit-will-5g-survive-the-age-of-the-european-empire/.

encourages USTR to closely monitor developments in the region and discourage any intended or unintended protectionism.

Further, as part of the ambitious Digital Single Market strategy under the previous European Commission, the EU finalized a number of regulations and policies which, as they are being implemented by EU Member States, will affect digital imports. Many of these policies continue to have a lasting impact on the state of innovation within the EU and impact digital exports to the European market.

Restrictions on Cross-Border Data Flows and Data Localization

Industrial Policies and Technological Sovereignty

As part of the EU-wide push for "technological sovereignty" there are proposals to craft EU industrial policy measures that will facilitate data localization and force out U.S. cloud providers. New measures would build and promote European cloud services at the expense of market-leading U.S. cloud services, with many policymakers calling for a "trusted" European cloud.

This has been supported by a number of European policy makers including, but not limited, to the following:

- Internal Market Commissioner Thierry Breton has explicitly called for localization of European data on European soil as well as exclusive application of EU law on European data.[123]
- French President Macron stated that Europe should not rely "on any non-European power" for data security.[124]
- European Council Conclusions from October 2, 2020 note that "the need to establish trusted, safe and secure European cloud services in order to ensure that European data can be stored and processed in Europe, in compliance with European rules and standards."[125]
- A declaration signed by 25 Member States on October 15, 2020 stated the need to develop "a truly competitive EU cloud supply" to reverse the current trend towards cloud infrastructure market convergence "around four large non-European players"**,** and address "concerns over cloud users' ability to maintain control over strategic and sensitive personal and non-personal data." The Declaration recommends excluding providers of cloud services from the so-called European Cloud Federation if they are subject to "laws of foreign jurisdictions," unless they can demonstrate they have put in

[123] POLITICO Virtual Brussels Playbook Interview with Thierry Breton (Sept. 1, 2020), *available at* https://www.youtube.com/watch?v=L6qWkdq9xSQ&t=1445.

[124] *France's Macron says Europe has "lost" the global battle in cloud computing*, REUTERS (Sept. 14, 2020), https://uk.reuters.com/article/us-france-tech-macron/frances-macron-says-europe-has-lost-the-global-battle-in-cloud-computing-idUSKBN26532N.

[125] General Secretariat of the Council, Special meeting of the European Council (Oct. 2, 2020), https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf.

place "verified safeguards" to ensure that any foreign request to access EU (personal and non-personal) data is compliant with EU law.[126]

- U.S. cloud providers have been relegated to observers in the Franco-German GAIA-X cloud project.
- The French government is looking to migrate French citizens' health data ('Health Data Hub') from Microsoft to a French or European cloud service provider, "because of the invalidation of Privacy Shield".[127]

As CCIA raised in previous NTE comments, there have already been attempts to establish an EU-wide cloud that would localize data within EU borders.[128] Following the original announcement in 2019 by Germany, this June German Federal Minister of Economic Affairs and Energy Peter Altmaier and the French Minister of Economy and Finance Bruno Le Maire unveiled details on plans to create Europe's own cloud services, titled "GAIA-X".[129] According to the documents made available, the goal of the project is the "development of a trustworthy and sovereign digital infrastructure for Europe" and "GAIA-X will support the development of a digital ecosystem in Europe, which will generate innovation and new data-driven services and applications."[130]

At the same time, the French Economy Minister has characterized the U.S. CLOUD Act and other U.S. laws (*e.g.*, FISA Section 702, Executive Order 12333) as an overstep into France's sovereignty and is helping local industry players and excluding U.S. industry from public procurements.[131] At the same time, European criticisms of (non-EU) extraterritorial government data access laws and practices are at odds with Member States' support for the EU's proposed e-

---

[126] Declaration, Building the next generation cloud for businesses and the public sector in the EU, *available at* https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=70089.

[127] Julien Lausson, *Health Data Hub: Cédric O prévoit de quitter Microsoft pour un prestataire français*, NUMERAMA (Oct. 9 2020), https://www.numerama.com/tech/656229-health-data-hub-cedric-o-prevoit-de-quitter-microsoft-pour-un-prestataire-francais.html.

[128] 2019 CCIA NTE Comments, *supra* note 95 (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.)

[129] Liam Tung, *Meet GAIA-X: This is Europe's bid to get cloud independence from US and China giants*, ZDNET (June 8, 2020), https://www.zdnet.com/article/meet-gaia-x-this-is-europes-bid-to-get-cloud-independence-from-us-and-china-giants/; *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/; *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..

[130] Federal Ministry for Economic Affairs and Energy (BMWi), *GAIA-X - the European project kicks off the next phase* (June 4, 2020), https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=13.

[131] *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; *France's Health Data Hub to replace Microsoft with European cloud infrastructure provider*, TELECOMPAPER (Oct. 13, 2020), https://www.telecompaper.com/news/frances-health-data-hub-to-replace-microsoft-with-european-cloud-infrastructure-provider--1357565.

Evidence Regulation,[132] EU legislation akin to the U.S. CLOUD Act that would allow European law enforcement to request access to data irrespective of the location of the data.

Industry reports that additional work on a fiscal stimulus package designed to offset the economic effects of the COVID-19 pandemic may also distort equal access to finance between U.S. and EU-based firms.[133]

Privacy laws and data transfers to the U.S. post-*Schrems II*

The EU's approach to privacy protections presents barriers for some U.S. exporters. The General Data Protection Regulation (GDPR) was adopted on April 27, 2016, and went into effect on May 25, 2018.[134] 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.

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. In July 2020 the CJEU invalidated the European Commission's decision on the EU-U.S. Privacy Shield framework which more than 5,000 companies relied on for the transatlantic commercial data transfer.[135] The ruling created immediate legal uncertainty for thousands of companies, a majority of which are SMEs. CCIA encourages the European Commission and the U.S. Administration to quickly develop a durable new framework, fully in line with EU law, to enable the data flows between the world's most important trading partners.[136] In the short and medium term, consistent enforcement and practical guidance for companies transferring data to countries which do not benefit from an "adequacy" status is essential. Unfortunately, some national regulators are expressing their own restrictive views on how companies can or cannot transfer EU personal data to 'non-adequate' countries.[137] This could lead to enforcement fragmentation and inability to serve products in parts of the EU.

---

[132] Press Release, EU Council, Regulation on cross border access to e-evidence: Council agrees its position, (Dec. 7 2018), https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/.

[133] Industry reports that these plans include (1) investment in 'key value chains' for Europe's 'strategic autonomy' in sectors around the EU's green and digital transitions, and (2) support of the solvency of EU-based companies by the European Investment Bank.

[134] 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"].

[135] Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, case C-311-18, CJEU, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

[136] Press Release, EU Top Court Strikes Down Privacy Shield, CCIA Calls for Urgent Legal Certainty and Solutions (July 16, 2020), https://www.ccianet.org/2020/07/916160/.

[137] *See, e.g.*, Statement from the Berlin Supervisory Authority (July 17, 2020), https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf ("Data should not be transferred to the US until [the U.S.] legal framework is reformed"); Statement from the Hamburg Supervisory Authority (July 16, 2020), https://datenschutz-

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.[138] The EU has presented this text within the context of the WTO Joint Statement Initiative on Electronic Commerce.

The EU also has been working on amending the existing ePrivacy Directive and proposed the "ePrivacy Regulation" in 2017.[139] The proposal seeks to expand the existing Directive, which only applies to telecommunication services, to all "electronic communication services" including over the top services.[140] Rules that were originally created for traditional telecommunication services would then 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 scope expansion by observing that since the enactment of the ePrivacy 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."[141] This is based on a flawed understanding of the services at issue and it is ignoring that the Internet has flourished largely due to *not* treating over-the-top services like traditional telecommunications providers.

Following a rise in data localization measures across EU Member States,[142] 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.[143] The regulation aims to remove national mandated data

---

hamburg.de/pressemitteilungen/2020/07/2020-07-16-eugh-schrems ("A data transfer to countries without an adequate level of data protection will therefore no longer be allowed in the future"); French Supervisory Authority's (CNIL) observations submitted to the Conseil d'Etat, 8 October 2020, https://assets.documentcloud.org/documents/7224049/Me-moireCnilHDH.pdf (lack of particularized review of "all the circumstances" surrounding (hypothetical) data transfers by Microsoft in the context of the performance of a service to the French Health Data Hub, as well as a general recommendation to use service providers which are only subject to EU laws).

[138] 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.").

[139] 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"].

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

[141] *Id*. at recital 6.

[142] 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.

[143] 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.

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 and provide legal clarity for companies and users.[144] 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.[145]

Market-Based Regulations

The Commission is preparing extensive regulatory proposals (under the planned Digital Markets Act). In recent years, U.S. technology firms have seen a rise in protectionist actions relating to competition in the forms of antitrust enforcement and new regulations.

First, the EU has announced plans to impose new regulations on certain "structurally significant" digital businesses. This "ex ante" proposal is expected to be released in December 2020, and will restrict the competitive capabilities of large technology companies, making it harder to operate in European competitively. These regulations would largely apply to large U.S. platforms and exclude most European competitors.[146]

According to media reports, these proposals will operate under the assumption that restoring "competitiveness" to Europe's digitally enabled markets requires outright prohibitions of certain types of conduct (e.g. so-called "self-preferencing"), structural separation obligations ("line of business restrictions"), and even opening up assets and infrastructure to less capable rivals (access obligations), helping European companies piggy-back off rivals' innovations and investments. In December, the Commission is expected to present its "Digital Markets Act" (a combination of both "ex ante" regulation and new digital market-only investigation and remedy powers, originally intended to apply horizontally as a "New Competition Tool", or "NCT"). It is possible that other jurisdictions will follow the European approach to restricting the competitive threat of U.S. companies.

If implemented, these reforms would push competition law in a new direction towards a structural approach that favors smaller European competitors while ignoring the dynamic competition that takes place, the consumer welfare generated by the existing framework, and the innovation and investment incentives necessary to generate future technological breakthroughs.

Industry also reports that app-based services also face additional barriers aimed at protecting incumbents, infringing on EU established principles on freedom of establishment, equality, non-discrimination, and access to profession. Despite the EU's own acknowledgement of these

[144] 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/.

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

[146] For additional context, CCIA's comments to the EU consultation are available at https://www.ccianet.org/2020/09/ccia-responds-to-public-consultation-on-eu-proposal-for-a-new-competition-tool/.

discrepancies,[147] the enforcement of these principles has not taken place. This deters new entrants and lowers the quality of services provider to customers.

Digital Taxation

Since the introduction of a now-abandoned, digital services tax by the European Commission in 2018, national measures have proliferated on a global scale.[148] Many countries have used the original EU proposal in many respects 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.

The EU has indicated that it will once again pursue an EU-wide digital tax in 2021 if the OECD does not reach an agreement by 2020.[149] Some EU policymakers have also indicated that a digital tax could be tied with any economic recovery plans.[150] CCIA has raised further concerns about the EU's plans on pursuing a DST once again in 2021 in USTR's pending Section 301 Investigation into various DSTs.[151]

For background, the European Commission presented a package of two digital tax proposals in March 2018.[152] 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 percent of companies' gross revenues from making available advertisement space, intermediation services, and transmission of user data.[153] As explained in other country sections of these comments, national DSTs largely reflect this framework, with variations on rate and covered digital activities.

Online Content Regulations

The Commission has announced a forthcoming "Digital Services Act" (DSA), which will further depart from transatlantic norms on liability for online services.[154] New rules will be considered for illegal content, counterfeiting, collaborative economy services, but also hate speech,

---

[147] EUROPEAN COMMISSION, *Study on passenger transport by taxi, hire care with drive and ridesharing in the EU* (2016), *available at* https://ec.europa.eu/transport/sites/transport/files/2016-09-26-pax-transport-taxi-hirecar-w-driver-ridesharing-final-report.pdf.

[148] *Supra* p. 10.

[149] Ryan Heath, *EU pushing ahead with digital tax despite U.S. resistance, top official says*, POLITICO (June 23, 2020), https://www.politico.com/news/2020/06/23/eu-digital-tax-united-states-336496.

[150] Matt Schruers, *To Fund Emergency Measures, Tax Collectors Tap Tech*, DISRUPTIVE COMPETITION PROJECT (May 18, 2020), https://www.project-disco.org/21st-century-trade/051820-to-fund-emergency-measures-tax-collectors-tap-tech/.

[151] *CCIA DST Comments*, *supra* note 30.

[152] *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.

[153] See CCIA's 2018 NTE Comments for full criticism of the EU's DST, *available at* http://www.ccianet.org/wp-content/uploads/2018/10/CCIA-Comments-to-USTR-for-2019-NTE.pdf at 50.

[154] CCIA's comments to the EU regarding the consultation are available at https://www.ccianet.org/library-items/ccias-submission-to-the-eu-dsa-consultation/.

disinformation, or product safety. The Commission wants to "set global standards which could be promoted at international level."

Based on discussion documents released, the DSA could create new obligations such as due diligence obligations: notice & action, 'know your business customer', transparency of content moderation, and cooperation with authorities. There could also be increased requirements on the transparency of recommender systems and advertising. Large online platforms may also have enhanced obligations on reporting and data access, audit, and co-regulation. The Commission is expected to present its DSA package on December 2, 2020.

The EU is also currently negotiating over a Regulation aimed at reducing the dissemination of terrorist content online[155] which might include filtering requirements and a shot-clock deadline for content removal. The proposal is principally aimed at U.S. firms, not all of which have the capacity to meet such a burden. EU policymakers will have a fifth inter-institutional meeting ("trilogue") on October 29, 2020 to discuss the EU proposal. The German Council Presidency hopes to reach an agreement by the end of the year.

This initiative 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 all platforms "to ensure that they are not misused for the dissemination of terrorist content online" with a requirement to take proactive measures "depending on the risk of terrorist content being dissemination" on each platform; and impose strong financial penalties up to 4 percent of global turnover in case of "systematic failures to remove such content following removal orders".

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.[156] CCIA is also advocating for a clear definition of terrorist content to avoid any legal uncertainty or instrumentalization 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. While policymakers have global platforms in mind, this new law could put a lot of burden on small and medium-sized players. Some might not have the resources needed to comply which could force them out the EU market.

[155] *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.

[156] *See* https://www.ccianet.org/wp-content/uploads/2020/09/2020-09-21-TCO-joint-letter-ahead-of-the-4th-trialogue-negotiations.pdf.

Copyright Liability Regimes for Online Intermediaries

On May 17, 2019, the Copyright Directive was published in the Official Journal of the European Union.[157] 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 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 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. Some have noted that 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 inaccurate for two reasons. First, while the text itself does not explicitly "ban memes," the effect of the actions 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, with many Member States in final stages of legislation.

As Member States craft legislation and guidance, 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

[157] Directive (EU) 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) 92, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:130:FULL&from=EN.

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 for Article 17 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. The European Commission is expected to provide guidelines to the Member States on their implementation of Article 17 by the end of the year.

Imbalanced Copyright Laws and "Link Taxes"

CCIA remains concerned with the Copyright Directive on Article 15 and the creation of a press publishers' right.[158] 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 offering such services.

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

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 2019. The press can request money from platforms when they display their content online. Following this development, Google announced on September 25, 2019 that it would change the way articles appear in search results instead of signing licensing agreements.[159] On October 2, 2019, the French competition authority opened an investigation on Google in relation to conduct aimed at complying with the French law transposing the Copyright Directive, and in April 2020, the competition authority ordered Google to pay French publishers under the new law.[160] After weeks of negotiations, Google and the "Alliance de la Presse d'Information Générale", which represents newspapers such as Le Monde, announced a breakthrough on October 7.[161] Future

[158] *Id*.

[159] Richard Gingras, *How Google invests in news*, THE KEYWORD (Sept. 25, 2019), https://www.blog.google/perspectives/richard-gingras/how-google-invests-news/.

[160] *France rules Google must pay news firms for content*, REUTERS (Apr. 9, 2020), https://www.reuters.com/article/us-google-france/france-rules-google-must-pay-news-firms-for-content-idUSKCN21R14X.

[161] Foo Yun Chee, *Google poised to strike deal to pay French publishers for their news*, REUTERS (Oct. 7, 2020), https://www.reuters.com/article/us-alphabet-france-publishing/google-poised-to-strike-deal-to-pay-french-publishers-for-their-news-idUSKBN26S33C.

licensing agreements would be based on criteria such as the publisher's audience, non-discrimination and the publisher's contribution to political and general information.

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.[162] The ruling honors EU residents' 'right to be forgotten' (RTBF) without compromising the constitutional rights of citizens outside of the EU. The decision concludes that a service provider subject to the RTBF is not obligated to de-index outside of the EU.[163] 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.[164] Further, a subsequent decision issued in October 2019 authorizing national courts to issue global content takedown injunctions indicates that EU courts may be trending in a direction that would conflict directly with the U.S. 2010 SPEECH Act, which was designed to combat libel tourism abroad.[165]

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.[166] Under the GDPR, the fine for noncompliance with these and other provisions can be up to 4 percent of a company's global operating costs. Putting the onus on companies to respond to all requests in compliance with the "right to be forgotten" ruling and Article 17 of the GDPR is administratively burdensome. For example, popular U.S. services have fielded hundreds of thousands of requests

---

[162] 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.

[163] *Id.* at ¶ 74 ("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).

[164] *Id.* at ¶ 72.

[165] 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").

[166] GDPR art. 17.

since the policy went into effect.[167] 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.

Regulations on Artificial intelligence

The European Commission will adopt a legislative package in Q1 2021 with a stated goal of building an ecosystem that can support the development and uptake of AI across the EU economy and public administration. The Commission's goal is to pool investment in to AI in order to bridge the gap with China and the U.S. The rules may require AI applications to respect European values such as fundamental rights (Charter of Fundamental Rights), human dignity and privacy (GDPR) and subject high-risk AI applications to compliance assessment before they can be deployed in the market. This could create barriers to entry for non-EU AI services and slow down their time-to-market. The EU should be encouraged to focus on reciprocity between U.S. and EU certification/testing methodology and avoid ex-ante conformity assessments in the EU for non-EU AI products.

Cybersecurity Regulations

Secure network and information systems in the EU are needed in order to keep the online economy resilient. The first pillar of the EU cybersecurity strategy is the EU Cyber Security Act, which entered into force in June 2019.[168] It provides a cybersecurity certification framework as part of which the European Commission and the European Union Agency for Cybersecurity (ENISA) will develop and adopt an EU-wide cloud computing cybersecurity scheme by mid-2021. Industry is concerns that this scheme may set market access conditions to favor local providers. The second pillar of the EU strategy is the revision of the Directive on security of networks and information systems (NIS) and the critical infrastructure protection Directive (CI) that could lead to a significant increase indirect oversight on cloud providers in Europe. These measures may constitute technical barriers to trade that would prevent non-EU companies from accessing the EU market.

Restrictions on Cloud Services

The EU has released a proposal to regulate how EU banks and other financial companies use cloud services. This is part of a package of measures to help digitize the financial sector and modernize the EU's rulebook for the online market. The package of measures include initiatives to harmonize companies' online defense and regulate digital financial assets. There are also policy strategies on retail payments and capital markets, and addresses concerns about dependence on a small group of U.S. providers. The proposal would create an oversight system designed to preserving the European Union's financial system stability, along with monitoring of

[167] Alex Hern, *Google takes right to be forgotten battle to France's highest court*, THE GUARDIAN (May 19, 2016), https://www.theguardian.com/technology/2016/may/19/google-right-to-be-forgotten-fight-france-highest-court.

[168] *See* https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

operational risks, which may arise as a result of the financial system's reliance on critical outsourced services.

M. 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. Reports continue to show the government's increased use of censorship, website blocking, and mandated content filtering.[169]

In May 2020, Egypt's top media regulator issued Decree no. 26 of 2020 that enforces a strict licensing regime on Media and Press outlets.[170] This includes online platforms. Under the regulation, there is a 24-hour timeline for removing harmful content. Further, international companies are obligated to open a representative office within country, while naming a liable legal and content removal point of contact. There are no safe harbor protections for foreign companies, and the regulation stipulates an average of $200k in licensing fees (which could conflict with the existing Media law of 2018). Companies must comply by November 16, 2020, extended from the previous date of September 16, 2020.

Additional E-Commerce Barriers

Industry reports a number of inconsistencies, subjectivity, and lack of clarity regarding import processes 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 register. This largely restricts smaller e-commerce sellers from expanding in the market.

N. 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.[171] Previously, French officials indicated that filters would be required under implementing legislation.[172] The proposal does not appear to reflect even the text of the Directive, omitting mention of protection of exceptions and limitations, the principle of proportionality, or that the actions required by the liability standard cannot amount

---

[169] *Freedom on the Net 2020: Egypt* (2020), https://freedomhouse.org/country/egypt/freedom-net/2020 ("At the end of the first quarter of 2020, 546 websites were reported blocked by the authorities.").

[170] *The New Press and Media Regulation Era in Egypt*, LEXOLOGY (May 16, 2020), https://www.lexology.com/library/detail.aspx?g=36e4982b-40ef-4fb5-9ee6-f4912a7271ac.

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

[172] 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-requirefilters-france-immediately-starts-promoting-filters.shtml.

to a duty to monitor. 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.[173] Instead, there is only an obligation to inform users about relevant exceptions in terms and conditions.

Government-Imposed Content Restrictions and Related Access Barriers

In March 2019, the National Assembly proposed a very broad law on combating hate speech ("*Lutte contre la haine sur internet*").[174] The law would require designated Internet services to take down hateful comments reported by users within 24 hours. The law targeted 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 percent of their global revenue and penalties could reach tens of millions of euros.

The French National Assembly adopted the law on May 13, 2020. However, the French Constitutional Court released a decision pertaining to the constitutionality of the new law on June 18, 2020.[175] The Court determined the legislation "undermines freedom of expression and communication in a way that is not appropriate, necessary and proportionate to the aim pursued" making the text not compatible with the French constitution. The French law required platforms to take down manifestly illegal content upon notification within 24 hours. Among others, the law targeted any hateful attack on someone's "dignity" on the basis of race, religion, sexual orientation, gender identity or disability.[176] The Court also struck down the one-hour removal deadline for terrorist propaganda and child pornographic contents as it contradicts the French Penal code (Art 227-3 and 421-2-5).

Digital Taxation

On July 24, 2019 French legislation implemented a 3 percent tax on revenue generated in France derived from digital intermediary services and digital advertising services.[177] 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.[178] French Government sites and representatives of

[173] *Article 17: Both French and Dutch implementation proposals lack key user rights safeguards*, COMMUNIA (Jan. 10, 2020), https://www.communia-association.org/2020/01/10/article-17-implementation-french-dutch-implementation-proposals-lack-key-user-rights-safeguards/.

[174] Lutte contre la haine sure internet, Assemblee National, http://www.assembleenationale.fr/dyn/15/dossiers/lutte_contre_haine_internet.

[175] Conseil constitutionnel [CC] [Constitutional Court] decision No. 2020-801DC, June 18, 2020 (Fr.), *available at* https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm.

[176] *See* Press Release, CCIA, Court Ruling Rejects Core of French Hate Speech Law (June 18, 2020), https://www.ccianet.org/2020/06/court-rules-rejects-core-of-french-hate-speech-law/.

[177] 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"].

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

the French National Assembly and Senate refer to the French DST as a "GAFA" tax and cite specific American companies in reports.[179] Based on French officials' own admission, the majority of firms that will pay the tax will be American.[180]

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. CCIA supported the agreement made by the U.S. and France to pause collection on the DST at the beginning of 2020. However, with the OECD's continued deliberation of a global solution into 2021, France has made clear that it will begin collecting on the DST prior to a global solution.

Data Localization

France first indicated that it will direct resources to build a national "trusted cloud" in 2019.[181] 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.[182]

As noted in the EU section of these comments, France and Germany released a joint statement on October 29, 2019 indicating their commitments to collaborate on a European data

[179] *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 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.]).

[180] Boris Cassel & 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-numerique-une-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.].

[181] 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.").

[182] *Id.*

infrastructure.[183] This serves as a protectionist barrier for U.S. cloud service providers in the public sector in France.

O. 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.[184] The NetzDG law mandates removal of "manifestly unlawful" content within 24 hours, and provides for penalties of up to 50 million euros.[185] 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 unlawful content"[186] have led to companies removing lawful content, erring on the side of caution in attempts to comply.[187] 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[188] and groups have expressed concerns about its threats to free expression.[189]

Further concerning is the potential domino effect of this policy on other regimes. This law has been used as the basis for a number of concerning content regulations including legislation in

---

[183] 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_%20FrancoGerman%20Collaboration%20on%20Data%20In.%20w%20logo_.pdf.

[184] 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-fortechcompanies-c352efbbb993.

[185] Id. § 3(2).

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

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

[188] 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-complaintsidUSKCN1TX1IC.

[189] *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.").

Russia, Singapore, Turkey, and Venezuela.[190] Cases arising under this law will also have implications on extraterritoriality.[191]

In a 2020 review of the law, the German government has acknowledged flaws and needs for improvement.[192] In June 2020, there were further amendments proposed.[193]

Data Localization

The German Economy Minister announced in 2019 that they were working on a plan to create Europe's own cloud services, titled "GAIA-X".[194] This project would connect existing central and decentralized infrastructure solutions via open source applications and interoperable solutions. France and Germany released a joint statement on October 29, 2019 indicating their commitments to collaborate on a European data infrastructure. U.S. cloud service providers could be disadvantaged from operating in these markets as a result of these protectionist measures.

Asymmetry in Competition Frameworks

Germany is currently in the process of reforming its competition rules, with a draft bill introduced in 2020.[195] 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." 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.

---

[190] Jacob Mchangama & Natalie Alkiviadou, *The Digital Berlin Wall: How Germany built a prototype for online censorship*, EURACTIV (Oct. 8, 2020), https://www.euractiv.com/section/digital/opinion/the-digital-berlin-wall-how-germany-built-a-prototype-for-online-censorship/.

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

[192] Bundesministerium der Justiz und für Verbraucherschutz, Evaluierungsbericht zum Netzwerkdurchsetzungsgesetz (NetzDG) vorgelegt (Sept. 9, 2020), https://www.bmjv.de/SharedDocs/Artikel/DE/2020/090920_Evaluierungsbericht_NetzDG.html.

[193] Madeline Earp, *Germany revisits influential internet law as amendment raises privacy implications*, COMMITTEE TO PROTECT JOURNALISTS (Oct. 7, 2020), https://cpj.org/2020/10/germany-revisits-influential-internet-law-as-amendment-raises-privacy-implications/

[194] 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-aeuropean-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-imoktober/24974718.html.

[195] *Updating German Competition Rules for Big Players in the Digital Economy*, BEITEN BURKHARDT (Sept. 23, 2020), https://www.lexology.com/library/detail.aspx?g=de3a20dd-20c9-4da0-86a4-11c57cfe70f2.

P. India

India is a region of continued concern for U.S. Internet exporters. India has an increasingly vibrant e-commerce market, illustrated by the high value of digital exports and imports.[196] 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 fourth consecutive year.[197] However, the government has continued to pursue a digital agenda that undermines this growing potential. New regulations on data localization, protectionist policies that would mandate data access to competitors, and taxation plans ultimately hinder global trade flows.

Digital Taxation

In March 2020, the Indian Parliament expanded the scope of India's existing "equalization levy" in its amended national 2020 Budget.[198] This included a new 2 percent tax on the sale of goods and services by non-Indian companies over the Internet into India. A wide range of companies are required to pay this tax, given the broad definition of those in scope. Without any public consultation, the tax was set to apply beginning April 1, 2020.

While structurally different from DSTs from European countries, the tax is similarly concerning insofar as it discriminates against U.S. firms and exempting local businesses. Under the tax, "e-commerce operators" are defined as "non-residents who own, operate or manage a digital or electronic facility or platform for online sale of goods, online provision of services, or both". Pursuant to this definition, the scope is far broader than DSTs such as those in Europe. Further the threshold is set at approximately $267,000 compared to the 750 million euro global threshold.

As a number of industry groups observed (including CCIA), the Indian tax represents the broadest framing of a unilateral tax on e-commerce firms, and runs directly counter to the Indian Government's commitment to reaching a multilateral solution in ongoing negotiations at the OECD on the taxation challenges of digitalization to the global economy.[199]

---

[196] 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.").

[197] *Ease of Doing Business in India*, THE WORLD BANK, https://www.doingbusiness.org/en/data/exploreeconomies/india (last accessed Oct. 27, 2020).

[198] *India: Digital Taxation, Enlarging the Scope of 'Equalisation Levy'*, KPMG (Mar. 24, 2020), https://home.kpmg/us/en/home/insights/2020/03/tnf-india-digital-taxation-enlarging-the-scope-of-equalisationlevy.html.

[199] *Global Lobbying Groups Call for Delay To India's New Digital Tax*, REUTERS (Apr. 29, 2020), https://www.reuters.com/article/us-india-tax-digital/global-lobbying-groups-call-for-delay-to-indias-new-digital-taxidUSKCN22B0EL.

The new equalization level follow previous protectionist tax measures in India against foreign digital services. In 2016, the government introduced a 6 percent level on foreign digital advertising businesses. The government also proposed the concept of "significant economic presence" in 2018, but deferred implementation until there was international consensus on this question.

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.[200] 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 NTE comments.[201] The climate for market access continues to decline with additional proposals that are in deep conflict with global best practices on data protection and data localization. Below are key developments for U.S. services in the region.

The Personal Data Protection Bill (PDPB), introduced in December 2019, remains under consideration in India by a Joint Committee in Parliament. CCIA has raised concerns with the following aspects of the current draft: the scope of the PDPB's data portability requirements (Section 19), proposed restrictions on transferring personal data outside India (Chapter VII), issues regarding the independence of the proposed Data Protection Authority (outlined in Chapter IX), and the proposed authority for the Central Government to compel the production of anonymized or non-personal corporate datasets for formulating policy or targeting services (Section 91).[202]

The Bill would introduce extensive localization requirements on "sensitive personal data" which is broadly defined to include routinely processed financial and other business data. Cross-border transfers of this data would only be permitted under narrow legal basis. Localization requirements for "critical personal data" are stricter, with even narrower allowances for cross-border transfer. "Critical personal data" would be prescribed by the central government. Given

[200] DEP'T FOR PROMOTION OF INDUSTRY & 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.").

[201] *2019 CCIA NTE Comment*, *supra* note 95.

[202] See CCIA Comments on the Personal Data Protection Bill, 2019 (Feb. 24, 2020), https://www.ccianet.org/wp-content/uploads/2020/02/2020-02-24-CCIA-Comments-on-Personal-Data-Protection-Bill.pdf.

the uncertainties and open-ended definitions of data categories, the PDPB risks serious impediments to cross-border trade.

The Ministry of Electronics and Information Technology is also currently considering a Report by the Committee of Experts on Non-Personal Data Governance Framework released in August 2020. The proposed Framework would require mandatory sharing and access to aggregated data held by private companies, and compel industry to share this data with competitors and government agencies. This would pose conflicts with obligations under international commitments relating to IP and trade secrets protection by mandating disclosure of protected and business confidential information. Further, the Framework would impose additional localization mandates and disclosure requirements. A wide coalition of industry has raised concerns with these recommended measures that would "create powerful disincentives for India's innovation ecosystem."[203]

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.[204] Reports as of April 2020 suggest that the government is in the final stages of notifying these amendments.[205]

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).

Additional E-Commerce Barriers

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 on cross-border data flows and restrictions on foreign direct investment. The development of the draft policy had significant process and representation concerns. CCIA outlined concerns with the policy in 2019, with particular attention to extensive new data and infrastructure localization mandates, requirements to transfer source code and other proprietary data based on flawed assumptions of data, and preferential treatment for local

[203] Global Industry Statement on Non-Personal Data Report (Sept. 18, 2020), https://www.ccianet.org/wp-content/uploads/2020/09/Global-Industry-Statement-on-Non-Personal-Data-Report-final.pdf.

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

[205] Surabhi Agarwal, *Government set to notify new social media norms*, THE ECONOMIC TIMES (Apr. 9, 2020), https://economictimes.indiatimes.com/tech/internet/government-set-to-notify-new-social-media-norms/articleshow/75059440.cms.

competitors.[206] Reports suggest that the revised framework retains concerning provisions that would negatively impact U.S. services including proposed regulations on required data access and competition, anti-counterfeiting and other revisions to intermediary liability law, and forced localization and related measures.[207]

Regulations on Cloud Services

In September 2020, the Telecom Regulatory Authority of India released recommendations on a Regulatory Framework for Cloud Service Providers (CSPs).[208] This proposal will be sent to the Department of Telecommunications to decide whether to make these recommendations binding. The recommendations include (1) mandatory enrollment of all CSPs with a government-controlled industry body, (2) government oversight on the industry body, including the ability to issue directions, rules and standards, and to cancel registrations of "errant" CSPs, and (3) an exemption for channel partners and SaaS businesses, who may voluntarily enroll in these industry bodies. Failure to comply with the requirements could cause telecom service providers will be disallowed from providing these CSPs with infrastructure services.

Q. Indonesia

Digital Taxation

In March, Indonesia introduced tax measures targeting digital services as part of an emergency economic response package. One of these taxes applies to e-commerce transactions carried out by foreign individuals or digital companies with a significant economic presence. Per reports, the significant economic presence will be determined through the companies' gross circulated product, sales and/or active users in Indonesia.[209] Companies determined to have a significant economic presence will be declared permanent establishments and as a result subject to domestic tax regulations.[210] If this determination of permanent establishment conflicts with an existing treaty, such as the U.S.-Indonesia tax treaty, then a new "electronic transaction tax" (ETT) would apply to income sourced from Indonesia.[211] While structurally different from DSTs from European countries, the tax is similarly concerning insofar as it looks to increase U.S. firms' tax

[206] CCIA Comments on Draft National e-Commerce Policy: India's Data for India's Development (Mar. 29, 2019), https://www.ccianet.org/wp-content/uploads/2019/03/CCIA-Comments-on-India-National-E-Commerce-Strategy.pdf.

[207] Aditi Agrawal, *India's new draft e-commerce policy focuses on data, competition, counterfeiting, consumer protection*, MEDIANAMA (July 3, 2020), https://www.medianama.com/2020/07/223-second-draft-ecommerce-policy-india/. Industry also reports that the current draft makes the following recommendations on localization: (i) certain categories of data such as defense, medical records, biological records, cartographic data, and genome mapping data should not be transferred outside India; (ii) certain categories of e-commerce data should be mirrored/stored in India (with the government/a proposed e-commerce regulator deciding the categories).

[208] Press Release, Telecom Regulatory Authority of India, Recommendations on 'Cloud Services' (Sept. 14, 2020), *available at* https://trai.gov.in/sites/default/files/PR_No.70of2020.pdf.; *TRAI Recommends Industry-Led Body for Cloud Service Providers*, MEDIANAMA (Sept. 17, 2020), https://www.medianama.com/2020/09/223-trai-cloud-service-providers/.

[209] *Indonesia Taxes Tech Companies Through New Regulation*, THE JAKARTA POST (Apr. 1, 2020), https://www.thejakartapost.com/news/2020/04/01/indonesia-taxes-tech-companies-through-new-regulation.html.

[210] *Id.*

[211] *Indonesia Government Proposes Key Tax Changes*, EY (Mar. 19, 2020), https://taxnews.ey.com/news/2020-0604-indonesian-government-proposes-key-tax-changes

payments in the region by departing from longstanding international taxation norms. U.S. companies were cited as targets of these tax measures.[212] Governments should be discouraged from pursuing discriminatory taxes on foreign companies to fund economic response measures.[213]

Customs Duties on Electronic Transmissions

Indonesia issued Regulation No.17/PMK.010/2018 (Regulation 17) in 2018.[214] 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[215] and most recently reaffirmed in December 2019.[216] 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 during the 12th WTO Ministerial Conference scheduled to be held next year. Indonesia must rescind Regulation 17 and remove Chapter 99 from its HTS.

Backdoor Access to Secure Technologies

Indonesia established a new cybersecurity agency in 2018 — the National Cyber and Encryption Agency — and is expected 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 new Agency.[217] The planned approach appears to follow authoritarian cybersecurity models such as those of China and Russia.

Restrictions on Cross-Border Data Flows

The Government of Indonesia introduced Government Regulation 71/2019 to revise the previous Government Regulation 82/2012. While it represents slight progress, concerns for U.S. services remain and data localization mandates are retained. In the GR 71/2019 draft implementation

---

[212] *Indonesia Defends Digital Tax Policy Despite US Scrutiny*, THE JAKARTA POST (June 16, 2020), https://www.thejakartapost.com/news/2020/06/16/indonesia-defends-digital-tax-policy-despite-us-scrutiny.html.

[213] *To Fund Emergency Measures, Tax Collectors Tap Tech*, *supra* note 150.

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

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

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

[217] *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-oncyber-security-before-passing-it-into-law-122342 (providing an overview of the draft legislation and background of the process).

regulations,[218] storing and processing of data offshore by any "Electronic Systems Providers (ESPs)" will require prior approval from the government.[219] These requirements present market access barriers for foreign services when delivering products and services online.

GR 71/2019 provides great visibility on its data localization policy, the implementing regulations continue to be a significant barrier to digital trade and inhibit the ability of U.S. firms to participate in the e-commerce market in Indonesia. The definition of Public Scope ESPs includes public administration, which goes beyond nationals security and intelligence data. There is no further clarity regarding the circumstances by which data can be stored and process offshore in the case of Public Scope ESPs, including the guidelines that the Minister of Communications and Informatics will use when reviewing every data offshoring required by Privacy Scope ESPs. U.S. firms have lost, and will continue to lose business in Indonesia due to the ambiguity in the data localization requirements.

While GR 71 represents a progress towards reforming Indonesia' data localization policy and further digital trade, these reforms risk being undermined by other existing policies that are incongruent with the GR 71 umbrella regulation.[220] For example, data localization policies remains in place for banking and financial sectors despite the possibility of Private Scope ESPs to store and process data offshore under GR 71. Further, GR 71 establishes an interagency committee to set up and oversee the exception for Public Scope ESPs to store and process data offshore. Industry reports concerns with the limited progress on the finalization of the GR 71 implementing regulations, which creates business uncertainty and increased compliance risks.

Indonesia is also considering its Personal Data Protection bill which, as drafted, differentiates the responsibilities between data controllers and data processors, drawing from the EU's GDPR. Data transfer across borders is limited to countries which have equivalent standards of data protection, however there are no guidelines on assessing the level of data protection across countries. The bill would also impose extraterritoriality as its cross-jurisdictional basis, again similar to GDPR.

The Minister of ICT intends to release a Regulation on the Governance of Privacy Electronic System Operators by October 2020, which imposes a requirement for companies in Indonesia to submit government preapproval prior to storing and process data offshore.

Indonesia's Government Regulation No. 80/2019 on E-Commerce distinguishes between domestic and foreign e-commerce business actors, and also prohibits personal data from being sent offshore unless otherwise approved by the Ministry of Trade.[221] This effectively requires e-commerce business actors to locally store personal data for e-commerce customers. Trade

[218] "Communications & Informatics Ministerial Regulation on the Governance of Electronic Systems Providers for Private Scope."

[219] *Draft regulation may require all local and foreign websites and apps to register with MOCI*, LEXOLOGY (Apr. 8, 2020), https://www.lexology.com/library/detail.aspx?g=9ae4aa21-dcb0-4c26-8e68-840f483873f6.

[220] *Indonesia: New Regulation on Electronic System and Transactions*, BAKER MCKENZIE (Oct. 28, 2019, https://www.bakermckenzie.com/en/insight/publications/2019/10/new-regulation-electronic-system-and-transactions

[221] *Indonesia issues e-commerce trading regulation*, EY (Jan. 15, 2020), https://www.ey.com/en_gl/tax-alerts/ey-indonesia-issues-e-commerce-trading-regulation.

Regulation 50/2020 on E-Commerce, an implementing regulation of GR 80, also requires e-commerce providers to appoint local representatives if it has over 1,000 domestic transactions annually, promote domestic products on their platform, and share corporate statistical data to the government. Both GR 80 and TR 50 pose *de facto* data localization measures and local content requirements, which increase overhead costs for foreign entities and create undue market barriers.

Indonesian financial services are still blocked from using offshore data centers. The Bank of Indonesia still requires financial payment to be processed domestically. The Financial Services Authority (OJK) has incrementally allowed some electronic systems to be processed offshore in the banking and insurance sector, but this has not been permitted in sectors including multi-financing and lending based technology. Industry reports these rules are motivated in part by of regulators lack of trust in multilateral law enforcement systems.

Additional E-Commerce Barriers

Government Regulation 80/2019 on Electronic Commerce (followed by Trade Minister Regulation No. 50/2020) requires that any e-commerce provider that meets a certain threshold[222] to set up or appoint a local trade representative to act on behalf of the foreign entity. This representative is required to handle consumer protection promotion of domestic products, and dispute resolution within the country. This effectively requires U.S. businesses to establish a local presence which triggers unintentional tax consequences. Indonesia should consider alternative measures to ensure consumer protection without mandating local presence for digital products and services.

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 further logistics is limited to 67 percent, provided that each of these services is not ancillary to the main business line. Legislation is scheduled to take effect in November 2020 that aims to add clarity for e-commerce firms.[223]

Indonesia's Ministry of Industry issued regulation No. 22/2020 (IR22) on the Calculation of Local Content Requirements (LCR) for Electronics and Telematics. Industry reports that the regulation is motivated by the government's target to achieve 35 percent import substitution by 2025, which will force U.S. companies to use local manufacturing partners. IR22 provides specific and extensive requirements for manufacturing and development for both digital and non-digital physical products. The policy will have an additional administrative burden to physical ICT products that are needed for ICT companies to operate in Indonesia. This regulation could

[222] More than 1000 transactions or more than 1000 delivery packages in one year.

[223] Michael S. Carl & Asri Rahimi, *Indonesia: Indonesia Introduces New Requirements For E-Commerce Companies*, MONDAQ (June 22, 2020), https://www.mondaq.com/corporate-and-company-law/956332/indonesia-introduces-new-requirements-for-e-commerce-companies ("MOT Regulation No. 50 of 2020 regarding Provisions on Business Licensing, Advertising, Guidance and Supervision of Businesses Trading Trade through Electronic Systems ("**MOT Reg. 50/2020**"). It is an implementing regulation for Government Regulation No. 80 of 2019 regarding Trading through Electronic Systems ("**GR 80/2019**"). MOT Reg. 50/2020 was issued on May 19, 2020 and will take effect on November 19, 2020.").

lead to an importation threshold for ICT equipment. Industry reports that the government has also signaled intention to build on this LCR requirement and add similar LCRs for software and applications, which will become a primary blocker for digital platform companies that provide services over the internet. The Government plans to introduce a draft by end of 2020.

R. Italy

Digital Taxation

Italy's 2020 Budget introduced a 3 percent digital services tax closely aligned with the EU's original proposal.[224] Covered services started accruing tax on January 1, 2020, and payments are due in 2021. The global revenue threshold is set at 750 million euros, and the local threshold is 5.5 million euros. The tax applies to revenue derived from the following digital activities: (1) the "provision of advertising on a digital interface targeted to users of the same interface"; (2) the "provision of a digital multilateral interface aimed at allowing users to interact (also in order to facilitate the direct exchange of good and services)"; and (3) the "transmission of data collected from users and generated by the use of a digital interface".[225]

The tax is expected to predominantly affect U.S. firms. 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.[226] It appears that this remains the case with the current tax.

S. Japan

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

As noted in CCIA's 2019 comments,[227] the Japanese Ministry of Communications is considering changes to expand application of its telecommunications law to foreign services. A bill was submitted to the Japanese Diet in February 2020.[228] These changes are expected to oblige foreign over-the-top (OTT) services using third-party facilities (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 obligations under its Telecommunications Business Act.

---

[224] Italy included a digital tax in the Italian Budget Law 2019 (Law no.145/2018), but never took the final steps to implement the tax.

[225] *Tax Alert: Italy Digital Services Tax Enters into Force*, EY, https://www.ey.com/en_gl/tax-alerts/ey-italys-digital-services-tax-enters-into-force-as-of-1%C2%A0january-2020 (last accessed Oct. 27, 2020).

[226] *Web tax in arrivo*, ADNKRONOS (Dec. 19, 2018), https://www.adnkronos.com/soldi/economia/2018/12/19/web-tax-arrivodi-maio-rassicura-solo-per-gigantirete_JEfFksy3wkwzPPJaG7vxuI.html.

[227] CCIA 2019 NTE Comments, *supra* note 201.

[228] *Japan - Amendments to expand application of Telecoms law to overseas IT companies*, BAKER MCKENZIE (June 3 2020), https://www.lexology.com/library/detail.aspx?g=504e9814-cffa-4545-9a85-1635758230b6

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 and a number of documents were released in 2020.[229]

"Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc." were finalized on December 17, 2019.[230] These Japan Fair Trade Commission Guidelines look to address and provide clarity regarding the application of "abuse of superior bargaining position" to business-to-consumer transactions regarding online platforms including treatment of personal information.

The Headquarters for Digital Market Competition in Japan also published an interim report in 2020 on "Competition in the Digital Advertising Market".[231] There are concerns with the mischaracterizations that the Interim Report contains regarding the digital advertising industry and possible regulatory action that the DMCH might pursue to address the purported challenges.[232]

T. Kenya

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

A new ICT Policy was released in August 2020, which includes a clause on "equity participation".[233] The policy proposes an increase to 30 percent of the local ownership rules, currently set at 20 percent. The requirement would take effect in three years. If these provisions were enacted, only firms with 30 percent "substantive Kenyan ownership" would be licensed to provide ICT services. Additionally, the ICT Policy requires that Kenyan data remains in Kenya, and that it is stored safely and in a manner that protects the privacy of citizens. This provision conflicts with the 2019 Data Protection Act, which enables cross-border data transfers subject to conditions set out by the Data Commissioner. The Data Commissioner has still not been appointed almost a year after the Act was written into law, adding to regulatory uncertainty.

---

[229] *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.

[230] English translation available here: https://www.jftc.go.jp/en/pressreleases/yearly-2019/December/191217DPconsumerGL.pdf.

[231] English summary is available at https://www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_200616.pdf.

[232] *See* CCIA Comments on the Interim Report on Evaluation of Competition in the Digital Advertising Market from the Headquarters for Digital Market Competition of the Cabinet Secretary (July 25, 2020), https://www.ccianet.org/wp-content/uploads/2020/10/Final-CCIA-Comments-to-DMCHs-Interim-Report.pdf.

[233] *See Publication of the National Formation Communication and Technology Policy Guidelines, 2020*, BOWMANS LAW (Sept. 1, 2020), https://www.bowmanslaw.com/insights/technology-media-and-telecommunications/publication-of-the-national-information-communication-and-technology-policy-guidelines-2020/.

U. Korea

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

The Ministry of Science & ICT is currently considering regulations made pursuant to amendments to the Telecommunications Business Act passed earlier this year.[234] There are concerns that the new rules would impose impractical obligations on foreign services, and certain provisions may conflict with Korea's trade commitments to the United States.

The rules would subject predominantly U.S. Internet services to disproportionate levels of risk and responsibility regarding network management outside their practical control. The proposed rules inappropriately shift the burden for several responsibilities pertaining to network management to "value-added telecommunications service providers" (VTSPs), even though they lack the technical or information capabilities to control end-to-end delivery of the content. Internet service providers who control the network infrastructure and management remain the most adept to primarily control service reliability. These changes could also lead to unbalanced bargaining positions resulting in discriminatory or anti-competitive behavior by ISPs to the detriment of VTSPs, which could lead to demands for increased usage fees or other contractual conditions. Further, the new requirements as currently drafted lack sufficient clarity for VTSPs, which could increase the risk of legal disputes and pose problems for implementation and enforcement.

The Korean government continues to maintain a protectionist stance to keep global cloud service providers out of the local public sector market through the Korea Internet & Security Agency (KISA) Cloud Security Assurance Program (CSAP). Industry reports that the four main technical requirements that has prevented all global CSPs from being able to obtain the CSAP: (1) physical separation; (2) Common Criteria (CC) certification; (3) vulnerability testing; and (4) use of domestic encryption algorithms.

Through these onerous requirements that department from international standards, the CSAP effectively casts technical blockers to trade and prohibits global CSPs from accessing public sector workloads in Korea. The government has also begun requiring CSAP in other sectors, such as in healthcare, with the Ministry of Health and Welfare (MOHW)'s recent inclusion of the CSAP as a requirement for Electronic Medical Record (EMR) system providers who seek to use public cloud services. While MOHW claims that the CSAP is not mandatory, it plans to provide medical insurance reimbursement premiums only to medical institutions with certified EMR systems, thus creating an unleveled playing field for companies who are unable to obtain the CSAP.

[234] Kim Eun-jin, *Enforcement Decree of 'Netflix Law' Feared to Hurt Korean Internet Companies*, BUSINESSKOREA (Sept. 9, 2020), http://www.businesskorea.co.kr/news/articleView.html?idxno=51497.

Government-Imposed Content Restrictions and Related Access Barriers

Rules announced in 2019 by the Korean Communications Commission will enable officials to filter online content and block websites based outside the country.[235] While in the pursuit of enforcing existing laws regarding illegal content, some have raised concern that it follows authoritarian models of Internet regulation.[236]

V. Mexico

Digital Taxation

On September 8, 2020, the Secretary of Finance & Public Credit, Arturo Herrera, presented to the Mexican Congress the legislative project for the Government's Budget for 2021. Included in the proposal is the implementation of a "kill switch," which is an enforcement mechanism that the Mexican government initially proposed in their 2020 Budget against non-resident entities that do not comply with the application of the VAT on non-resident supplies of digital services to Mexican consumers.

Industry raised concerns with a previous attempt to implement this in 2019,[237] and the kill switch was removed in the previous Budget. However the fact that a limited number of companies registered in the government's regime (35 companies in Mexico, compared to more than 100 in Chile in the same timeframe, due to Mexico's incredibly complex registration process) has led them to reintroduce the measure as a way to force compliance. The proposal would empower the tax authority to work with the telecom regulator to require Internet Service Providers (ISPs) to block Internet access to non-resident entities making cross-border supplies.

Copyright Liability Regimes for Online Intermediaries

Mexico made reforms to its Federal Copyright Law in 2020 in attempts to bring its law in compliance with commitments under USMCA. There are concerns that the text of the provisions implementing Article 20.87-88 of the USMCA inappropriately narrows the application of this framework for Internet services.

Additional E-Commerce Barriers

Mexico published new regulations that increased import rates on shipments from the U.S. and Canada valued between USD $50-117 by 1 percent (from 16 percent to 17 percent). These changes were made without following appropriate protocols or advance notice, and they became effective immediately. Mexico should fully implement its commitments under USMCA's

---

[235] 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"],

[236] *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/.

[237] Industry Letter (Oct. 14, 2019), *available at* https://www.ccianet.org/wp-content/uploads/2019/10/Multi-Association-Letter-on-Mexican-Tax-Issue.pdf.

Customs Chapter, including eliminating the new import rates and implementing an informal clearance threshold for shipments up to USD $2,500.

Industry is tracking proposed financial sector regulations. The National Banking and Securities Commission and the Central Bank of Mexico have issued Draft Provisions Application to Electronic Payment Fund Institutions (IFPEs). Articles 50 and 49 are of most concern to U.S. cloud computing services. The regulations further undermine U.S. financial service providers, who already report lengthy and uncertain approval processes from financial sector regulations in order to use secure U.S.-based cloud computing services. The regulations could also lead to U.S. cloud services being disadvantaged in the region compared to local data center firms.

Article 50 would impose the obligation of data residency and multi-scheme provider to IFPEs that use cloud computing services. Notably, Article 50 of the draft regulation imposes on the IFPEs that use cloud services the obligation of data residency, or alternatively, a multi-provider scheme, once they reach certain transaction thresholds. This proposed Article requires IFPEs that use cloud services to have a secondary infrastructure provider, once they reach certain transaction thresholds. Either this provider must have an in-country infrastructure, or its controlling company must be subject to a different jurisdiction than that of the first cloud provider. A similar data localization requirement is being imposed on financial service providers that have requested to participate in Mexico's national payments system (SPEI), regulated and operated by the Central Bank. Industry reports that financial sector regulators, most notably the Central Bank, have been requiring financial service providers to have data residing in Mexico, and introducing regulatory biases against cloud computing services.

Article 49 would establish an authorization model with a high degree of discretion and lack of transparency for the use of cloud computing services.

These provisions would conflict with the localization principles established in USMCA digital and financial commitments.

Local Content Requirements

In September 2020, Senator Ricardo Monreal presented a legislative proposal that seeks to reform the Federal Telecommunications Act and require a 30 percent local content quota for over-the-top (OTT) platforms operating in Mexico. A local content quota for OTT platforms would violate Mexico's commitments under Articles 14.10 and 19.4.1 of USMCA. Local content requirements also limit free expression and consumer choice, distort the growing audiovisual market, and stifle investment and competitiveness.

The draft bill would also expand the Federal Telecommunications Institute (IFT) licensing requirement for restricted TV and audio services to cover OTT services — even those operating from abroad. Imposing such onerous new licensing requirements on OTT services would be inconsistent with USMCA Article 18.14.1 on applying requirements of public telecommunications to value-added services which are not public telecom services.

W. New Zealand

Digital Taxation

In June 2019, the New Zealand 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.[238] The first option, the national DST, would be a 3 percent 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.

Government-imposed Content Restrictions and Related Access Barriers

In May 2020, the Government introduced the "Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill" into Parliament.[239] There are concerns that the draft legislation includes an overly broad definition of "objectionable content". The bill also contemplates government-imposed content-blocking mechanisms.

X. 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 2021 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.

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

In 2020, the Digital Government Secretariat of Peru released Emergency Decree 007 - Digital Trust Framework draft regulations for consultation.[240] The proposal appears to give preferential

---

[238] TAX POLICY, INLAND REVENUE, *Options for Taxing the Digital Economy: A Government Discussion Document* (2019), http://taxpolicy.ird.govt.nz/sites/default/files/2019-dd-digital-economy.pdf [New Zealand]; Benjamin Walker, *Analysing New Zealand's Digital Services Tax Proposal*, AUSTAXPOLICY (Apr. 23, 2020), https://www.austaxpolicy.com/analysing-new-zealands-digital-services-tax-proposal/.

[239] Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill, https://www.parliament.nz/en/pb/bills-and-laws/bills-proposed-laws/document/BILL_97940/films-videos-and-publications-classification-urgent [New Zealand] (last accessed Oct. 29, 2020).

[240] José Antonio Olaechea, *Doing business in Peru: overview*, THOMSON REUTERS PRACTICAL LAW, https://uk.practicallaw.thomsonreuters.com/0-500-7812?transitionType=Default&contextData=(sc.Default)&firstPage=true (last accessed Oct. 29, 2020).

treatment to domestic data storage and domestic service providers. Industry reports that the draft proposal includes: (1) the creation of a whitelist of permitted countries for cross-border transfer of data, even though the Peruvian Data Protection Law does not include such restrictions; (2) the issuance of digital security quality badges for private companies which will be the governmental cybersecurity certification (ignoring the existence of global security standards); and (3) the creation of a national data center intended to host the information provided by the public sector entities. The proposal also includes broad definitions of digital services providers, failing to consider key differences among digital services and the differences in these services ability to access client's information, or organizations that use digital channels to provide their services. The Data Protection Authority would determine model contract clauses, which appear to exceed what is currently required under the Data Protection Law. The National Data Center would incentivize domestic data storage by providing infrastructure to domestic data center operations, granting the government control over the data.

As noted elsewhere in these comments, the ability to move data and access information across borders is essential for businesses regardless of size or sector. Peru should instead rely on the already approved Guidelines for the Use of Cloud Services for entities of the Public Administration, and endorse the use of international standards and best practices, which are accepted and adopted, such as ISO 9001, ISO 27001, ISO 27002, ISO 27017, ISO 27018 y SOC 1, 2 y3.

Y. Russia

Government-Imposed Content Restrictions and Related Access Barriers

In May 2019, 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.[241]

In March 2019, Russia passed two laws aimed at eliminating "fake news". The Federal Law on Amending Article 15-3 of the Federal Law on Information, Information Technologies and Protection of Information[242] and the Federal Law on Amending the Code of Administrative Violations,[243] establish penalties for "knowingly spreading fake news" and establish a framework for ISPs to block access to websites deemed to be spreading "fake news."[244]

[241] *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-thecountry-from-the-world-wide-web/.

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

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

[244] 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/.

In December 2019, Russia adopted a law that requires the pre-installation of Russian software on certain consumer electronic products sold in Russia and sets a dangerous precedent.[245] The law is due to take effect January 2021. The scope of devices is likely to include smartphones, computers, tablets, and smart TVs, and the scope of applications is likely to include search engines, navigation tools, anti-virus software, software that provides access to e-government infrastructure, instant messaging and social network software, and national payment software.

Z. 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, with revisions made in 2019.[246] The rules contain a provision on data localization that may restrict access to the Saudi market for foreign Internet services.[247] 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.

The National Cybersecurity Authority (NCA) 2018 Essential Cybersecurity Controls (ECC) framework states that data hosting and storage when using cloud computing services must be located with the country.[248] The draft NCA 2020 Cloud Cybersecurity Controls (CCC) framework requires operators to provide cloud computing services from within country, including all systems including storage, processing, monitoring, support, and disaster recovery centers. The requirement applies to all levels of data.[249] Neither the ECC, nor the draft CCC, distinguish between data localization requirements for different levels of data classification, which conflicts with the 2018 Cloud Computing Regulatory Framework (CCRF).[250]

---

[245] *Russia passes law forcing manufacturers to install Russian-made software*, THE VERGE (Dec. 3, 2019), https://www.theverge.com/2019/12/3/20977459/russian-law-pre-installed-domestic-software-tvs-smartphones-laptops.

[246] *Saudi Arabia's cloud computing regulatory framework 2.0*, LEXOLOGY (Mar. 1, 2020), https://www.lexology.com/library/detail.aspx?g=f32fe934-c8f6-4a99-acc8-f5dd50342c53.

[247] *Id.* ("With regard to cloud computing, the ECC:2018 requires entities subject to its requirements to ensure that the hosting and storage of their data occurs in Saudi Arabia. This seems to be a very broad restriction on the use of cloud services based outside the Kingdom, and it is likely to have a significant impact on the cloud market in Saudi Arabia. Cloud service providers with infrastructure in the Kingdom are likely to do well; cloud service providers based outside the Kingdom are going to need clarity as to the impact on their business; and cloud customers in the Kingdom that are subject to the ECC:2018 are likely to need their cloud service providers to confirm compliance.").

[248] NATIONAL CYBERSECURITY AUTHORITY, *Essential Cybersecurity Controls*, *available at* https://itig-iraq.iq/wp-content/uploads/2019/08/Essential-Cybersecurity-Controls-2018.pdf.

[249] *See Saudi Arabia's draft Cloud Cybersecurity Controls*, LEXOLOGY (Apr. 29, 2020), https://www.lexology.com/library/detail.aspx?g=7e35491b-6ab0-40c6-8d10-26351fb2bc37.

[250] The CCRF allowed for lower sensitivity levels of data to be hosted outside the country, including: non-sensitive public authority data, sensitive private sector data where no sector-specific regulations apply, or "Content qualifying for Level 1 or Level 3 treatment, for which the Cloud Customer elects Level 2 treatment." *See* COMMUNICATIONS & INFORMATION TECHNOLOGY COMMISSION, Cloud Computing Regulatory Framework, https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx.

The ECC and draft CCC should only apply to government organizations (including ministries, authorities, establishments and others), its companies and entities, as well as private sector organizations owning, operating or hosting Critical National Infrastructures (CNIs). However, the NCA has expanded the scope of their ECC enforcement powers by applying this localization mandate to companies that are neither government-owned or CNIs. These requirements prevent U.S. and Saudi companies that use global cloud infrastructure to serve their customers in country, as it would force them to transition to domestic cloud service providers, who may not meet the same standards, pricing, or service parity.

Additional E-Commerce Barriers

In 2018, Saudi Arabia began enforcing a new product compliance regulation that imposes import barriers to the Saudi market. The new regulations impose several additional requirements on international shipments, including registration requirements, additional documentation that must be uploaded to online portals, obtaining prior authorization for officials, payment of additional fees, and submission of legal declarations. Specific product categories such as wireless electronic devices require additional permits from the Saudi telecom regulator. Industry also reports extensive documentation requirements that depart from global practice in developed countries.[251]

AA. Singapore

Government-Imposed Content Restrictions and Related Access Barriers

The Protection from Online Falsehoods and Manipulation Bill became effective starting on October 2, 2019.[252] The law requires 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.[253] It places 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, these rules could spread more misinformation while restricting platforms' ability to continue to address misinformation issues. There are also threats to undermine security and privacy.[254]

[251] 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.

[252] 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.

[253] *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-singaporesdangerous-response-combating-misinformation-online/.

[254] Jennifer Daskal, *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.

BB. Spain

Digital Taxation

On October 7, 2020, the Senate approved legislation to impose a digital tax of 3 percent of revenue derived from online advertising services, the sale of online advertising, and the sale of user data.[255] The current legislation tracks previous attempts to introduce a digital tax in Spain. The global threshold is 750 million euros, with a local threshold of 3 million euros. U.S. companies were cited throughout legislative debate on the legislation making the targets clear.[256]

CC. 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 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-governmental 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.[257]

DD. Taiwan

Taiwan's National Communications Commission is considering a draft bill that would impose registration requirements on over-the-top (OTT) services. The bill would introduce broad requirements, including disclosure of subscriber numbers, appointment of a local representative, and membership of a self-regulatory body.[258] The new rules would present barriers to foreign-based OTT services, including by requiring the disclosure of commercially sensitive data.

---

[255] Available at: https://www.hacienda.gob.es/Documentacion/Publico/GabineteMinistro/Notas%20Prensa/2020/S.E.%20PRESUPUESTOS%20Y%20GASTOS/06-10-20%20Presentaci%C3%B3n%20Techo%20de%20gasto%202021.pdf

[256] Daily Sessions of Congress of the Plenary Members and Permanent Membership, 2020 XIV Legislature No. 26, June 4, 2020), http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu14&DOCS=1-1&QUERY=%28DSCD-14-PL-26.CODI.%29#(P%C3%A1gina14). ("¿De qué estamos hablando? Estamos hablando de que empresas tecnológicas grandes, multinacionales como Google, Amazon, Facebook o Apple paguen impuestos como la España que madruga." [What are we talking about in this debate? We are talking if we want big tech companies such as Google Amazon Facebook and Apple pay taxes (in Spain).]);.Daily Sessions of Congress of the Plenary Members and Permanent Membership, 2020 XIV Legislature No. 26, June 4, 2020), http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu14&DOCS=1-1&QUERY=%28DSCD-14-PL-26.CODI.%29#(P%C3%A1gina14) ("Volviendo al impuesto, la Red es un espacio, evidentemente como el resto, donde la riqueza se acumula. Nos parece bien planteado gravar el tráfico de datos, de contenidos y de publicidad. De hecho, el capitalismo de plataforma —empresas como Amazon o como Glovo, o aplicaciones como Facebook, Telegram o WhatsApp— acumulan miles de millones de beneficios a costa del uso de la ciudadanía." [Returning to the tax, the Internet is a space, obviously like the rest, where wealth accumulates. It seems appropriate to us to tax data, content and advertising traffic. In fact, platform capitalism - companies like Amazon or Glovo, or applications like Facebook, Telegram or WhatsApp - accumulate billions of benefits at the cost of the use of citizenship (online).]).

[257] *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.

[258] *Taiwan: NCC Issues the Draft of a New OTT Law*, LEXOLOGY (July 28, 2020), https://www.lexology.com/library/detail.aspx?g=a30f7272-39d9-4670-9d39-facff20682dc.

EE. Thailand

Government-Imposed Content Restrictions and Related Access Barriers

CCIA has previously raised concerns with the Computer Crime Act, amended in 2016. In November 2019, the Ministry of Digital Economy and Society established an Anti-Fake News Center to combat what is considered "false and misleading" in violation of the Computer Crimes Act.[259] The government has also issued emergency decrees in relation to the global pandemic that further restrict online and press freedom.[260]

In 2019, Thailand passed a controversial Cybersecurity Law following amendments in 2018. Industry has criticized the law due to provisions that enable government surveillance.[261] Under the new law, officials are granted authority to "search and seize data and equipment in cases that are deemed issues of national emergency."[262] This could "enable internet traffic monitoring and access to private data, including communications, without a court order."[263]

FF. Turkey

Government-Imposed Content Restrictions and Related Access Barriers

Turkey remains one of the most restrictive markets for Internet services, and continues to utilize censorship tools to limit online speech.[264] CCIA has previously identified laws that preemptively block websites on vague grounds, and specific instances of blocking by Turkish authorities.[265]

---

[259] *Freedom on the Net 2020: Thailand* (2020), https://freedomhouse.org/country/thailand/freedom-net/2020

[260] *Id.*

[261] *See* Asia Internet Coalition Statement, Feb. 28, 2019, https://aicasia.org/wp-content/uploads/2019/03/AICStatement_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.").

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

[263] *Id.*

[264] *Freedom on the Net 2020: Turkey* (2020), https://freedomhouse.org/country/turkey/freedom-net/2020.

[265] Alexandra de Cramer, *Silence descends on social media in Turkey*, ASIA TIMES (Sept. 11, 2020), https://asiatimes.com/2020/09/silence-descends-on-social-media-in-turkey/ ("Ifade Ozgurlugu Platformu, a Turkish Internet-freedom watchdog, reports that at the end of 2019, Turks were denied access to more than 408,000 websites. Twitter's "transparency report" for the first half of 2019 ranked Turkey in second place globally for taking legal action to remove content."); CCIA 2018 NTE Comments, https://www.ccianet.org/wp-content/uploads/2018/10/CCIA-Comments-to-USTR-for-2019-NTE.pdf, 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* Emile Aben, *Internet Access Disruption in Turkey 2016* (July 19, 2016), https://labs.ripe.net/Members/emileaben/internet-access-disruption-in-turkey.

Turkish lawmakers passed legislation ("Law on Amendment of the Law on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications") in July 2020 that grants the government sweeping new powers to regulate content on social media.[266] The law went into effect October 1, 2020. The law requires social network providers with more than 1MM users to: (1) establish a representative office in Turkey, (2) respond to individual complaints in 48 hours or comply with official take-down requests of the courts in 24 hours, (3) report on statistics and categorical information regarding the Requests every 6 months, and (4) take necessary measures to ensure the data of Turkish resident users are kept in country. Social network providers face serious monetary fines and 50-90 percent possible bandwidth reduction to their platform in cases of noncompliance.

Digital Taxation

Turkey enacted a 7.5 percent digital tax which became effective March 1, 2020. The legislation also permits the President of Turkey to either reduce the rate to 1 percent, or double the tax to 15 percent.[267] Global threshold is 750 million euros, with a local threshold of 20m TYR. The tax applies to revenue generated from the following services: (1) "all types of advertisement services provided through digital platforms" ; (2) "the sale of all types of auditory, visual or digital contents on digital platforms . . . and services provided on digital platforms for listening, watching, playing of these content or downloading of the content to the electronic devices or using of the content in these electronic devices"; and (3) "[s]ervices related to the provision and operation services of digital platforms where users can interact with each other".[268] Digital service providers that provide the covered services, but whose revenue does not make them subject to the tax, still must certify that they are exempt.[269]

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 creates important security measures and obligations.[270] Article 3 prohibits public institutions and organizations' data from being stored in cloud storage services that are not under the control of public institutions. The Circular also requires that critical information and sensitive data be stored domestically. Draft regulation is expected that will also mandate localization of data produced by banks and financial services.

The Regulation on Information Systems of Banks, published on March 15, 2020, still requires banks and financial services to keep their primary (live/production data) and secondary (back-

---

[266] *Silence descends on social media in Turkey*, *supra* note 265; *Facebook to defy new Turkish social media law*, THE FINANCIAL TIMES (Oct. 5, 2020), https://www.ft.com/content/91c0a408-6c15-45c3-80e3-d6b2cf913070.

[267] Law numbered 7194 published in the Official Gazette dated 07.12.2019 and numbered 30971, *available at* https://www.mevzuat.gov.tr/MevzuatMetin/1.5.7194.pdf.

[268] Turkey Revenue Administration, Digital Service Tax Office, https://digitalservice.gib.gov.tr/kdv3_side/maindst.jsp?token=d1078f5e3dc646b78d5d4e5842f21e97feb48d366bc7617458b6679dec12675154a01fccc42292bb04d926bc259dbc75e39dd8e202535fd70a7098396c74a6f7&lang=en.

[269] *Turkey: Digital Services Tax, A Primer*, KPMG (Apr. 21, 2020), https://home.kpmg/us/en/home/insights/2020/04/tnf-turkey-digital-services-tax-a-primer.html.

[270] *New Presidential Decree on Information and Communication Security Measures*, LEXOLOGY (July 25, 2019), https://www.lexology.com/library/detail.aspx?g=8e18f85a-286f-4d29-b017-b17541c3c66b.

ups) information systems within the country.[271] The Regulation establishes a framework for use of cloud services as an outsourced services, but only applies for services located in Turkey.[272]

The Law on the Protection of Personal Data (numbered 6698) governs international transfer of data, which is permitted under the following conditions: (1) when transferring personal data to a country with adequate level of protection, (2) obtaining explicit consent of data subjects, or (3) ad-hoc approval of the Data Protection Board to the undertaking agreement to be executed among data transferring parties.[273] However, industry reports that conditions make it hard to transfer data under these frameworks. Turkey has not yet announced a list of countries that meet the standard of adequate level of protection. Further, the Data Protection Board has yet to grant approval to companies that have sought the ad-hoc approval. While Turkey and the U.S. are aiming to increase trade relations, restrictions created by Turkish data protection legislation confine companies' ability to actively participate in the Turkish economy.

GG. Ukraine

Legal Liability for Online Intermediaries

Ukraine adopted a law, "On State Support of Cinematography" in March 2017 which established a notice-and-takedown system for copyright enforcement. However, the final law goes beyond what the notice-and-takedown system under Section 512 of the DMCA requires in the United States and in the many U.S. trading partners who have adopted similar systems for FTA compliance. The legislation revised Article 52 of Ukrainian copyright law to impose 24- and 48-hour "shot clocks" for online intermediaries to act on demands to remove content in order for them to avoid liability. This deadline may be feasible at times for some larger platforms who can devote entire departments to takedown compliance, but will effectively deny market access to smaller firms and startups, and is inconsistent with the "expeditious" standard under U.S. copyright law. 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.

HH. 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.[274]

---

[271] *New Regulation on Bank IT Systems and Electronic Banking Services*, LEXOLOGY (Mar. 18, 2020), https://www.lexology.com/library/detail.aspx?g=820f9766-219b-4196-9554-bfc715fd1676.

[272] *Id*.

[273] Law on the Protection of Personal Data, *available at* https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aea97a33-089b-4e7d-85cb-694adb57bed3.pdf.

[274] *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, 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, http://www.ccianet.org/wp-content/uploads/2019/05/CCIA-Comments-to-ITC-UK-SME-Trade-Barriers.pdf.

Government-Imposed Content Restrictions and Related Access Barriers

In April 2019, the UK government presented the Online Harms White Paper ("the White Paper") to Parliament that outlines an unprecedented approach to regulating content online.[275] 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. The proposal not only has trade implications, but also free expression concerns, to the extent these rules would conflict with U.S. law. The proposal also anticipates placing burdens on small businesses. 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 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. The UK Office of Communications also released a report on regulating online platforms to address online harms.[276]

Digital Services Tax

Following a public consultation, the UK announced in 2019 it would impose a digital services tax. The 2020 Finance Budget, presented on March 11, 2020, included legislation to introduce a digital services tax of 2 percent. The tax is to be paid on an annual basis, with accruals beginning April 1, 2020. The UK has moved forward with steps to implement the legislation with the major parties in Parliament approving the measure's passage. The tax applies to revenues of "digital services activity" which are (1) "social media platforms", (2) "internet search engines", or (3) "online marketplaces". The legislation seeks to address double taxation in instances where a firm owes multiple digital services taxes, but it is not clear whether sufficient certainty is provided to reduce double taxation under existing corporate tax structures. The UK expects to raise 2 billion pounds over a five-year period with the DST. The practical effect of the tax will be that a handful of U.S. companies will contribute the majority of the tax revenue. UK domestic constituencies have also made requests to triple the DST to 6 percent.

---

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

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

While the proposal document itself purports to have a non-discriminatory intent, statements from policymakers suggest otherwise.[277] The U.S. should push back against the tax as part of the negotiations for a U.S.-UK free trade agreement.

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.[278] The UK also recently joined the United States and Australia in a concerning request to Facebook regarding undermining the security of user communications.[279]

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.[280] If the UK intends to maintain GDPR compliance following Brexit, as expected pursuant to the EU Withdrawal Act (2018),[281] 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.

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

[277] Tweet of HM Treasury, Oct. 29, 2018, https://twitter.com/hmtreasury/status/1056942074271072258 ("We will now introduce a UK Digital Services Tax....It will be carefully designed to ensure it is established tech giants – rather than our tech start-ups - that shoulder the burden of this new tax."); *Hammond Targets US Tech Giants With Digital Services Tax*, THE GUARDIAN (Oct. 29, 2018), https://www.theguardian.com/uk-news/2018/oct/29/hammond-targets-us-tech-giants-with-digital-services-tax (then-UK Chancellor of the Exchequer Philip Hammond described this as a "narrowly targeted tax", noting that "It's only right that these global giants, with profitable businesses in the UK, pay their fair share towards supporting our public services.").

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

[279] 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/.

[280] *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-some-companies-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.

[281] DEPT'T FOR DIGITAL, CULTURE, MEDIA & SPORT, Guidance, Using Personal Data in Your Business After the Transition Period (Oct. 16, 2020), https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation-after-the-transition-period.

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

II. 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. The Law on Cybersecurity took effect January 1, 2019. 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. According to the text, data localization requirements would be enforced after issuance of detailed guidance in an implementing decree. Industry reports that the latest draft of this Decree was discussed in August 2020. The localization rules as contemplated by the current draft appear to indicate that the Government is creating barriers for foreign services to favor local telecommunications and cloud service providers.[282]

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. Latest drafts include requirements for all companies to comply with data requests, content takedown, and domain name seizures.[283] 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 noncompliance.

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 disparaging of the Vietnamese government. Companies have already been fined under this provision.[284]

---

[282] Industry reports that the current draft being discussed includes a provision that would require all domestic companies to keep their data onshore, while foreign companies would only have to onshore their data if they do not adequately cooperate with law enforcement. If all domestic entities are required to localize data under this implementing decree, no hyper-scale cloud service providers will be able to sell to Vietnamese customers, as none of them currently have a local region. Conversely, if localization mandates are issued to foreign entities with no local presence, these foreign entities will incur significant additional overhead costs vis-à-vis their local entities.

[283] *Vietnam: Draft Decree on Personal Data Protection*, BAKER MCKENZIE (Apr. 1, 2020), https://www.bakermckenzie.com/en/insight/publications/2020/04/draft-decree-on-personal-data-protection.

[284] *Vietnam Says Facebook Violated Controversial Cybersecurity Law*, REUTERS (Jan. 8, 2019), https://www.reuters.com/article/us-vietnam-facebook/vietnam-says-facebook-violated-controversial-cybersecuritylaw-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/vietnamquick-to-enforce-new-cybersecurity-law/.

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. 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.

On August 19, 2020, the Ministry of Information and Communications released a draft Decree to amend the Decree 181/2013 Decree on Elaboration of some Article s on the Law on Advertising.[285] The draft rules would regulate advertising content, and expanded the scope of these rules to applications and social media. As drafted, the Decree (1) lacks clarity on definitions, procedures and restrictions, (2) imposes onerous reporting requirements, and (3) obligates providers to actively manage ad content and placement. Revisions are needed to remove clauses to avoid confusion and prevent overlapping liability and duplication.[286]

Technical Barriers to Enforce Digital Protectionism

On June 3, 2020, Vietnam's Prime Minister signed Decision 749/QD-TTg, announcing the country's National Digital Transformation Strategy by 2025.[287] The Decree calls for the creation of technical and non-technical measures to control cross-border digital platforms.

The Ministry of Information and Communications (MIC) has subsequently issued Decisions 1145 and 783 to announce a local cloud standard and cloud framework, respectively, which set forward cloud technical standards and considerations for state agencies and smart cities projects in favor of local private cloud use.[288] These decisions aim to create a preferential framework for domestic cloud service providers. The MIC Minister has stated a desire for Vietnamese firms to attain a stronger hold in cloud computing and digitalization infrastructures, as they have with physical networks.[289] While these standards are technically voluntary, in practice, these standards are expected to be adopted by the Vietnamese public sector.

Digital Taxation

The Tax Administration Law, effective July 1, 2020, taxes cross-border e-commerce and other digital services.[290] Industry reports that the Ministry of Finance is drafting the implementation

[285] *Draft Amendment to Decree No. 181/2013ND-CP: The Impact on Cross-Border Advertising Activities*, LEXOLOGY (Oct. 2, 2020), https://www.lexology.com/library/detail.aspx?g=31329819-83f3-4b8e-8554-87daf272bb1b.

[286] For example, take-down requests and tax obligations should only be regulated pursuant to Decree 72 and relevant tax laws.

[287] *See* https://vanbanphapluat.co/decision-749-qd-ttg-2020-introducing-program-for-national-digital-transformation.

[288] *Vietnam Issues Guidelines on Cloud Computing for E-Government Deployment*, LEXOLOGY (Apr. 15, 2020), https://www.lexology.com/library/detail.aspx?g=e567a057-5b54-4760-bcd9-937ca888773f.

[289] *Ministry Launches Digital Transformation Campaign*, VIETNAM NET (May 23, 2020), https://vietnamnet.vn/en/sci-tech-environment/ministry-launches-digital-transformation-campaign-643379.html.

[290] *Vietnam's Tax Administration Law Takes Effect*, R GLOBAL (Aug. 7, 2020), https://www.irglobal.com/article/vietnams-tax-administration-law-takes-effect-in-july-2020-0f67/.

circular, which will mandate that cross-border digital service providers register, declare and pay taxes (VAT and CIT) from January 2021. As it operates as a tariff on foreign-provided digital goods and services, this tax is explicitly discriminatory.

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 Report.