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-2021-0016

COMMENTS OF THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION REGARDING FOREIGN TRADE BARRIERS TO U.S. EXPORTS FOR 2022 REPORTING

October 26, 2021

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 86 Fed. Reg. 51,436 (Sept. 15, 2021), 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 is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For nearly fifty years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy.[1] CCIA welcomes the opportunity to document various regulations and policy frameworks that serve as market access barriers for Internet services.

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. As evidenced through the COVID-19 pandemic, digital technologies have enabled regular business activities in cross-border communication. Several small businesses have reported increased adoption of digital services to operate during the pandemic.[2] They will continue to play an important role in the economic recovery.

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. Governments are increasingly using the "techlash" as a justification to exclude or restrict U.S. digital services in foreign markets.

Further, there is a rise in authoritarian government's control of Internet services to restrict speech and undermine security of users. This risks fragmentation of the global digital economy. Censorship and denial of market access for foreign Internet services has long been the case in restrictive markets like China, but it is becoming increasingly common in emerging digital markets as well as some traditional large trading partners, and accomplished through using different tools and methods. Because the business community has a limited technical capacity to assess and respond to interference with cross-border flow of services, products, and information by nation-states, allied governments have a critical role to play in partnering with technology companies and leading in the defence of Internet freedom and open digital trade principles.

As the Internet is essential to international commerce and communications online, it is essential that such barriers are identified and quelled. For the 2022 National Trade Estimate report, CCIA

[1] For more, visit www.ccianet.org.

[2] SHRM, *Small Businesses Get Creative to Survive Pandemic* (Sep. 2020), https://www.shrm.org/hr-today/news/all-things-work/pages/small-businesses-get-creative-to-survive-during-the-pandemic.aspx; Connected Commerce Council, *Digitally Driven: U.S. Small Businesses Find a Digital Safety Net During COVID-19* (2020), https://connectedcouncil.org/wp-content/uploads/2020/09/Digitally-Driven-Report.pdf.

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

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.

From 2005 to 2019, the digital economy grew at an annual rate of 6.5 percent, compared to 1.8 percent overall economic growth.[3] According to U.S. Department of Commerce estimates, the digital economy accounted for 9.6 percent ($2,051.6 billion) of current-dollar gross domestic product (GDP) ($21,433 billion) in 2019.[4] Further, the digital economy supported 7.7 million jobs, which accounted for 5.0 percent of total U.S. employment (155.2 million jobs) in 2019.[5] The digital economy supported more jobs than the construction industry and the industry made up of "other" services, except in government.[6]

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.[7]

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 favour domestic innovation and specifically target U.S. companies, ushering in a new form of discrimination.

Trading partners' pursuit of "technological sovereignty", with protectionist features, continues to be a concerning trend. 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.

---

[3] BUREAU OF ECONOMIC ANALYSIS, *Updated Digital Economy Estimates - June 2021* (2021), https://www.bea.gov/system/files/2021-06/DE%20June%202021%20update%20for%20web%20v3.pdf

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *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".[8] 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. CCIA encourages the United States to pursue 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 2021 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 trade barriers affecting U.S. technology companies' ability to export, in addition to those outlined in this section below, are also included in country profiles in Section III.

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.[9] Since that time, industry continues to see countries pursue policy and regulatory frameworks that restrict the free flow of information across borders.[10]

---

[8] 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.

[9] 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*"].

[10] INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION, *How Barriers to Cross-Border Data Flows are Spreading Globally, What They Cost, and How to Address Them* (2021), *available at* https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost ("In 2017, 35 countries had implemented 67 such barriers. Now, 62 countries have imposed 144 restrictions—and dozens more are under consideration.").

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 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.[11] 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.[12]

Rather than promote domestic industry, data localization policies are likely to hinder economic development and restrict domestic economic activity,[13] and impede global competitiveness.[14]

---

[11] 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.

[12] 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.

[13] *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).

[14] 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

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.[15] 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.[16]

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.[17] More recently, industry has tracked initiatives in the EU to establish an EU-wide cloud that would localize data within EU borders.

Continued opposition from the U.S. and likeminded allies is needed at the multilateral stage considering these growing trends.[18]

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

CCIA has long viewed foreign censorship of U.S. Internet services as having an international trade dimension, and is supportive of efforts to identify certain practices that either amount to trade violations or market access barriers. The U.S. technology sector is on the front lines worldwide in the battle against government censoring, filtering, and blocking of Internet content. Many U.S. companies publish transparency reports that detail increased cases of Internet service disruptions, government requests for data, and content takedowns.[19] For example, Facebook

---

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 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.").

[15] 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).

[16] *See* Chander & Lê, Data Nationalism, *supra* note 11; 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*"].

[17] 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.

[18] 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.

[19] See, e.g., Google Transparency Report, Traffic and Disruptions to Google, https://transparencyreport.google.com/traffic/overview; Government Requests to Remove Content,

notes that its services were interrupted 84 times in 19 countries in the second half of last year, compared to 52 disruptions in eight countries that took place during the first half of the year.[20] Just last summer, Nigeria announced an "indefinite ban" on Twitter in the country following the company's decision to remove posts from political leaders that violated its abusive behaviour policy.

Censorship and denial of market access for foreign Internet services has long been the case in restrictive markets like China, but it is becoming increasingly common in emerging digital markets as well as some traditional large trading partners, and accomplished through using different tools and methods. Because the business community has a limited technical capacity to assess and respond to interference with cross-border flow of services, products, and information by nation-states, allied governments have a critical role to play in partnering with technology companies and leading in the defense of Internet freedom and open digital trade principles. However, to tackle these urgent issues, identification of key barriers is critical.

Government-imposed censorship of digital services and content takes multiple forms, and the risks associated with each method or regulatory framework providing for censorship methods can vary greatly. For example, some types of content restrictions may be reasonable and legally permissible in certain contexts, but may result in overbroad removals of user speech if attached to filtering or monitoring requirements. Other trade concerns arise where content policies are not applied equally to both domestic and foreign websites. Furthermore, an increasing number of content restrictions do not comply with World Trade Organization (WTO) principles of transparency, necessity, minimal restrictiveness, and due process to affected parties.

1. Online Content Regulations

U.S. firms face an increasingly hostile regulatory environment in a variety of international markets which impedes U.S. Internet companies of all sizes from expanding their services abroad. Some of these regulations are in pursuit of legitimate and valid goals to address illegal content online; however, some proposals are more expansive in scope and directly conflict with U.S. law and free expression values. For example, there is a concerning trend in recent years among authoritarian governments pursuing content regulations to fight "fake news", which often go beyond standard efforts to remove disinformation and instead have the primary effect of targeting dissidents and political opposition.[21]

---

https://transparencyreport.google.com/government-removals/overview (last visited Oct. 26, 2021); Twitter Transparency Removal Requests Report, https://transparency.twitter.com/en/reports/removal-requests.html#2020-jul-dec (published July 14, 2021).

[20] *Facebook Says Government Internet Shutdowns Are on the Rise*, AXIOS (May 20, 2021), https://www.axios.com/facebook-government-internet-shutdowns-censorship-a1c1c181-dc01-4450-9945-e1465f5139e8.html.

[21] *The Rise of Digital Authoritarianism: Fake News, Data Collection and the Challenge to Democracy*, FREEDOM HOUSE (Oct. 2018), https://freedomhouse.org/article/rise-digital-authoritarianism-fake-news-datacollection-and-challenge-democracy ("Citing fake news, governments curb online dissent: At least 17 countries approved or proposed laws that would restrict online media in the name of fighting "fake news" and online manipulation. Thirteen countries prosecuted citizens for spreading allegedly false information.").

Separately, there are increasing foreign trends that require U.S. companies to:

- remove speech that may be legal within a country but that conflicts with vaguely defined norms about "harmful" content;
- adhere to broadly defined "duties of care" that require general monitoring of all user content posted to an Internet service;
- allow foreign governments access to data and systems, sometimes without a court order;
- pre-install, give preferential treatment to, or provide data to foreign technology companies that may restrict speech or surveil users in a manner that conflicts with U.S. law and values;
- break encryption by enabling the "traceability" of originators of content; and
- designate local employees that will be subject to imprisonment in cases of noncompliance with a local content requirement.

Context and how certain rules are being enforced in a market are important when evaluating regulations pertaining to removal of online content and may determine risk of censorship and potential trade-distortive practices. For instance, the presence, or lack thereof, of legal norms such as due process may help reduce impact for U.S. firms operating abroad. It is important that good regulatory practices are followed as governments consider new rules on addressing harmful and illegal content; are designed to limit unintended consequences, especially those that impact online speech; and are compliant with trade commitments.

To be clear, an increasing number of Internet services recognize the importance of ensuring user trust and safety in their platforms and have significantly increased resources to ensure that their services remain spaces for free expression, that users comply with their terms of service, and that illegal and harmful content that violates their terms of service is identified and removed from their platform. But the expanding array of censorship obligations described in these comments often have the impact of making it harder, rather than easier, for U.S. Internet companies to strike the right balance between promoting free expression and taking action against illegal content.

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 favour 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.[22] Access Now documented over 50 Internet shutdowns in 21 countries just in the first five months of 2021.[23] Internet shutdowns are also costly,7 with one study finding that countries lose $23.6 million (per 10 million in population) for every day that the Internet is shut down.[24] Despite these costs, governments continue to filter and block Internet content, platforms, and services for various reasons. For example, Iran has completely shut off access to the Internet in response to protests in the past.[25] And as discussed further below, the services of many U.S. Internet platforms are currently either blocked or severely restricted in the world's largest online market: China.

Whether deliberate actions to stifle political dissent 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.[26]

Such blocking is likely to violate international commitments, such as the World Trade Organization's rules on market access and national treatment.

With respect to GATT obligations, while the function of GATT governs trade in physical goods, there is the possibility for the application of these commitments in the digital context. It is certainly the case that online services which implicate neither downloaded nor stored goods, such as search and social media, must be considered "services," analyzed with reference to GATS, not GATT. Nevertheless, disagreements remain regarding products that are downloaded, and kept in digital form, "like newspapers, songs, software, audio and electronic books. While the WTO has yet to rule on the issues, or its members to agree, the better position is that the digital versions of

---

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

[23] ACCESS NOW, #KeepItOn Update: Who Is Shutting Down the Internet in 2021, https://www.accessnow.org/who-is-shutting-down-the-internet-in-2021/.

[24] DELOITTE, The Economic Impact of Disruptions to Internet Connectivity, A Report for Facebook, at 6 (Oct. 2016), https://globalnetworkinitiative.

[25] *Internet Disrupted in Iran Amid Protests in Multiple Citie*s, NET BLOCKS (Nov. 15, 2019), https://netblocks.org/reports/internet-disrupted-in-iran-amid-fuel-protests-in-multiple-cities-pA25L18b.

[26] 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.

goods remain goods subject to GATT."[27] In any event, physical goods may be purchased through digital means, and thereby implicating the objectives embodied in GATT. GATT requires a contracting party to afford goods supplied from abroad similar status to like products originating from domestic suppliers.[28] Yet in many cases platforms and services through which digital products can be obtained are subjected to specific censorship that provides a competitive advantage to similar products originating in China. Certain U.S. social media services, for example, have been completely blocked in China, while their Chinese equivalents Weibo and Renren are allowed to operate with selective filtering. GATT similarly requires "[l]aws, regulations, judicial decisions and administrative rulings of general application" to be published promptly, and to be administered in a "uniform, impartial and reasonable manner."[29] The filtering, blocking, and censorship that U.S. services encounter, however, generally remains unpublished and unevenly applied. Moreover, little legal recourse exists to dispute the administration of such measures.

With respect to GATS, numerous provisions of GATS prohibit the filtering, blocking, and censorship that is applied to Internet services. GATS imposes considerable obligations on WTO Members, mandating transparency, impartiality, and nondiscrimination in trade-related government actions, and requires that affected parties be afforded opportunities for judicial or independent review of trade-related administrative decisions. While exceptions to these obligations exist, such as for "public morals/order"[30] GATS derogations are only permissible when necessary to achieve the stated objective, where no reasonable, less restrictive alternative exists, and when applied without prejudice.[31] Where nations implement filtering, blocking, and censoring of online services, these standards are rarely met. It is necessary to note that whereas GATT imposes blanket commitments, GATS governs sectors and "modes" where a contracting party has made specific commitments. The Chinese Government has made specific commitments pertaining to various web-based service sectors, however, as well as value-added telecommunications.[32] As with GATT, GATS requires reasonable publication and impartial administration of trade related regulatory measures. When U.S. services encounter arbitrary restrictions, often at odds with what domestic competitors are subjected to, it likely constitutes a GATS violation.[33] The market access commitments contained in GATS Article XVI also apply in this context.

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

[27] Tim Wu, The World Trade Law of Censorship and Filtering (May 2006), at http://ssrn.com/abstract=882459, at 7.

[28] GATT Art. III:4 (1947 text).

[29] GATT Arts. X:1, X:3(a)-(b).

[30] Exceptions for "public morals"/ "public order" may be found in GATT Art. XX(a) and GATS Art. XIV(a).

[31] GATS Art. XIV. *See* Tim Wu, The World Trade Law of Censorship and Filtering (May 2006), http://ssrn.com/abstract=882459, at 13.

[32] Frederik Erixon, Brian Hindley, & Hosuk Lee-Makiyama, Protectionism Online: Internet Censorship and International Trade Law (2009), http://www.ecipe.org/publications/protectionism-online-internet-censorship-andinternational-trade-law/.

[33] GATS Art. XVII:1.

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

As CCIA has previously stated 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.[36] Furthermore, such restrictions must comply with WTO principles of transparency, necessity, minimal restrictiveness, and due process to affected parties.

CCIA is supportive of efforts by the U.S. International Trade Commission to document the trade impacts of foreign censorship and has provided written comments and oral testimony.[37]

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. These comments document key DST proposals or implemented measures, but may not include all discriminatory digital tax measures at time of filing.[38]

CCIA welcomes the announcements made pursuant to the OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting Project in 2021. CCIA has long supported 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

---

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

[35] 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/.

[36] CCIA Comments, In re Request for Public Comments To Compile the National Trade Estimate Report on Foreign Trade Barriers, Docket. No. 2020-0034, filed Oct. 29, 2020, *available at* https://www.ccianet.org/wp-content/uploads/2020/10/USTR-2020-0034-CCIA-Comments-on-2021-National-Trade-Estimates-Report-1.pdf [hereinafter "*2020 CCIA NTE Comments*"].

[37] See Comments of CCIA, U.S. INT'L TRADE COMM. Invest. No. 332-585: Foreign Censorship Part 1: Policies and Practices Affecting U.S. Businesses (filed July 21, 2021), available at https://www.ccianet.org/wp-content/uploads/2021/07/Investigation-No.-332-585-CCIA-Comments-Foreign-Censorship-Practices-Part-1.pdf.

[38] 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.

remains the only path forward to provide certainty, and reduce trade tensions caused by countries' decisions to enact unilateral measures.

On October 8, 2021, the Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy was released outlined the agreed-upon framework for global corporate tax reform.[39] The document states:

> The Multilateral Convention (MLC) will require all parties to remove all Digital Services Taxes and other relevant similar measures with respect to all companies, and to commit not to introduce such measures in the future. No newly enacted Digital Services Taxes or other relevant similar measures will be imposed on any company from 8 October 2021 and until the earlier of 31 December 2023 or the coming into force of the MLC. The modality for the removal of existing Digital Services Taxes and other relevant similar measures will be appropriately coordinated.[40]

Pursuant to this commitment, all countries that have agreed to this framework cannot introduce any new unilateral measures and CCIA encourages countries to abandon any national plans to implement. Further, while the most appropriate action would be an immediate withdrawal of existing DSTs in exchange for terminating the Section 301 investigations, CCIA is supportive of the compromise reached by the United States, Austria, France, Italy, Spain, and the United Kingdom regarding existing measures. CCIA encourages policymakers to continue work on swift implementation of the global framework.[41]

Often based on inaccurate estimates, some countries assert that digital services fail to pay adequate taxes and should be subject to additional taxation.[42] 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 and the use of

---

[39] Press Release, CCIA Welcomes Historic Global Tax Reform Tax Agreement (Oct. 8, 2021) https://www.ccianet.org/2021/10/ccia-welcomes-historic-global-tax-reform-agreement/.

[40] OECD G20/Base Erosion and Profit Shifting Project, Statement on a Two-Pillar Solution to Address to the Tax Challenges Arising from the Digitalization of the Economy (Oct. 8, 2021), https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.pdf.

[41] U.S. DEP. OF TREASURY, Joint Statement from the U.S., Austria, France, Italy, Spain, and the United Kingdom Regarding a Compromise on a Transition Approach to Existing Unilateral Measures During the Interim Period Before Pillar 1 is in Effect (Oct. 21, 2021), https://home.treasury.gov/news/press-releases/jy0419 [hereinafter "*Unilateral Measures Compromise*"]; OFFICE OF THE U.S. TRADE REP., *USTR Welcomes Agreement with Austria, France, Italy, Spain and the United Kingdom on Digital Services Taxes* (Oct. 21, 2021), https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/october/ustr-welcomes-agreement-austria-france-italy-spain-and-united-kingdom-digital-services-taxes.

[42] 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/.

retaliatory action may be helpful to hasten the removal of existing measures pursuant to commitments under the OECD framework.

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.[43] 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 digitalization of the global economy. These taxes, wherever imposed, warrant a substantial, proportionate response from the United States.[44]

D. Market-Based Platform Regulation

A general but ill-defined desire for "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. In all instances policymakers struggle to separate procompetitive conduct from that which they seek to regulate. The effectiveness of such proposals has been called into question to the extent it serves the purposes of promoting innovation in the tech sector.[45]

---

[43] *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.

[44] 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").

[45] 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.").

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. The EU is currently debating a wide liability regime that should not extend beyond U.S. standards. Another concerning trend is the failure of current U.S. trading partners to fully implement existing carefully negotiated intermediary protections in free trade agreements.[46] 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.[47] 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.[48] 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.[49] USTR also stated in 2017 its commitment to seek "the commitment of our free

[46] *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.

[47] 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.

[48] 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.

[49] 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

trade agreement partners to continuously seek to achieve an appropriate balance in their copyright systems, including through copyright exceptions and limitations."[50] Within the last thirty years, such rules have enabled the development of innovative new products and services such as the VCR, DVR, iPod, cloud computing, search engines, social media services, and 3D printing. Similarly, users of copyrighted works — including consumers, libraries, museums, reporters, and creators — depend upon concepts like fair use and other limitations and exceptions to engage in research, reporting, parody, and political discourse. These innovations are jeopardized by weak or nonexistent limitations and exceptions in the copyright laws of other countries.[51] 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.[52] A USITC report also observed that these laws tend to have "generated unintended consequences" to small online publishers.[53] 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

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.

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

[51] 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.").

[52] Office of the U.S. Trade Rep., National Trade Estimates Report 2020, https://ustr.gov/sites/default/files/2020_National_Trade_Estimate_Report.pdf.

[53] *2017 Global Digital Trade 1*, *supra* note 9, 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.").

barrier to trade.[54] CCIA would encourage U.S. policymakers to carefully evaluate the trade implications of imposing ancillary rights in the United States.[55]

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.[56] These initiatives often are 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.[57]

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.[58] Enforcing extraterritorial judgments on U.S. services not only imposes significant compliance costs, but also exposes 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,

---

[54] 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.

[55] The U.S. Copyright Office is currently soliciting comments on ancillary rights, including its compliance with international obligations. *See* Publishes' Protections Study: Notice and Request for Public Comment, 86 Fed. Reg. 56,721 (Oct. 12, 2021), *available at* https://www.govinfo.gov/content/pkg/FR-2021-10-12/pdf/2021-22077.pdf.

[56] 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.

[57] *Id.*

[58] *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.

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 Progressive Agreement for Trans-Pacific Partnership (CPTPP),[59] Article 19.3 of the U.S.-Mexico-Canada Agreement (USMCA),[60] and Article 8.72 of the EU-Japan Economic Partnership Agreement.[61]

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 several 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.[62] Analysis on duties on electronic transmissions for economic development shows

[59] 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.

[60] 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"].

[61] 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.

[62] *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

that this is not supported.[63] The United States should continue to advocate for the permanent extension of the moratorium at the WTO at the upcoming Ministerial Conference in December 2021, 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 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.[64]

These exceptional access regimes run contrary to the consensus assessments of security technologists because they are technically and economically infeasible to develop and implement.[65] 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 many 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.

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.

[63] 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*, REAL CLEAR POLICY (Mar. 13, 2019), https://www.realclearpolicy.com/articles/2019/03/13/explainer_understanding_digital_trade_111113.html; Nigel Cory, *The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of* 2018, ITIF (Jan. 2019), at 24, http://www2.itif.org/2019-worst-mercantilist-policies.pdf.

[64] 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/.

[65] 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.

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 non-discrimination 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 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.[66]

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 Monitoring System.[67] 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.[68] 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.

---

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

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

[68] 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.

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.[69] 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.[70] 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."[71] Combined, these controls and taxes are making it increasingly difficult, and at times impossible, for foreign companies to sell to Argentine customers.

B. Australia

Market-Based Regulations

In February 2021, the Australian Government passed the News Media and Digital Platforms Mandatory Bargaining Code.[72] Under the Code, designated platform services companies are required to engage in negotiations with Australian news publishers for online content. 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 disclose proprietary information related to private user data and algorithms.[73]

If forced negotiations break down, or an agreement is not reached within three months between a news business and designated platform, the bargaining parties would be subject to compulsory mediation. If mediation is unsuccessful, the bargaining parties would proceed with arbitration, with arbitrators seeking to determine a fair exchange of value between the platforms and the news businesses. In addition to the negotiation and arbitration requirements, the Bargaining Code imposes information sharing requirements, including a requirement that platforms provide advance notice of forthcoming changes to algorithms if the change is likely to have a significant effect on the referral traffic for covered news content.

---

[69] *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.

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

[71] *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.

[72] Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2021, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6652 [Aus.].

[73] *The Dangers of Australia's Discriminatory Media Code*, DISRUPTIVE COMPETITION PROJECT (Feb. 19, 2021), https://www.project-disco.org/21st-century-trade/021921-the-dangers-of-australias-discriminatory-media-code/.

Under the Code, the Australian Treasury would have the utmost discretion to determine which companies these mandates are applied to by determining whether the platform holds significant bargaining power imbalance with Australia news media businesses. The Treasurer must also consider if the platform has made a significant contribution to the sustainability of the Australian news industry through agreements relating to news content of Australian news businesses. Only two companies have been identified throughout deliberations. There are significant concerns from a procedural,[74] competition,[75] trade,[76] and intellectual property[77] perspective that USTR should pay close attention to. In particular, U.S. officials should monitor the implementation of the Code and its adherence to the principles of transparency, fairness and non-discrimination as consistent with the U.S.-Australia FTA.

At time of filing, no platform has been officially designated, although the Code is subject to an annual review by the Treasurer commencing February 2022. In view of the impending Australian Federal election and that news publishers are integral to the election, industry reports that the process has become especially politicized.

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.[78] The legislation authorizes the Australian government to use three new tools to compel assistance from technology companies in accessing information within electronic communications. These tools are technical assistance requests (TARs), which seek voluntary assistance from communications providers; and technical assistance notices (TANs) and technical capability notices (TCNs). These tools call upon providers to do one or more specified acts which could include building new technical capabilities as required by the Attorney General. While the legislation specifically forbids a notice to provide a "systemic weakness or vulnerability" into an encrypted system, it does provide sufficiently broad authority to undermine encryption through other technical means with little oversight. Companies have called for amendments to the bill citing the broad language and failure to address concerns during the drafting process.[79]

---

[74] *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/.

[75] *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/.

[76] *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/.

[77] *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/.

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

[79] 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-

Copyright Liability Regimes for Online Intermediaries

Failure to implement obligations under existing trade agreements serves as a barrier to trade.[80] 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.[81] This oversight was not addressed by the 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.[82] 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 this material.[83] Criticism for the legislation was widespread, with particular concern about the

---

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.

[80] *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.

[81] 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.

[82] 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/.

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

rushed nature of the drafting and legislative process.[84] The legislation applies to a broad range of technology and Internet services, including U.S.-based social media platforms, user-generated content and live streaming services, and hosting services. However, the law does not consider the varying business models of these services in scope of the law and their varying capabilities or roles in facilitating user-generated content. CCIA encourages governments to enact policies affecting online content only after consultation by all stakeholders.[85] Australian officials have also indicated that the country will soon block access to Internet domains hosting terrorist material and will pursue additional legislation that will impose new content requirements on digital services.[86]

The Online Safety Act, which was passed in June 2021 and will come into force in January 2022, gives the "eSafety regulator" the power to demand the removal of adult cyber abuse and other content that is deemed "harmful".[87] This legislation also compels eight different online industry sectors to develop co-regulatory codes of conduct that detail how companies will prevent both illegal and legal but harmful content from being viewed by minors.[88] The 'Basic Online Safety Expectations' being created under the Act will require international service providers to report on the steps they take to, among other things, 1) provide Australian-specific safety information from the regulator; 2) take steps to identify people behind anonymous accounts; and 3) monitor encrypted communications for harmful content.[89] The eSafety Commissioner has also made clear that the enforceable industry codes required under the Act, which will apply to all international services accessible by Australians, need to include obligations for companies to prevent harm from occurring, and also to conduct regular mandatory transparency reporting.

Industry is concerned with the following aspects of the law: the scope of services caught by this legislation (which includes social media services, user-generated content platforms, search engines, app distribution marketplaces, and enterprise hosting services), the 24-hour timelines for content removal, the lack of transparency and accountability of decisions made by the regulator,

---

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

[85] *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.").

[86] 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.

[87] Online Safety Bill 2021, *available at* https://perma.cc/637E-N5AF [Aus.].

[88] *Australia: Online Safety Bill Passed*, LIBRARY OF CONGRESS (Aug. 10, 2021), https://www.loc.gov/item/global-legal-monitor/2021-08-10/australia-online-safety-bill-passed/.

[89] The Australian Government is currently soliciting input on aspects of this law. *See* Online Safety (Basic Online Safety Expectations) Determination 2021 Draft, *available at* https://www.infrastructure.gov.au/sites/default/files/documents/draft_online_safety_basic_online_safety_expectations_determination_2021.pdf.

and the definition of "harm" that lacks sufficient clarity which will lead to lawful content being taken down.

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.[90] Companies with over $75,000 AUD in sales to Australian customers are required to register and lodge returns with the Australian Tax Office.

Critical Infrastructure Reforms

In December 2020, Australia announced changes to its critical infrastructure framework, with the introduction of the Security Legislation Amendment (Critical Infrastructure) Bill 2020.[91] The Government's stated objective of the Bill is to "protect the essential services all Australians rely on by uplifting the security and resilience of our critical infrastructure."[92] The proposed legislation significantly expands the sectors considered critical infrastructure (including companies that provide 'data storage or processing' services). It will impose additional security obligations for critical infrastructure assets (including risk management programs and cyber incident reporting), enhanced cyber security obligations, and government assistance measures that would enable Australian government agencies to require critical infrastructure entities to install monitoring software on their networks, to 'take control' of an asset or to follow directions of the Australian Signals Directorate. Industry has raised concerns with the bill, in particularly the government assistance measures, arguing they go above and beyond what is necessary for action and support by the government in the data storage or processing sector.[93]

Hosting Strategy Certification Framework

In 2019, the Australian Government released the Hosting Strategy,[94] providing policy direction on how government data and digital infrastructure would enable the Digital Transformation Strategy, focused on data center facilities, infrastructure, data storage and data transmission. In March 2021, the certification framework for the policy was released to operationalize the Hosting Strategy. [95]

---

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

[91] Security Legislation Amendment (Critical Infrastructure) Bill 2020: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657.

[92] Explanatory Memorandum Security Legislation Amendment (Critical Infrastructure) Bill 2020, available at https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6657_ems_928e0092-fabb-4c31-a67b-b47ac1123e17/upload_pdf/JC000738.pdf;fileType=application%2Fpdf.

[93] *See Global Tech Groups Seek Changes to Critical Infrastructure Bill*, INNOVATION AUSTRALIA (Oct. 14, 2021), https://www.innovationaus.com/global-tech-groups-seek-changes-to-critical-infrastructure-bill/.

[94] Digital Transformation Agency, Hosting Strategy: https://www.dta.gov.au/our-projects/whole-government-hosting-strategy

[95] Digital Transformation Agency, Hosting Certification Framework, March 2021: https://www.dta.gov.au/sites/default/files/files/digital-

The certification requires hosting providers, data center operators and cloud service providers to allow the government to specify ownership and control conditions. The framework has the effect of imposing data localization and data residency requirements, plus personnel requirements, on all protected-level data and data from whole-of-government systems.

Audiovisual Services

In November 2020, the Australian Government issued the Media Reform Green Paper.[96] The Green Paper proposes setting the "expectation" that subscription and advertising video-on-demand ("SVOD") services invest a percentage of their Australian revenue in Australian content, in the form of commissions, co-productions, and acquisitions. If service suppliers fail to meet investment expenditure "expectations" for two consecutive years, then the Minister of Communications will have the power to implement regulatory requirements.

As drafted, the proposal would not apply to Australian SVODs that have a free-to-air TV broadcaster within their corporate group of companies. At the same time the Australian Government established a voluntary reporting framework administered by Australian Communications and Media Authority (ACMA) under which SVOD services report to ACMA on their level of investment in Australian content. The first report of ACMA published in August 2020 showed SVODs had invested AUD$268 million in Australian content.[97] Were the Australian Government to mandate SVODs invest a percentage of their Australian revenue in Australian content, it would *prima facie* conflict with its obligations under the U.S.-Australia Free Trade Agreement, which contains an obligation that Australia accord to service suppliers of the other Party treatment no less favorable than that it accords, in like circumstances, to its own service suppliers.

C. Austria

Digital Taxation

Austria implemented a 5 percent digital tax on revenues from digital advertising services provided domestically.[98] The global revenue threshold is 750 million euros, 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

identity/New%20Accreditation%20Templates/Hosting%20Certification%20Framework%20-%20March%202021.v2.pdf

[96] Media Reform Green Paper: Modernising television regulation in Australia (Nov. 2020), available at https://www.infrastructure.gov.au/sites/default/files/documents/media-reform-greenpaper-december2020_0.pdf [Australia].

[97] ACMA, Spending by subscription video on demand providers 2019-20, https://www.acma.gov.au/spending-subscription-video-demand-providers-2019-20. *See also* ACMA Data Reveals SVOD Spend on Australian Programming (Aug. 13, 2021), https://www.if.com.au/acma-data-reveals-svod-spend-on-australian-programming/.

[98] 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.

advertising, search engine advertising and comparable advertising services.[99] Per officials, a covered service is deemed to have been provided domestically "if it is received on a user's device having a domestic IP address and is addressed (also) to domestic users in terms of its content and design."[100] 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."[101]

While the most appropriate action would be an immediate withdrawal of existing DSTs in exchange for terminating the Section 301 investigations, CCIA is supportive of the compromise reached by the United States, Austria, France, Italy, Spain, and the United Kingdom regarding existing measures.[102] CCIA encourages policymakers to continue work on swift implementation of the global framework and removal of the DST.

D. Bangladesh

Government-Imposed Content Restrictions and Related Access Barriers

The Digital Security Act of 2018 criminalizes a wide range of online activity, creating challenges for Internet-based platforms and digital media firms.[103] The Act criminalizes publication of information online that hampers the nation, tarnishes the image of the state, spreads rumors, or

[99] Federal Ministry Republic of Austria, Digital Tax Act 2020, https://www.bmf.gv.at/en/topics/taxation/digital-tax-act.html (last visited Oct. 25, 2021).

[100] Id.

[101] 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.]).

[102] *Unilateral Measures Compromise*, *supra* note 41.

[103] *See How Is Bangladesh's Digital Security Act Muzzling Free Speech*?, DW (Mar. 3, 2021), https://www.dw.com/en/how-is-bangladeshs-digital-security-act-muzzling-free-speech/a-56762799.

hurts religious sentiment. The Act provides for criminal penalties up to $120,000 and up to 14 years in prison for certain infractions.

The Information and Communication Technology Act of 2006 (the Act), amended in 2013, authorizes the government of Bangladesh to access any computer system for the purpose of obtaining any information or data, and to intercept information transmitted through any computer resource.[104] Under the Act, Bangladesh may also prohibit the transmission of any data or voice call and censor online communications. The Bangladesh Telecommunication Regulatory Commission (BTRC) ordered mobile operators to limit data transmissions for political reasons on several occasions in 2019 and in 2020 ahead of politically sensitive events, including local and national elections. The BTRC ordered mobile operators to block all services except for voice calls in the Rohingya refugee camps in Cox's Bazar from September 2019 until August 2020. In November 2018, the BTRC instructed all international Internet gateway licensees to temporarily block a U.S. Voice over IP service supplier; the block lasted for one day. Such interference, even on a temporary basis, undermines the value of Internet-based services, decreasing the incentive to invest and raises costs for firms in the market.[105]

E. 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 government has announced that they would wait for an OECD solution. Industry is monitoring political developments.[106]

[104] Available at: https://samsn.ifj.org/wp-content/uploads/2015/07/Bangladesh-ICT-Act-2006.pdf.

[105] *See also* HUMAN RIGHTS WATCH, *Bangladesh: Internet Blackout on Rohingya Refugees* (Sep. 13, 2019), https://www.hrw.org/news/2019/09/13/bangladesh-internet-blackout-rohingya-refugees.

[106] *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.

F. 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.[107] It officially came into force in August 2020, and in August 2021 sanctions were effective.

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.[108] 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.[109] 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.[110]

The national authority released its regulatory agenda and included "International transfer of data" as part of "Phase 2", meaning that the issue is expected to be subject to public consultation by mid-2022. The Data Protection Authority is expected to release guidelines to define what constitutes the international transfer (for example, storage on international servers contracted for cloud service) and the content of standard contractual clauses.

Other localization barriers reported include tax incentives for locally sourced information and communications technology (ICT) goods and equipment,[111] government procurement preferences for local ICT hardware and software,[112] and non-recognition of the results of conformity assessment procedures performed outside of Brazil for equipment connected to telecommunications networks.[113] 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.[114] The Presidency Institutional Security Group (GSI), led by a military, published a Normative Instruction which establishes new rules for the contracting of cloud services by the Federal Public Administration. It established requirements for data and metadata

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

[108] 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.

[109] 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).

[110] *Brazil's New Data Protection Law: The LGPD*, *supra* note 108.

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

[112] 2014 Decrees 8184, 8185, 8186, 8194, and 2013 Decree 7903.

[113] ANATEL's Resolution 323.

[114] *Brazil's New Data Protection Law: The LGPD*, *supra* note 108.

residency exclusively in national territory in a few situations that are red flags for U.S. digital services providers. 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.

Copyright Liability Regimes for Online Intermediaries

The Ministry of Citizenship held a consultation in 2019 on Brazil's Copyright Law.[115] 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. There is also the pressure to change the Brazilian copyright regime in order to create a press publishers' right, following the EU's adoption of a press publisher right pursuant to the Digital Single Market Copyright Directive.

Digital Taxation

Brazil is currently considering at least five different 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.[116] 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.[117]

Of particular concern to CCIA is the Social Contribution on Digital Services (CSSD), with a rate of 3 percent on the gross revenue from digital services, and 10 percent on the revenue from online betting.[118] The bill targets companies domiciled in Brazil or abroad, that have earned in

---

[115] 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/.

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

[117] *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.").

[118] KPMG, Brazil: Review of Digital Services Tax Proposals (April 14, 2021), https://home.kpmg/us/en/home/insights/2021/04/tnf-brazil-review-of-digital-services-tax-proposals.html.

Brazil a gross revenue greater than BRL 100 million (USD 17 million). Industry reports that bill has support from some members of Congress, but neither the speakers of the House and the Senate nor the Ministry of Economy endorsed any of the proposals.

Brazil's proposals share characteristics with the French Digital Services Tax enacted in July 2019, many of which contravene long-standing international taxation principles and present significant burdens for companies in the tech sector as well as the companies that rely on these services. The Brazilian Government should refrain from introducing any tax measure that is discriminatory in nature and to recommit reaching a multilateral solution to the tax challenges arising from the digitalization of the global economy. Additionally, any tax changes to reflect the digitalization of the economy should be pursued at a global level through the OECD, not unilaterally.

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.[119] The differential treatment and low *de minimis* threshold for consumer-to-consumer transactions create barriers to international trade by increasing transaction costs for Brazilian businesses while limiting consumer choice and competition amongst Brazilian businesses. Extending the *de minimis* threshold to business-to-consumer and business-to-business transactions and raising the *de minimis* threshold would help Brazil conform with international consumer standards and shopping behaviors. 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.[120]

Government-Imposed Content Restrictions and Related Access Barriers

A law designed to address "fake news" was passed in July 2020 - Internet Freedom, Responsibility, and Transparency Bill. While there were improvements from its initial draft,[121] concerns remain that some requirements would be used in a manner to pursue restrictions on speech.[122] Further, industry is monitoring developments around a possible Executive Order that

[119] 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.

[120] 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.

[121] *Brazil Senate Passes Fake News Bill*, ZD NET (July 1, 2020), https://www.zdnet.com/article/brazilian-senate-passes-fake-news-bill/.

[122] *Brazil's Bolsonaro Would Veto Bill Regulating Fake News in Current Form,* REUTERS (July 2, 2020), https://www.reuters.com/article/us-brazil-politics-fake-news-idUSKBN2433FN; FREEDOM HOUSE, *Brazil: Disinformation Bill Threatens Freedom of Expression and Privacy Online* (June 29, 2020), https://freedomhouse.org/article/brazil-disinformation-bill-threatens-freedom-expression-and-privacy-online.

would penalize firms if they enforced terms of service regarding harmful content against political leaders.

Tariff Reduction

The Ex-Tariff regime consists of the temporary reduction of the tax rate for the import of capital goods (BK), information technology and telecommunications (BIT), as shown in the Common External Tariff of Mercosur (TEC), when there is no national production equivalent. The Ex-Tariff regime promotes the attraction of investments in the country, since it exempts investments directed to productive enterprises. To attract even more investments, it is critical that Brazilian government ensures Mercosur's approval to extend the Ex Tariff regime, which will end in December 2021. Otherwise, all products that benefits from this regime, including cutting-edge technology for the Brazilian consumers, will resume its original imports tariff. The Brazilian imports tariff for ICT products, for example, is the one of the highest in the world.

G. Cambodia

Government-Imposed Content Restrictions and Related Access Barriers

Reports of censorship and mandated Internet filtering and blocking continue to rise in Cambodia.[123] Legislation passed in April 2020 grants extensive authorities to the government to restrict information online if a state of emergency is imposed.[124]

A sub-decree signed in February 2021 established the National Internet Gateway, which would create a single point of entry for internet traffic regulated by a government-appointed operator.[125] While the specifics of the implementation remain unclear, there is potential that this could be abused and misused to block online content and keep out certain foreign digital services, akin to China's "Great Firewall", raising human rights concerns.[126]

A draft Cybercrime bill has also been discussed by the Interior Ministry that could hold intermediaries liable for third party content.[127] The bill also contemplates new data localization mandates.

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

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

[125] *Cambodia's New China-Style Internet Gateway Decried as Repression Tool*, REUTERS (Feb. 18, 2021), https://www.reuters.com/article/us-cambodia-internet/cambodias-new-china-style-internet-gateway-decried-as-repression-tool-idUSKBN2AI140.

[126] *Cambodia: Internet Censorship, Control Expanded*, HUMAN RIGHTS WATCH (Feb. 18, 2021), https://www.hrw.org/news/2021/02/18/cambodia-internet-censorship-control-expanded.

[127] *Activists: Cambodia's Draft Cybercrime Law Imperils Free Expression, Privacy*, VOA (Oct. 11, 2020), https://www.voanews.com/a/east-asia-pacific_activists-cambodias-draft-cybercrime-law-imperils-free-expression-privacy/6196959.html.

H. Canada

Digital Taxation

Canada announced its plans to proceed with a DST as part of its annual Budget. The tax would be 3 percent on "digital services reliant on the engagement, data and content contributions of Canadian users" and in scope revenue include revenue derived from online marketplaces, social media, and online advertising. The thresholds would be set at firms who collect global revenue of 750 million euros or more per year, and in-scope revenue associated with Canadian users of more than $20 million per year.[128]

CCIA is concerned that despite the announcements in October regarding progress on a global solution, and the clear commitment not to proceed with any new measures, that Canada still intends to finalize this legislation by January 1, 2022.[129]

While the measure would not be imposed until January 1, 2024, after the deadline for implementation of the OECD framework, it is discouraging to see countries move forward with unilateral measures regardless. There is also a retroactive component where if the global solution is not implemented by 2024, companies are still obligated to pay the tax accrued since January 1, 2022. This would be an extremely concerning framework for other countries to follow.

Content Restrictions

Canada announced a proposed legislative and regulatory framework to "address harmful content online". The proposal includes a number of concerning proposals including 24-hour takedown requirements, content filtering and monitoring, and site-blocking.[130] The broad definition of "harmful" content could lead to requirements to take down otherwise lawful content. This follows initiatives like Germany's NetzDG law, and the UK's Online Harms Proposal. As with these overbroad proposals, it is likely to result in censorship of Canadian speech and collateral harm to U.S. companies carrying such speech. Industry also reports that there has been insufficient stakeholder involvement throughout the proposal's development.[131]

The Canadian government also introduced Bill C-10, which extends Canada's broadcasting regulations to online platforms. Under Bill C-10, the Canadian Radio-Television and Telecommunications Commission is empowered to apply new "discoverability" obligations to any site of service hosting audio or audio-visual content (including "social media services") which

[128] CCIA provided comments on the specifics of the Canada DST, *available at* https://www.ccianet.org/wp-content/uploads/2021/06/Comments-of-CCIA-Canada-Digital-Services-Tax-2021.pdf.

[129] DEPT. OF FINANCE CANADA, Statement by the Deputy Prime Ministers On New International Tax Reform Agreement (Oct. 8, 2021), https://www.canada.ca/en/department-finance/news/2021/10/statement-by-the-deputy-prime-minister-on-new-international-tax-reform-agreement.html.

[130] Gov't of Canada, Canadian Heritage, Consultation: The Government's Proposed Approach to Address Harmful Content Online, https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html.

[131] *See* Michael Geist, *Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation* (July 30, 2021), https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/.

would compel the service to give preferential treatment to Canadian content and creators.[132] This has profound censorship and digital trade implications, as it necessarily means non-Canadian audio and audio-visual communications will be demoted.

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.[133]

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.[134]

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 Personal Information Protection and Electronic Documents Act.[135] After industry concerns, the OPC determined that it would not amend the guidelines.[136] Rather, it intends to direct lawmakers to reevaluate existing law and determine whether legislative changes are needed. The Government of Quebec adopted Bill 64 in September 2021 which is privacy legislation that, amongst other things, would make data transfers extraordinarily difficult.[137] Under the new rules public and private sector entities may only transfer personal data outside the province to jurisdictions with privacy protections equivalent to Quebec's privacy law. The law is expected to come into force by 2023.

---

[132] Bill C-10, *An Act to amend the Broadcasting Act and to make consequential amendments to other Acts* Nov. 18, 2020, *available at* https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c10.html [Canada].

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

[134] 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.

[135] 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"].

[136] 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/.

[137] IAPP, *Quebec Enacts New Privacy Legislation* (Sep. 22, 2021), https://iapp.org/news/a/quebec-enacts-new-privacy-legislation/.

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.

I. 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.

J. 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.[138] 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.

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 several localization and protectionist measures.[139] 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. China also actively censors cross-border Internet traffic, blocking some 3000 sites and services, including that of many American online services. These regulations all are fundamentally protectionist and anticompetitive, and contrary to China's WTO commitments and separate commitments to the United States.[140]

[138] 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/.

[139] 2019 CCIA NTE Comments, *supra* note 135 at 34-40.

[140] 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.

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.[141] There is confusion regarding how this draft affects prior draft legislation on cross-border data and localization mandates issued pursuant to the Cybersecurity Act.[142]

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.[143] "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."[144]

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.[145] The draft amendments released on February 1, 2019 set out the following: enhanced notice and consent requirements, new requirements on personalized recommendations and target advertising, requirements on access by third parties and data integration, revised notification requirements for incident response, and requirements to maintain data processing records.[146]

The two draft Measures above are reportedly being submitted for deliberation during the National People's Congress term ending in 2023.[147]

---

[141] 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/.

[142] 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").

[143] 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/.

[144] *Id.*

[145] 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/.

[146] 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/.

[147] 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/.

In 2021, China finalized measures on the protection of security for critical information infrastructure ("CCI").[148] The measures provide a non-exhaustive list of the sectors for CII, including public communications and information services, energy, transportation, water utilities, finance, public services, e-government, and national security. Industry reports that the ever-expanding scope of CIIs and the cybersecurity review creates compliance cost and potential entry barrier to certain sectors. It is important that the various regulatory mechanisms to establish remain transparent and narrow in scope. This includes ensuring that terms such as 'national security', 'national economy and people's livelihood', and 'public interests' are not interpreted extensively

In August 2021, the Personal Information Protection Law was passed. Its extraterritorial application of data protection requirements and strict restrictions on international transfer of personal information data will add burden to multinational companies, and limit the ability of U.S. companies to operate in China.

Industry further reports data localization and cross-border data flow restrictions in various industry regulations, such as financial services, auto, ride hailing, Internet publication, mapping, and pharmaceutical sectors. The lack of necessary clarifications on data, unclear procedures for cross-border data review as well as for triggering a data security review, increase the already complex and uncertain compliance burdens. In addition to posing heavy operational burdens, these requirements can essentially act as market access barriers for FIEs, due to their high frequency of cross-border data transfer for normal operational reasons and in response to their headquarters' requests, among other reasons.

Data Security Act

In June 2021, China passed its Data Security law which created new rules and liabilities, including extraterritorial liabilities, 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.[149] The law also provides greater authority for the Chinese government to retaliate against foreign governments that impose restrictions on Chinese foreign investment or technologies. The law further states China will establish a data security review mechanism, and data processors shall obtain licenses, cooperate with national security agencies and go through data review processes for various data related activities in China.

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 has 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

[148] *China Publishes Protection Measures for Critical Information Infrastructure*, CMS LAW NOW (Aug. 18, 2021), https://www.cms-lawnow.com/ealerts/2021/08/china-publishes-protection-measures-for-critical-information-infrastructure.

[149] 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/.

positive balance of trade.[150] 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.

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 to operate in the Chinese market. 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 implements a licensing system for telecommunications business operations. Only companies established in China, after obtaining a telecom business license, can engage in telecom business activities. Foreign companies' participation in value added telecommunication (VAT) sector is highly restrictive. Based on *Telecommunications Regulations of the People's Republic of China, Classification Catalogue of Telecommunications Services,* and *Special Administrative Measures for Foreign Investment Access (Negative List) (2020 Version),* foreign companies are still denied access to the business sectors critical to cloud services, namely B11 Internet data center business, and B12 content distribution network service.

While the foreign service suppliers can earn a licensing or revenue-sharing fee through a contractual partnership with the Chinese company, the existing laws and regulations would (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 owning and operating its own data centers; (6) prohibit foreign CSPs from contracting with Chinese telecommunication carriers for Internet connectivity; (7) restrict foreign CSPs from broadcasting IP addresses within China; (8) prohibit foreign CSPs from providing customer support to Chinese customers; and (9) require any cooperation between foreign CSPs and Chinese companies be disclosed in detail to regulators.

Over the past one year, both central and some local governments announced plans to open up the VAT sector in pilot FTZs (Free Trade Zones), such as Hainan and Shanghai Lingang, yet the proposed open up has been delayed continuously.[151]

The Cybersecurity Review Measures, effective in 2020, puts in place a review process to regulate the purchase of ICT products and services by critical information infrastructure operators in China. In addition, the draft revision of Information Security Technology - Security Capability Requirements of Cloud Computing Services (GB/T 31168) and Basic Rules for the Regulation of Financial Cloud Services, community cloud model with physical separation of the servers has been proposed for critical workloads in government sector and financial service sector respectively.

---

[150] 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.

[151] *See* KPMG, *China: Plans Aimed to Develop Free-Trade Port, Hainan Island* (June 12, 2020), https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf.

These actions 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.

Backdoor Access to Secure Technologies

In October 2019, China adopted a Cryptography Law that includes restrictive requirements for commercial encryption products that "involve national security, the national economy and people's lives, and public interest," which must undergo a security assessment, arising concerns that the new Cryptography Law will lead to unnecessary restrictions on foreign ICT products and services.

Export Controls

China finalized a new export law in October 2020 that took effect on December 1, 2020.[152] 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.

Additional E-Commerce Barriers

China passed its first law regulating "e-commerce" in August 2018 which took effect in January 2019.[153] 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."[154] Requirements include the need to obtain a business license to operate, which could place a burden on small businesses.

Separately, with respect to cross-border e-commerce, Chinese government efforts against cross-border counterfeit crimes remain insufficient.

Industry reports two key problems. First, there is a lack of border measures to prevent cross-border movement of counterfeit goods, especially the sharing of necessary data on counterfeits stopped at the border with right owners to track down bad actors. Second, extraterritorial

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

[153] 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/.

[154] *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.

evidence cannot be used as formal evidence in court. For evidence of selling counterfeits seized by foreign law enforcement or recognized by judicial procedures, if the case meets the threshold for starting a criminal investigation, the Public Security Bureau should file the case and recognize the seizure value as the criminal amount to pursue the criminal liability of counterfeiters.

The Chinese government should enhance international cooperation on IPR protection, fully utilize the multilateral or bilateral mechanisms to strengthen cross-border judicial assistance, and work closely with judicial agencies in the U.S., EU, UK, ASEAN, etc. to achieve consensus on the fight against online crimes, and build the common rules for digital forensics across borders.

Electronic Payment Regulations

The People's Bank of China (PBOC) released Notification No.7 in March 2018 that restricts foreign institutions that intend to provide electronic payment services for domestic or cross-border transactions.[155] 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 licenses, 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.

K. 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.[156] Revision to the legislation in 2018 that sought to implement the U.S.-Colombia FTA copyright chapter includes no language on online intermediaries.[157] 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 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.

National Strategy on Artificial Intelligence

Colombia presented its final version of the Ethical Framework for AI,[158] a core component of its national strategy on AI. While the Framework adopted some good practices such as taking a

[155] *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.

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

[157] 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/.

[158] Presidential Advisory for Economic Affairs and Digital Transformation Presidency of the Republic of Colombia, Ethical Framework for Artificial Intelligence in Colombia (2021),

risk-based approach for AI solutions, it also included several obligations that might lead to unique standards, onerous certifications, audit of algorithms, among other concerning matters which would add undue burden to U.S. companies operating in the Colombian market.

Data Localization

While Colombia has a legal regimen that allows cross data flow (Law 1581 2012 and Circular externa SIC 02/18) and cloud friendly environment, the Ministry of Defense issued a regulation with data localization requirements in March 2021. This regulation conflicts with the national digital transformation plan adopted by the National Government, and departs from the guidelines and standards issued by the Presidential Council for Economic Affairs and Digital Transformation and the ICT Ministry. These include the Cloud Computing Manual, issued in February 2021, and the Cloud Computing Guide G.ST.02., issues in May 2018. This is particularly true with respect to the definitions and scope of cloud services, as well as the absence of data localization requirements. It further conflicts with Presidential Directive 03 of 2021, which defined the guidelines for the use of cloud services, artificial intelligence, digital security and data management in public entities of the executive branch of national order.

De Minimis Rules

The U.S.-Colombia Free Trade Agreement (the "Agreement") was signed on November 22, 2006 and entered force on May 15, 2012. Under Article 5.7(g) of the Agreement, the parties established a *de minimis*, the value threshold below which no customs duties or taxes are charged on imported goods. The Agreement's *de minimis* threshold is set at $200. In December 2012, a tax reform implemented the VAT benefit, but the Colombian government only fully implemented it regarding customs duties in August 2020. The application of *de minimis* is to all express and postal shipments arriving into Colombia, no matter the country of origin.

On September 8, 2021, the Colombian Congress approved a new tax reform that adjusted the application of the *de minimis*. The VAT exemption for shipments under $200 will limit the application to Free Trade Agreement partners that explicitly include such VAT exemption (i.e., U.S.) and for shipments with no commercial use. Industry is monitoring how the government defines 'shipments with no commercial use' and is concerned that this will impact the ability to leverage this shipment method and compliance with the Agreement.

L. Cuba

Government-Imposed Content Restrictions

There have been many cases of the Cuban government disrupting access or blocking certain Internet services to stifle political dissent and organization.[159] Government ownership and

https://dapre.presidencia.gov.co/dapre/SiteAssets/documentos/ETHICAL%20FRAMEWORK%20FOR%20ARTIFICIAL%20INTELLIGENCE%20IN%20COLOMBIA.pdf.

[159] *Cuba's Social Media Blackout Reflects an Alarming New Normal*, WIRED (July 13, 2021), https://www.wired.com/story/cuba-social-media-blackout/. ("Cuba's national telecommunications company Etecsa, which offers both broadband and Cubacel mobile data, was founded in 1994. But the government historically has heavily restricted who could have an internet connection and only began slowly opening up access in 2016. In 2019 the regime first began allowing limited connections in private homes and businesses. The combination of total

control of the *Empresa de Telelcommunicaciones de Cuba S.A*, the telecommunications services provider for the country, increases the risk of censorship. In response to political protests, Cuban authorities have blocked access to many U.S. social media platforms including Facebook, WhatsApp, and Twitter in November 2019, and most recently in July 2021.[160]

M. Czech Republic

Digital Taxation

Announced by the Ministry of Finance in July 2019,[161] the Czech Republic is currently finalizing its digital tax.[162] 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.[163] 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.[164] The effective date has been delayed. Policymakers have cited the need to tax U.S. companies despite support for an OECD solution.

N. European Union

The European Commission is pursuing an expansive agenda and new regulatory frameworks designed to bring the EU closer to achieving "technological sovereignty". European politicians have stated that the purpose of technological autonomy is to create a "new empire" of European industrial powerhouses to resist American rivals.[165] This includes regulations on industrial policy, 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

---

control and nascent user base makes it relatively easy for the government to carry out both widespread internet shutdowns and platform-specific blocking.").

[160] *Id*. *Faced with Rare Protests, Cuba Curbs Social Media Access, Watchdog Says*, REUTERS (July 13, 2021), https://www.reuters.com/world/americas/cuba-curbs-access-facebook-messaging-apps-amid-protestsinternet-watchdog-2021-07-13/

[161] 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.

[162] *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.

[163] *KPMG Digital Taxation Report*, *supra* note 44, at 7.

[164] *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/.

[165] 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.

Structured dialogues such as the EU-U.S. Trade & Technology Council will be key for U.S. policymakers to raise concerns with diverging approaches to digital governance that discriminates against U.S. services.[166]

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. A new EU Data Act, scheduled early December, could include several data transfer restrictions for non-personal data as well as cloud service restrictions even where data is stored in the EU.[167] To mitigate concerns about non-EU government access laws and practices over EU sensitive corporate data, the European Commission is considering requiring cloud providers to disclose non-EU government data access requests to business users and to notify the European Commission of all non-EU extraterritorial government data access laws to which they are subject. The European Commission could then publicise the information received from U.S. vendors. Additional obligations for cloud providers could include putting in place "reasonable legal, technical and organisational measures", similar to what is required under Standard Contractual Clauses in the GDPR. This could entail companies having to assess to what extent non-EU government data access laws may apply to their services, whether the data is stored abroad or within the EU, and identify remedies to circumvent the application of non-EU laws.

The November 2020 Data Governance Act (DGA)[168] proposes restrictions to the transfer of certain non-personal data held by public agencies, be they data protected by EU trade secrets or intellectual property laws. These restrictions are similar to the General Data Protection Regulation ranging from 'adequacy decisions', consent, standard contractual clauses, as well as an outright ban for sensitive non-personal data.[169] However, the GDPR governs restrictions for personal data, while the DGA extends these obligations to non-personal data.

[166] Press Release, CCIA Offers Recommendations Ahead of the First Meetings of the EU-U.S. Trade & Technology Council (Sep. 24, 2021), https://www.ccianet.org/2021/09/ccia-offers-recommendations-ahead-of-the-first-meetings-of-eu-u-s-trade-technology-council/.

[167] Legislative options under consideration can be found in the European Commission Inception Impact Assessment on the Data Act, May 2021, available on https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en

[168] Proposal for a Regulation of the European Parliament and of the Council on European Data Governance ("Data Governance Act"), Com/2020,767, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.

[169] See Article 5(4), (6), (9)-(11) of the proposed Data Governance Act, available on https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0767&from=EN.

The December 2020 new cybersecurity legislation (NIS2)[170] would entail increased security and incident notification requirements as well as ex ante supervision for "essential" service providers (e.g. cloud providers, operators of data centers, content delivery networks, telecommunications services, Internet Exchange Points, DNS). This would also include the obligation for such providers to be certified against an EU certification scheme to be developed under the EU Cybersecurity Act (CSA).[171] One of the first EU cybersecurity schemes under development relates to cloud services and it is subject to intense debates between ENISA (EU cybersecurity agency) and Member States. Some Member States are pushing ENISA to include in this scheme data localization requirements and jurisdictional restrictions that are going beyond security controls.

This regulatory trend towards data localization 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.[172]

- French President Macron stated that Europe should not rely "on any non-European power" for data security.[173]

- 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."[174]

- 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

[170] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148,

COM/2020/823 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN.

[171] See Article 21 of the proposed NIS2 Directive allowing Member States to require a European cybersecurity scheme developed under the Data Act. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

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

[173] *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.

[174] 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.[175]

- U.S. cloud providers have been relegated to observers in the Franco-German-led GAIA-X cloud project.

The discussion at EU level also reflects recent national preferences for data localization:

- In May 2021, the French government adopted a National Cloud Strategy requiring all government agencies and nudging enterprises to select vendors that have a French cybersecurity certification requiring data storage in France or in the EU.[176] To date, only French companies have obtained or are looking to obtain this certification.[177]

- The Italian Cloud Strategy (September 2021)[178] bears many similarities with the French strategy. However, it also explicitly requires the storage and processing of encryption keys in Italy. This requirement will apply for any certified (or 'qualified') commercial cloud services that may be used to host local and central administrations' "critical" and "strategic" data and services. The Strategy also implies the advent of national localisation requirements for other data and services, beyond encryption keys. The roll-out of a new National Strategic Hub, made of at least 4 data centres "geographically distributed throughout the country", will "offer (…) licensed private / hybrid cloud and qualified private cloud services". It "will [also] be entrusted to qualified national providers" to host, e.g., "encryption tools integrated on a Public Cloud". The definitions of "critical" and "strategic" data and services will be later decided by the Italian national cybersecurity agency and the Department for Digital Transformation.

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.[179] Following the original announcement in 2019 by Germany, in June 2020, German Federal Minister of Economic Affairs and Energy Peter Altmaier and the French Minister of Economy and Finance Bruno Le

---

[175] 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.

[176] Stratégie Nationale pour le Cloud, 17 May 2021, *available at* https://www.numerique.gouv.fr/uploads/Strategie-nationale-pour-le-cloud.pdf.

[177] Cloud services and companies which are 'SecNumCloud' certified are available at p. 11 of https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf; Cloud services and companies which are currently undergoing a certification are available at https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/.

[178] Data localization considerations in the Italian Cloud Strategy can be found on https://assets.innovazione.gov.it/1631016886-strategiaclouditalia2021en.pdf, pages 11-14)

[179] 2019 CCIA NTE Comments, *supra* note 135 (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.)

Maire unveiled details on plans to create Europe's own cloud services, titled "GAIA-X".[180] 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."[181] GAIA-X company members commit to letting customers demand that their data be processed and stored exclusively in the EU.[182]

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.[183] 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-Evidence Regulation,[184] an 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.[185] Among others, several Member States, supported by the European Commission,[186] are looking to support a European multi-cloud infrastructure alternative to the existing offer. To do so, Member States are expected to inject subsidies into several European cloud vendors while exempting them from EU state aid rules. France and Germany have

---

[180] 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.

[181] 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.

[182] Gaia-X Draft Policy Rules Document (2021), *available at* https://www.gaia-x.eu/sites/default/files/2021-05/Gaia-X_Policy%20Rules_Document_2104.pdf.

[183] *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.

[184] 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/.

[185] 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.

[186] European Comm'n, *Europe Remains Open, But on Our Terms* (May 5, 2021), https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-remains-open-our-terms_en.

spearheaded this Important Project of Common European Interest, or 'IPCEI', for cloud, and 11 Member States have already opened calls for expression from local vendors.[187] This IPCEI would add to 10 billion euros pledge that 25 Member States and the European Commission had already signed up to in late 2020.[188]

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) went into effect on May 25, 2018.[189] 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, several 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.[190] The ruling created immediate legal uncertainty for thousands of companies, most which are SMEs.

Since July 2020, thousands of companies continue to be impacted by the resulting legal uncertainty for transatlantic data transfers, restrictive interpretations of the ruling risk triggering additional compliance and operational challenges. 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.[191]

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, European regulators have laid down very strict requirements on how companies can or cannot transfer EU personal data to 'non-adequate' countries.[192] In fact, the collective impact of the Recommendations of the European Data Protection Board would prevent the

[187] More information about the preparatory work for the Cloud IPCEI available on https://www.bmwi.de/Redaktion/EN/Pressemitteilungen/2021/07/20210709-cloud-ipcei-entering-next-phase.html

[188] *See* Joint Declaration Building the next generation cloud for businesses and the public sector in the EU, October 2020, *available at* https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe

[189] 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"].

[190] 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

[191] *See* Industry Letter, July 14, 2021, available at ://www.ccianet.org/wp-content/uploads/2021/07/2021-07-14-Joint-industry-letter-Transatlantic-industry-urge-swift-agreement-on-EU-US-data-flows.pdf/.

[192] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data available on https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

majority of data transfers outside the EEA resulting in significant economic and social drawbacks without corresponding benefits in the protection of European citizens' data.[193] This has led several regulators to issue enforcement decisions that impose a quasi-data localization requirement in Europe.[194] Furthermore, some regulators appear to require U.S. and non-EU companies to adopt "additional requirements" even if data stays in Europe.[195]

In the trade negotiation context, it is unfortunate that the EU's proposed text to facilitate cross-border data flows and digital trade includes provisions that would increase the likelihood of data localization rather than reduce barriers.[196] 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.[197] The proposal seeks to expand the existing Directive, which only applies to telecommunication services, to all "electronic communication services" including over the top services.[198] 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."[199] This is based on a flawed understanding of the services at issue and it is ignoring that the Internet

[193] *See* CCIA Comments on draft EDPB Recommendations on supplementary measures available on https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/12-21-2020_-_ccia_response_to_the_edpb_on_schrems_ii_guidelines.pdf

[194] Keir Lamont, *The Monkey's Pause: Mailchimp Data Transfers Halted in German Schrems II Inquiry*, DISRUPTIVE COMPETITION PROJECT (April 2021) https://www.project-disco.org/european-union/040621-the-monkeys-pause-mailchimp-data-transfers-halted-in-german-schrems-ii-inquiry/, and Keir Lamont and Alexandre Roure, *Portuguese Decision Another Foreboding Sign for Global Data Transfers*, DISRUPTIVE COMPETITION PROJECT (June 2021) https://www.project-disco.org/european-union/050721-portuguese-decision-another-foreboding-sign-for-global-data-transfers/.

[195] Keir Lamont & Alexandre Roure, *Portuguese Decision Another Foreboding Sign for Global Data Transfers*, DISRUPTIVE COMPETITION PROJECT (June 2021) https://www.project-disco.org/european-union/050721-portuguese-decision-another-foreboding-sign-for-global-data-transfers/

[196] Christian Borggreen, *How the EU's New Trade Provision Could End Up Justifying More Data Localisation Globally*, DISRUPTIVE COMPETITION PROJECT (May 14, 2018), http://www.project-disco.org/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.").

[197] 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"].

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

[199] *Id*. at recital 6.

has flourished largely due to *not* treating over-the-top services like traditional telecommunications providers.

Foreign Subsidies Proposal

In May 2021, the European Commission presented a proposed regulation on foreign subsidies distorting the internal market.[200] Under the new rules, the Commission would have broad powers to receive sensitive business information involving non-EU government contracts. The Commission will also have broad discretion to decide whether a non-EU subsidy would distort the EU single market and impose strict sanctions.

The proposal broadly defines non-EU subsidies as any financial contribution provided directly or indirectly by a non-EU Government that confers a benefit and is limited to an individual business or industry or several businesses or industries. This includes, but is not limited to, tax credits, tax exemptions, film credits, preferential tax treatment, cash grants, and the purchase of goods and services by government bodies.

The proposal then introduces three tools to investigate distortions into the EU single market: Tool 1 is a general investigative tool giving the Commission the ability to investigate any situation (without any justificatory threshold) based solely on a "suspicion" of distortion. This will force companies to give the Commission access to businesses' complete financial records and details of business transactions for the last 10 years (including sensitive procurement contracts), including onsite inspections and staff interviews. Tool 2 applies to large mergers and acquisitions (M&A) and Tool 3 tackles large EU public procurement. Tools 2 and 3 obligate businesses to disclose all foreign "subsidies" received in the last 3 years when participating in M&A and public procurement activities, respectively.

If foreign subsidies are found to distort the EU single market, companies may be subject to disciplinary measures, ranging from fines of up to 10 percent of global turnover, divestments from EU markets and assets, exclusion from on-going and future procurement for up to 3 years, publication of R&D results, and prohibitions on M&A.

In this context, the proposal is likely to discourage U.S. investments in the EU that are supported by foreign financial contributions, even if they do not have a distortive effect. The vagueness of the proposal creates the risk that U.S. firms might be suspected of benefiting from distortive foreign subsidies.

The legal uncertainty due to broad definitions and the tough redress measures will undoubtedly reduce the openness of the European economy to U.S. capital inflows.
The regulation would capture any company receiving any form of benefits or compensation from a non-EU state authority.[201] While this proposal will affect all foreign companies doing business

[200] Proposal for a Regulation of the European Parliament and of the Council on Foreign Subsidies Distorting the Internal Market, 2021/0114 (COD), *available at* https://ec.europa.eu/competition/international/overview/proposal_for_regulation.pdf.

[201] For example, the U.S. and the UK are singled out where proposal explains the correlation between FDI origins and subsidy spenders. *Id.* At 51.

in Europe and EU businesses doing business abroad, the European Commission has explicitly linked the proposal to its industrial policy ambitions in the tech space.[202]

Market-Based Regulations

In recent years, U.S. technology firms have identified concerns around a rise in protectionism relating to digital competition in the form of targeted regulation and increased antitrust actions against U.S. firms.

The Digital Markets Act (DMA) was introduced in December 2020. Under the proposed text, companies that operate a "core platform service" must notify the European Commission upon meeting pre-defined thresholds for European turnover, market capitalization, and number of European consumer users and business users. These thresholds have been set at levels where primarily U.S. technology companies will fall under scope, and some policymakers have proposed amending the thresholds to ensure that only U.S. firms fall under scope.[203] The list of "core platform services" furthermore carves out non-platform-based business models of large European rivals in media, communications, and advertising.

Once under the scope of the DMA, companies will be prohibited from engaging in a range of pro-competitive business practices (e.g., benefiting from integrative efficiencies). Furthermore, the Commission will be vested with gatekeeping authority over approval for future digital innovations, product integrations, and engineering designs of U.S. companies. The DMA would also in some cases compel the forced sharing of intellectual property, including firm-specific data and technical designs, with EU competitors, effectively requiring U.S. firms to subsidize rivals to promote competition. Unlike traditional competition enforcement, the Commission will be able to impose these interventions without an assessment of evidence, of any effects-based defenses, or of pro-competitive justifications put forth by the companies targeted.

In a number of areas, the DMA would break with longstanding transatlantic regulatory and competition norms, depriving companies of due process and creating a politicized alternative to traditional, process-oriented competition investigations.

CCIA notes that the Commission has hinted at other sector-specific legislative proposals, including in the mobility, delivery and logistics sector, which would further reduce the competitiveness of U.S. companies.

Digital Taxation

Since the introduction of a now-abandoned, digital services tax by the European Commission in 2018,[204] national measures have proliferated on a global scale. Many countries have used the

[202] Thierry Breton, *The Geopolitics of Technology* (July 27, 2021), https://www.linkedin.com/pulse/geopolitics-technology-thierry-breton/.

[203] *EU Should Focus on Top 5 Tech Companies, Says Leading MEP*, FINANCIAL TIMES (May 13, 2021), https://www.ft.com/content/49f3d7f2-30d5-4336-87ad-eea0ee0ecc7b.

[204] For background, the European Commission presented a package of two digital tax proposals in March 2018. 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

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.

Further, the Commission is considering introducing a "digital levy" in 2021. The proposal was scheduled to be presented in July 2021, but officials subsequently announced its delay until the end of the year.[205] 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.[206]

VAT: Complex VAT registration and compliance requirements in intra-EU trade

The cost of compliance with VAT requirements when selling into the EU Single Market is higher for non-EU businesses than for EU businesses and constitutes a significant non-tariff barrier. The current EU VAT registration system is generally found to be fragmented, complex and particularly costly for SMEs. As a result, access to EU trade is affected.

Online Content Regulations

The Commission proposed a "Digital Services Act" (DSA) in December 2020, which will further depart from transatlantic norms on liability for online services.[207] New rules will be considered for illegal content, counterfeiting, collaborative economy services, or product safety. The Commission wants to "set global standards which could be promoted at international level."

The DSA imposes new obligations such as due diligence obligations: notice & action, 'know your business customer', transparency of content moderation, and cooperation with authorities. Large platforms, notably U.S. companies, having 45 million active users, will have to comply with additional obligations such as strict transparency and reporting obligations, yearly audits, disclose the main parameters used in their recommender systems, and appoint a compliance officer. Fines can go up to 6 percent of annual turnover.

Some lawmakers have seized on the DSA as an opportunity to regulate a variety of other topics, some even in much detail. Some lawmakers have even gone as far as adding an entire new section targeted at marketplaces or online advertising, which would undermine the horizontal normative purpose of the DSA proposal.

Online marketplaces, including many U.S. companies, could become liable for every product sold through their channels. If so, online marketplaces will have to adopt a very cautious approach, especially with the high fines set out in the DSA. In case of doubt, online marketplaces would

companies' gross revenues from making available advertisement space, intermediation services, and transmission of user data. As explained in other country sections of these comments, national DSTs largely reflect this framework, with variations on rate and covered digital activities.

[205] *EU Delays Digital Levy as Tax Talks Proceed*, N.Y. TIMES (July 12, 2021), https://www.nytimes.com/2021/07/12/us/politics/eu-digital-tax.html.

[206] *CCIA DST Comments*, *supra* note 44.

[207] 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/.

bring products down, meaning fewer products would become available online. Some categories of products considered too risky, could even be closed. CCIA has encouraged EU lawmakers to address sector specific concerns in a sector-specific bill, e.g., the June 2020 General Product Safety Regulation (GPSR) proposal.[208] The GPSR seeks to update the existing Product Safety Directive to respond to new challenges related to online purchases including via marketplaces.[209]

Some European policymakers are threatening to severely limit or ban targeted advertising. This would impact European as well as U.S. companies.

Copyright Liability Regimes for Online Intermediaries

On May 17, 2019, the Copyright Directive was published in the Official Journal of the European Union.[210] The Member States had until June 7, 2021 to implement this new EU law. Only France, Denmark, Germany, the Netherlands, Hungary, Croatia, and Malta have implemented the new rules as of October 2021. The European Commission has opened an infringement procedure against the remaining member states for not transposing the bloc's copyright rules in time.[211]

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.

Only four days before the deadline, the European Commission released guidelines on implementation of Article 17 in June 2021.[212] 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.

---

[208] European Comm'n, The General Product Safety Directive, https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/consumer-product-safety_en (last visited Oct. 25, 2021).

[209] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety [E.U.], https://eur-lex.europa.eu/legalcontent/EN/ALL/?uri=CELEX%3A32001L0095.

[210] 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.

[211] Press Release, European Comm'n, Copyright: Commission calls on Member States to comply with EU rules on copyright in the Digital Single Market (July 26, 2021), *available at* https://digital-strategy.ec.europa.eu/en/news/copyright-commission-calls-member-states-comply-eu-rules-copyright-digital-single-market.

[212] Communication from the Comm'n to the European Parliament and the Council, Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1625142238402&uri=CELEX%3A52021DC0288.

As Member States transpose the EU Directive and issue 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 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.

Member States are currently working on implementation, with many Member States in final stages of legislation. It is important that Member States implement Article 17 in a harmonized fashion by transposing the text verbatim, rather than creating bespoke requirements, as is the case in Member States such as Germany.

USTR should work with its EU counterparts to ensure the Directive is implemented in a technologically neutral and future proof manner. EU countries should not in their implementing laws mandate either the use of a technological solution nor impose any specific technological solutions on service providers in order to demonstrate best efforts. Any requirement to render content unavailable must be proportionate and allow platforms the latitude needed to manage their systems without negatively impacting lawful user expression and legitimate uses of creative content.

It is imperative that national implementation does not impact on the freedom of contract and therefore diverge from the terms of the Directive by imposing mandatory licensing, "must carry and must pay" obligations. Moreover, EU Member States should refrain from inserting new payment obligations for authors and performers into their national laws (such as recently adopted in Germany) which would create commercial confusion that affects all stakeholders in the value chain.

CCIA remains concerned with the Copyright Directive's Article 15 and the creation of a press publishers' right.[213]

As EU countries are now moving forward with the implementation, they should ensure that national legislation follows the terms of the Directive as closely as possible in order to ensure the maximum harmonization of rules in the EU and respect the exceptions and limitations inserted in the Directive (including the exceptions inserted in the Directive in Article 15 which allow linking and short news extracts to be posted without the need for a license) in order to maintain a fair balance between the various fundamental rights. Moreover, it is imperative that national implementation does not impact on the freedom of contract and therefore diverge from the terms of the Directive by imposing mandatory licensing, "must carry and must pay" obligations.

[213] *Id.*

Finally, EU Member States should refrain from inserting new payment obligations for authors and performers into their national laws (such as recently adopted in Germany) which would create commercial confusion that affects all stakeholders in the value chain.

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.[214] The ruling honors EU residents' 'right to be forgotten' (RTBF). The decision concludes that a service provider subject to the RTBF is not obligated to de-index outside of the EU.[215] 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.[216] 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.[217]

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.[218] 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

[214] 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.

[215] *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).

[216] *Id.* at ¶ 72.

[217] 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").

[218] GDPR art. 17.

since the policy went into effect.[219] 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

On April 21, 2021, the European Commission presented its proposal for a regulation on Artificial Intelligence. The proposal is structured around horizontal risk-based rules, which classifies risks as unacceptable, high, limited and minimal. The focus of the regulation is on high-risk AI systems that can create an adverse impact on people's safety or fundamental rights. The AI regulation lists high-risk applications that are subject to certain additional obligations, including a conformity assessment, auditing requirements, and post-market monitoring. U.S. providers will be subject to the regulation's requirements if they make their AI system available in the EU. The law will also apply to both providers and users of AI systems where the "output" of that system is used in the EU. Fines can go up to 6 percent of annual global turnover. The broad definition of so-called "high-risk" application, cumbersome compliance requirements and steep fines, create new compliance burdens for U.S. companies doing business in the EU.

Cybersecurity Regulations

The December 2020 EU cybersecurity legislation (NIS2) entails increased security and incident notification requirements as well as *ex ante* supervision for "essential" service providers (e.g. cloud providers, operators of datacenters, content delivery networks, telecommunications services, Internet Exchange Points, DNS). This would also include the obligation for such providers to be certified against an EU certification scheme to be developed under the EU Cybersecurity Act (CSA).[220] One of the first EU cybersecurity schemes under development relates to cloud services and it is subject to intense debates between ENISA (EU cybersecurity agency) and Member States. Some Member States are pushing ENISA to include in this scheme data localization requirements and jurisdictional restrictions that are going beyond security controls.

O. 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.[221]

---

[219] 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.

[220] See Article 21 of the proposed NIS2 Directive allowing Member States to require a European cybersecurity scheme developed under the Data Act. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

[221] *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.").

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.[222] 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).

Additional E-Commerce Barriers

Industry reports several 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.

P. Finland

Data Localization

In September 2021, the Finnish Institute for Health and Welfare launched a consultation regarding additional restrictions for the processing and storage of Finnish healthcare data. According to the draft decrees issued, systems that involve the provision of health and care services, and systems that contain particularly sensitive data (i.e., patient and pharmaceutical data systems) would be subject to a localisation requirement. According to the draft decrees, systems handling data that is considered necessary in abnormal situations (contingency or emergency planning) must continue to operate even when network connections are limited to Finland. The physical location limitation also covers administration, backups and other maintenance solutions. Requirements also include a restriction on governance authorities of other countries having direct or indirect access to the data.

If implemented, cloud service providers without local data centers will not be able to access and support most the healthcare sector in Finland. Industry is currently working to change this requirement together with cloud service providers and there is a good possibility that this threat can be mitigated. Absent mitigation, this will pose a barrier that can harm competition in Finland and restrict the free operation of the healthcare market, in particular for international services.

Restrictions on Cloud Services

In a communication issued in 2018, the Finnish Ministry of Finance announced its intention to introduce requirement for companies in the financial sector to build back-up systems in Finland in the event of exceptional circumstances and serious disruptions. According to this, in-scope

[222] *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.

companies would be subject to precautionary measures to maintain in Finland such information systems and information resources that are necessary for the uninterrupted operation of the financial markets. Effectively, this could represent an indirect data localization requirement, presenting a market barrier and a risk to free market and competition in Finland for cloud services which don't have local data centers. In July 2020, the FIN-FSA requested entities under scope to submit by December 31, 20201 an entity-specific plan on how to ensure the operability and accessibility of critical services for end customers in circumstances where foreign service provision is completely unavailable. Firms' preparedness plans were requested to inform the work of the Ministry of Finance, with a view to issue legislation on this in 2021. Due to extensive resistance from both the FS industry and CSPs, the issue is currently on hold with no new legislation communicated from the Ministry of Finance during this year. The issue has not, however, officially been put to the side and thus requires continuous monitoring.

Q. France

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*").[223] 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" based on 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.[224] 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" based on race, religion, sexual orientation, gender identity or disability.[225] 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).

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

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

[225] *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/.

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.[226] The tax is applied retroactive to January 1, 2019, with the first pay date in November 2019. The tax carries a high revenue threshold, effectively targeting leading U.S. technology firms operating in France while carving out most French firms that offer the same services. French Finance Minister Bruno Le Maire has regularly referred to the tax as a "GAFA tax" and stated that the goal is to target the "American tech giants" for special taxation.[227] French Government sites and representatives of the French National Assembly and Senate refer to the French DST as a "GAFA" tax and cite specific American companies in reports.[228] Based on French officials' own admission, the majority of firms that will pay the tax will be American.[229]

CCIA supports USTR's decision to pursue a Section 301 Investigation under the Trade Act of 1974 regarding the French DST 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.

While the most appropriate action would be an immediate withdrawal of existing DSTs in exchange for terminating the Section 301 investigations, CCIA is supportive of the compromise reached by the United States, Austria, France, Italy, Spain, and the United Kingdom regarding

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

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

[228] *See, e.g.*, Assemblée nationale, Projet de loi de finances pour 2019, http://www.assembleenationale.fr/15/cri/2018-2019/20190108.asp (representatives making multiple reference on the intent of France to introduce a tax on GAFA and "ces géants du numérique souvent américains"); Remarks of M. Benoit Potterie, Assemblée nationale Commission des finances, de l'économie générale et du contrôle budgétaire, Apr. 2, 2019, http://www.assemblee-nationale.fr/15/cr-cfiab/18-19/c1819064.asp (citing the need to tax the digital giants ("des géants du numérique") and identifying the "GAFA (Google, Amazon, Facebook, Apple)"); "); Remarks of Mme Sabine Rubin, Assemblée nationale Commission des finances, de l'économie générale et du contrôle budgétaire, Apr. 2, 2019, http://www.assemblee-nationale.fr/15/cr-cfiab/18-19/c1819064.asp (stating that "Sur le fond, taxer davantage les grandes multinationales, en particulier les GAFA, est un souhait louable et partagé sur tous les bancs de cette commission et, je le suppose, de notre Assemblée." [Taxing more large multinationals, in particular the GAFA, is a laudable and shared wish by this commission and our Assembly.]).

[229] Boris Cassel & 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.].

existing measures.[230] CCIA encourages policymakers to continue work on swift implementation of the global framework and removal of the DST.

Data Localization

France first indicated that it will direct resources to build a national "trusted cloud" in 2019.[231] 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.[232]

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 infrastructure.[233] This serves as a protectionist barrier for U.S. cloud service providers in the public sector in France.

R. 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.[234] The NetzDG law mandates removal of "manifestly unlawful" content within 24 hours, and provides for penalties of up to 50 million euros.[235] 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"[236] have led to companies removing lawful content, erring on the side of

[230] *Unilateral Measures Compromise*, *supra* note 41.

[231] 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.").

[232] *Id.*

[233] 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.

[234] 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.

[235] Id. § 3(2).

[236] 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 publicly available. *See Germany: Social Media Platforms to Be Held*

caution in attempts to comply.[237] 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[238] and groups have expressed concerns about its threats to free expression.[239]

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 Russia, Singapore, Turkey, and Venezuela.[240] A similar law came into force in Austria in April 2021,[241] another one is in the pipeline in France,[242] and drafts have either been released or are expected to be released shortly in Poland and Denmark.[243] Cases arising under this law will also have implications on extraterritoriality.[244]

In a 2020 review of the law, the German legislator added several obligations through two legislative packages,[245] including the obligation to offer appeals for all content takedown decisions in Germany, and the obligation to proactively refer data (including content, user name and time stamp) to the German Federal Criminal Police Office.

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/.

[237] *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.

[238] *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.

[239] *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.").

[240] 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/.

[241] Kommunikationsplattformen-Gesetz (Communication Platforms Act, CPA) - https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20011415.

[242] Article 42 LOI n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République - https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043964778.

[243] Available at https://www.dr.dk/nyheder/indland/hvis-sociale-medier-bliver-tvunget-til-fjerne-indhold-kan-det-skubbe-ytringsfriheden.

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

[245] Available at: Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes - https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl121s1436.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1436.pdf%27%5D__1634814582691[Germany]

; Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität - https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl121s0441.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s0441.pdf%27%5D__1634814625497 [Germany].

The NetzDG (and similar laws in other EU Member States) likely violate the EU law country of origin principle and not only undermine the EU Digital Single Market but also create barriers for conducting business.

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".[246] 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 in this regard. U.S. cloud service providers could be disadvantaged from operating in these markets because of these protectionist measures. Partly, the project is viewed as an alternative to transatlantic data transfer with the objective to force international operators to store their data solely within the EU.

Asymmetry in Competition Frameworks

Germany recently reformed its competition rules, with a new law effective January 19, 2021.[247] The rules were amended to de-emphasize causality requirements and the Federal Cartel Office (FCO) was provided with completely new enforcement instruments, especially for digital platforms, providing much lower intervention thresholds and limiting possibilities for judicial review.

Under the new rules there is a two-step procedure: the FCO needs to first designate companies which have "paramount importance for competition across markets" (PICAM) under Section 19(a)(1) and can then prohibit, even as a preventive measure, "companies of paramount significance for competition across markets" from carrying out certain abusive actions (e.g., self-preferencing) under Section 19(a)(2). Both steps can be combined in one procedure. Section 19a creates an entirely new group of undertakings that will become subject to scrutiny by the FCO: companies that are active on multi-sided markets and have "paramount significance for competition across markets" under Section 19(a)(1). Where the FCO finds that a company has paramount cross-market relevance in the first step, it may in the second step issue an order under Section 19(a)(2) prohibiting the company from engaging in a number of "abusive" practices, such as: self-preferencing, abusive leveraging, data processing, and hampering of portability/interoperability. While these practices can be objectively justified by the company, the burden of proof for such justification lies with the company concerned. This makes it significantly easier for the FCO to use its new intervention powers, particularly since the company will sometimes not have the means of obtaining market-wide information necessary to

[246] 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.

[247] Das Zehnte Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein Wettbewerbsrecht 4.0 (The Act against Restraints of Competition) https://www.gesetze-im-internet.de/englisch_gwb/.

meet that burden of proof. Only the Federal Court of Justice has jurisdiction for appeals against Section 19a decisions of the FCO, eliminating the Düsseldorf Higher Regional Court role of judicial scrutiny as first instance review for appeals against FCO decisions.

Many of these rules are starkly inconsistent with longstanding U.S. and global competition norms and effectively serve as trade barriers. Most importantly, the new competition rules were written to be enforced solely against U.S. companies. Current investigations under this new regime are limited to U.S. tech companies.

S. Hong Kong

National Security Law

The national security law was promulgated in Hong Kong in June 2020.[248] It allows the Hong Kong authorities to request message publishers, platform service providers, hosting service providers and/or network service providers to remove a message deemed to constitute an offense endangering national security; restrict or cease access by any person to the message; or restrict or cease access by any person to the platform or its relevant parts. The Hong Kong authorities have reportedly demanded Internet service providers to block access to websites in Hong Kong.[249] As noted elsewhere in these comments further, website blocks are barriers to maintaining a free and open Internet which is critical to digital trade.

Cybersecurity of Critical Information Infrastructure bill

The Hong Kong government announced a plan to introduce a bill to strengthen the cybersecurity of critical information infrastructure in Hong Kong in 2022. Internet service providers may be included and considered "critical".[250] At time of filing, further details are not available. However, as the policy develops, USTR should ensure that no restrictions on cross-border data flows and no data infrastructure localization mandates should be included as part of the new law. Any new data localization requirements will put U.S. companies at a competitive disadvantage vis-à-vis their Chinese and Hong Kong competitors.

T. 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.[251] The

[248] See *How Hong Kong's Security Law is Changing Everything*, BLOOMBERG (Oct. 5, 2021), https://www.bloomberg.com/graphics/2021-hong-kong-national-security-law-arrests/.

[249] *Hong Kong Telecoms Provider Blocks Website for First Time Citing Security Law*, REUTERS (Jan. 14, 2021), https://www.reuters.com/article/us-hongkong-security-censorship/hong-kong-telecoms-provider-blocks-website-for-first-time-citing-security-law-idUSKBN29J0V6.

[250] *Hong Kong Policy Address: New Cybersecurity Law to Protect 'Critical Infrastructure'*, HKFP (Oct. 6, 2021), https://hongkongfp.com/2021/10/06/hong-kong-policy-address-new-cybersecurity-law-to-protect-critical-infrastructure/.

[251] WORLD TRADE ORGANIZATION, *World Trade Statistical Review 2018* (2018), *available at* https://www.wto.org/english/res_e/statis_e/wts2018_e/wts2018_e.pdf at 166; MCKINSEY GLOBAL INSTITUTE, *Digital India: Technology to Transform a Connected Nation* (Mar. 2019), *available at* https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation ("India is one of the largest and fastest-growing markets for digital consumers, with 560 million

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 fifth consecutive year.[252] 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.[253] 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.[254]

The new equalization levy follows 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" (SEP) in 2018, and the relevant provisions became effective from FY April 1, 2021 onwards.

---

internet subscribers in 2018, second only to China. Indian mobile data users consume 8.3 gigabits (GB) of data each month on average, compared with 5.5 GB for mobile users in China and somewhere in the range of 8.0 to 8.5 GB in South Korea, an advanced digital economy. Indians have 1.2 billion mobile phone subscriptions and downloaded more than 12 billion apps in 2018.").

[252] *Ease of Doing Business in India*, THE WORLD BANK, https://www.doingbusiness.org/en/data/exploreeconomies/india (last accessed Oct. 26, 2021).

[253] *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.

[254] *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.

In May 2021, the government notified the threshold limits for triggering the SEP provisions based on revenue or user-based threshold. The non-resident entities would be subject to SEP provisions if they derive revenue of INR 20 million (~$267,000) from India or when they are in "systematic and continuous soliciting of business activities or engaging in interaction" with at least 300,000 Indian users.[255]

Customs Duties on Electronic Transmissions

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

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

CCIA has raised concerns with the government of India's practices around data localization in previous NTE comments.[257] 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).[258]

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

---

[255] *Significant Economic Presence and Its Legal Significance*, HINDU BUSINESS LINE (June 7, 2021), https://www.thehindubusinessline.com/business-laws/significant-economic-presence-and-its-legal-significance/article34683362.ece.

[256] 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.").

[257] *2020 CCIA NTE Comments*, *supra* note 36.

[258] 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.

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

As of October 2021, discussion on the PDPB continues and policymakers have considered changes that would have an even greater impact on industry. Amendments have been offered to include sharing of non-personal data.[259] There are also reported plans to introduce "psychological manipulation as a violation" of the law.[260]

Anonymized data is expected to be excluded, but with exceptions. Under the exception, the government can direct any data fiduciary or processor to share any anonymized data or other 'non-personal data'. The two use cases defined are (1) to enable better targeting of service delivery; or (2) to promote evidence-based policy making. There is little rationale offered, or sufficient details that explain when these two use cases are likely to occur. It is also not clear with whom such data must be shared and what the modalities of such transfer will be. This provision also poses liability concerns for companies as the re-identification of de-identified data is a criminal offense.

The continued delay, and lack of transparency into the process over the past three years has drawn criticism from the Indian startup community.[261]

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."[262] Any proposed framework for Non-Personal Data should be deferred at least until work is completed on the PDPB and appropriate standards, rules and regulations have been issued in order to avoid conflicting requirements.

---

[259] *Looking at 'Bigger Umbrella' Personal Data Protection Bill Likely to Include Non-Personal Data*, THE INDIAN EXPRESS (Oct. 5, 2021), https://indianexpress.com/article/business/looking-at-bigger-umbrella-pdp-bill-likely-to-include-non-personal-data-7552240/.

[260] *Need Data Protection Bodies at State Level for Robust Law*, HINDUSTAN TIMES (Oct. 25, 2021), https://www.hindustantimes.com/india-news/need-state-level-data-protection-authorities-joint-parliamentary-committee-mp-amar-patnaik-101632679181340.html.

[261] *Data Protection Bill Will Increase Compliance Costs for Small Companies: Hasgeeek*, HINDU BUSINESS ONLINE (Sep. 21, 2021), https://www.thehindubusinessline.com/info-tech/data-protection-bill-will-increase-compliance-cost-for-small-companies-hasgeeek/article36584709.ece.

[262] 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.

Online Content Regulations

India is a priority region of concern for U.S. digital service exporters, given the vibrant digital economy and market opportunities with increased government control over online speech. There is great concern with the speed at which Indian policymakers and political leaders have increased censorship practices and increased restrictions on companies that fail to take down content political leaders deem "objectionable". This has been combined with a dramatic increase in the aggression by which enforcement agencies go after U.S. firms in the market and novel enforcement tactics.[263]

There have been concerning occasions in the past where the Indian government has blocked websites or made requests to take down specific content. However, recent legislative changes relating to digital services will pose greater challenges to U.S. exporters in India's vibrant digital market.[264]

Earlier this year, amendments to the Information Technology Act went into effect imposing additional requirements under the Intermediary Rules and imposing new obligations on intermediaries.[265] These new requirements include strict timelines for content takedown demands (72- and 24-hour timelines), new local presence requirements, and traceability mandates which pose significant security risks. New rules were also announced separately for 'publishers' to adhere to a prescribed Code of Ethics. This includes incidental product changes to ensure rating and classification as per prescribed guidelines and implement access and parental control mechanisms and to implement a three-tiered grievance redressal mechanism.

While there was a public consultation on the proposed changes in 2018, there was limited opportunity for industry and other stakeholders to provide input as the draft amendments and new obligations developed or sufficient notification of these rules.[266] Companies have all made determinations on how they want to operate in response to the new rules, as well as the increased enforcement tactics by Indian officials. Under the new rules, the Indian government is already asserting that at least one U.S. firm should be stripped of liability protection for user content.[267]

---

[263] *Twitter Says It's Concerned with India Intimidation, Requests 3 More Months to Comply with New IT Rules*, TECH CRUNCH (May 27, 2021), https://techcrunch.com/2021/05/27/twitter-says-concerned-with-india-intimidation-requests-3-more-months-to-comply-with-new-it-rules/.

[264] *India: An Update on India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, GLOBAL ADVERTISING LAWYERS ALLIANCE (June 2, 2021), https://www.mondaq.com/india/social-media/1074774/an-update-on-india39s-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-202.1

[265] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The Indian Government Press Release is available: https://pib.gov.in/PressReleseDetailm.aspx?PRID=1700749, and the full text is available: https://egazette.nic.in/WriteReadData/2021/225464.pdf.

[266] CCIA had filed comments in the 2018 public consultation regarding proposed amendments to the Information Technology (Intermediary Guidelines) Rules 2011. https://www.ccianet.org/wp-content/uploads/2019/02/Comments-of-CCIA-to-MeitY-on-Draft-Intermediary-Guidelines-2018-1.pdf

[267] *Twitter Has Lost Liability Protection in India, Government Says*, TECH CRUNCH (July 6, 2021), https://techcrunch.com/2021/07/06/twitter-has-lost-liability-protection-in-india-government-says/.

The rules also have a potential chilling effect on human rights and future investment, and will lead to over-removal and censorship of legitimate content, including political speech.

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 competitors.[268] 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.[269]

The rules also impose obligations on all e-commerce entities without regard to unique e-commerce models and relationships between the entities, buyers and sellers. It is also unclear how the requirement for every e-commerce entity to register itself with the DPIIT relates to protection against unfair trade practices by e-commerce entities, and creates an arbitrary and artificial distinction between offline sellers and e-commerce entities as registration requirements do not apply to offline sellers. Such additional non-tariff barriers have a dampening impact on the market access of foreign players into the Indian e-commerce market.

Geospatial Data Guidelines

In February 2021, guidelines regarding geospatial data and associated services were introduced with the goals of deregulation and opening up India's mapping policy.[270] However, some aspects of the new guidelines are discriminatory towards foreign service providers. Specifically, Indian companies are given preferential access to geospatial data through prohibitions on foreign entities from creating and owning geospatial data within a certain threshold. While foreign entities can obtain a license for such maps or data through an Indian entity provided it is used only for the purpose of serving Indian users, subsequent reuse and resale of such maps and data

[268] 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.

[269] 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).

[270] Sub: Guidelines for acquiring and producing Geospatial Data and Geospatial Data Services including Maps (Feb. 2021), *available at* https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data.pdf.

is prohibited. There is also a data localization requirement for such data, which has to be stored and processed on a domestic cloud or on servers physically located in India.

Regulations on Cloud Services

In September 2020, the Telecom Regulatory Authority of India released recommendations on a Regulatory Framework for Cloud Service Providers (CSPs).[271] 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.

In 2020, the DPIIT extended its demand for minimum local content to the procurement of software and services. As per the Notification, the local requirement to categorize a supplier as a 'Class I' supplier is 50 percent and a Class 2 Supplier is 20 percent. The formula for calculation of Local Content has not been explicitly defined and has been left to the discretion of the different procurement agencies. This policy introduces market entry barriers that will impact specifically multi-national companies that have global R&D centers and therefore cannot assign the cost of development to one country; in addition investments made in the ecosystem (such as the build of data centers or investments in startups) have also been ignored.

Local Content Requirement

Aligned with the Government of India's continued rhetoric on self-reliance, the Public Procurement (Preference to Make in India), Order 2017 and subsequent revisions mandates that only Class-I suppliers (with local value addition >50 percent) and Class-II suppliers (local value addition – 20 percent to 50 percent) are eligible to bid for Government procurement. This is applicable to both products and services.

While this order and compliance to this order is applicable to all entities, Indian or foreign, it poses a significant challenge to software and cloud service providers (CSPs) to demonstrate local value add. This model does not consider the investments and other contributions made by CSPs that enable the technology ecosystem in India and their global competitiveness, such as skilling initiatives, cloud innovation centers, and quantum computing lab.

U. Indonesia

Digital Taxation

In March 2020, Indonesia introduced tax measures targeting digital services as part of an emergency economic response package. One of these taxes applies to e-commerce transactions

[271] 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/.

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.[272] Companies determined to have a significant economic presence will be declared permanent establishments and as a result subject to domestic tax regulations.[273] 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.[274] While structurally different from DSTs from European countries, the tax is similarly concerning insofar as it looks to increase U.S. firms' tax payments in the region by departing from longstanding international taxation norms. U.S. companies were cited as targets of these tax measures.[275] Governments should be discouraged from pursuing discriminatory taxes on foreign companies to fund economic response measures.[276]

As of time of filing, implementation details have not been announced, and Indonesia officials have stated that they would align politics with the OECD consensus reached in October 2021. Recent tax reform[277] in Indonesia did not include additional ETT language, but as the ETT can be revived with a subsequent implementing declaration, U.S. trade officials should continue to monitor developments.

Customs Duties on Electronic Transmissions

Indonesia issued Regulation No.17/PMK.010/2018 (Regulation 17) in 2018.[278] 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[279] and most recently reaffirmed in December 2019.[280] Left

[272] *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.

[273] *Id.*

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

[275] *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.

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

[277] *Indonesia Passes Major Tax Overhaul Bill, VAT to Rise Next Year*, REUTERS (Oct. 7, 2021), https://www.reuters.com/world/asia-pacific/indonesian-parliament-vote-major-tax-overhaul-2021-10-06/

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

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

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

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 in December 2021. Indonesia must rescind Regulation 17 and remove Chapter 99 from its HTS.

Regulations on Subsea Cable Corridors

The Minister of Fisheries and Marine Affairs issued a Decree 14/2021 mandating that all subsea cables in Indonesian waters need to follow 14 prescribed routes and to have 4 pre-determined main landing points in Manado, Kupang, Papua and Batam.[281] More than half of existing cables are located out of these prescribed corridors, and there is limited justification for companies to follow such routes and landing points. This restricts the ability of U.S. cloud and infrastructure services providers to determine the best business case for such landings and gives preferential treatment to domestic providers.

Further, as part of the new GR 5/2021 on business licensing, subsea cable permits require a series of licenses from several Ministries such as Environment, ICT, Transport, and Investment. The requirement from ICT Ministry specifically asks for (1) foreign operators to partner with a local network operator, (2) the local partner to be part of the consortium, (3) a minimum of 5 percent stake by the local partner, and (4) obligation to land in Indonesia. Such requirements are significant market barriers for U.S. providers to establish their business operations in Indonesia.

Content Regulation on Private Electronic System Providers

The ICT Ministry issued Ministerial Regulation 5/2020 on private electronic systems providers (ESPs) in December 2020.[282] The Regulation took effect immediately. Under the new framework, local and foreign ESPs are required to register with the government and appoint local representatives to respond to government demands for access to data and information. ESPs are expected to comply with demands for data access for "supervisory and law enforcement purposes" within 5 days. Further, ESPs must comply with strict timelines for content removal - 24 hours for "prohibited content removal requests and only 4 hours for "urgent" removal requests. Vague definitions under the new Regulation open companies up for large consequences, from fines and/or service restrictions. Civil society groups have also raised concerns with aspects of the Regulation.[283]

---

[281] *Indonesia Officially Regulates Submarine Cables and Pipeline*, TEMPO (Feb. 23, 2021), https://en.tempo.co/read/1435866/indonesia-officially-regulates-submarine-cables-and-pipeline

[282] See Hogan Lovells, *Indonesian regulator set clearer terms for internet platforms (domestic and foreign): Registration, takedown, and (un)blocking* (Jan. 26, 2021), https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2021-pdfs/2021_01_26_corporate_and_finance_alert_indonesian_regulator_set_clearer_terms_for_internet_platforms.pdf ; *Indonesia's New Regulation on Private Electronic System Operators: Important Notes for Corporate Compliance of Domestic and Foreign Information Technology Companies* (May 11, 2021), https://www.zicolaw.com/resources/alerts/indonesias-new-regulation-on-private-electronic-system-operators-important-notes-for-corporate-compliance-of-domestic-and-foreign-information-technology-companies/.

[283] Article 19, Coalition Letter, *available at* https://www.article19.org/resources/indonesia-repeal-ministerial-regulation-5/.

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 regulations,[284] storing and processing of data offshore by any "Electronic Systems Providers (ESPs)" will require prior approval from the government.[285] 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 ESP includes public administration, which goes beyond national 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.

There is also a Ministry of Communications and Informatics Circular Letter which requires all Ministries to obtain clearance from the Ministry for any IT procurement or expenditure to ensure maximum utilization of the National Government Data Center, a challenge for cloud adoption by public agencies and a barrier to U.S. cloud services providers from servicing the Indonesian public sector market.

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.[286] For example, data localization policies remain 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.

Personal Data Protection Bill

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

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

[285] *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.

[286] *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

countries. The bill would also impose extraterritoriality as its cross-jurisdictional basis, again similar to GDPR.

Restrictions on Cloud Services in Financial Sector

The Indonesian market is restrictive for adoption of public cloud technology in the services industry, according to industry reporting.[287]

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 regulators' lack of trust in multilateral law enforcement systems.

Further, the OJK requires financial institutions to seek its approval 2 to 3 months before moving workloads to the public cloud. For instance, Regulation No. 38/POJK.03/2016 requires commercial banks planning to operate an electronic system outside Indonesia to seek approval from the OJK 3 months before the arrangement starts. In addition, financial institutions that plan to outsource the operation of their data centers or disaster recovery centers must notify the OJK at least 2 months before the arrangement starts.

Lastly, Regulation No. 9/POJK.03/2016 only allows commercial banks to outsource "support work" (i.e., activities that are low risk, do not require high banking competency and skills qualification, and do not directly relate to operational decision-making). These workloads that can be outsourced are all subject to the same regulatory requirements, with no differentiation in terms of materiality, unlike in other jurisdictions, such as Australia and Singapore.

Additional E-Commerce Barriers

Indonesia's Government Regulation No. 80/2019 on E-Commerce distinguishes between domestic and foreign e-commerce business actors, and prohibits personal data from being sent offshore unless otherwise approved by the Ministry of Trade.[288] This effectively requires e-commerce business actors to locally store personal data for e-commerce customers. Trade 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.

[287] Better on the Cloud Financial Services in the Asia Pacific Report 2021, *available at* https://www.techrepublic.com/resource-library/whitepapers/better-on-the-cloud-financial-services-in-asia-pacific-2021-report/.

[288] *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.

V. Italy

Digital Taxation

Italy's 2020 Budget introduced a 3 percent digital services tax closely aligned with the EU's original proposal.[289] 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".[290]

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.[291] It appears that this remains the case with the current tax.

With the announcement of a global OECD solution, Italy officials have stated that they expect the national measure to be removed by 2024 under the agreed framework.[292] While the most appropriate action would be an immediate withdrawal of existing DSTs in exchange for terminating the Section 301 investigations, CCIA is supportive of the compromise reached by the United States, Austria, France, Italy, Spain, and the United Kingdom regarding existing measures.[293] CCIA encourages policymakers to continue work on swift implementation of the global framework and removal of the DST.

Implementation of the EU Platform to Business Regulation

Italy implemented the EU Regulation on Platform to Business (P2B) by appointing the Communications Authority (Agcom) as the national agency in charge of its application and enforcement. Agcom implemented the Regulation by imposing burdensome obligations on platforms that will be subject to the Regulation in Italy in a way that goes well beyond the scope of the P2B regulation and is something unique to Italy, as no other agencies across the EU are asking for similar obligations. Italy recently implemented the EU Regulation on Platform to Business ("P2B") by appointing Agcom as the national agency in charge of its application and enforcement.

---

[289] 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.

[290] *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).

[291] *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.

[292] *After G20 Endorses Tax Deal, Italy Says Its Digital Levy Could Stay for Two More Years*, REUTERS (Oct. 13, 2021), https://www.reuters.com/world/europe/italy-says-remove-unilateral-digital-tax-by-2024-2021-10-13/.

[293] *Unilateral Measures Compromise*, *supra* note 41.

Agcom passed two resolutions that implement the Regulation on: (i) forcing entities providing intermediation services to sign-up to a national registry – which involves the payment of a yearly contribution to support Agcom's activities related to P2B ("ROC resolution"); and (ii) requesting signed-up entities to provide extensive disclosure of internal financial and accounting data, which goes well beyond the scope of the P2B regulation. Agcom should also approve soon a resolution setting the amount of the yearly contribution, which will be capped to a maximum of 2 percent of the national turnover. As a result, the estimated annual contribution could amount to up to EUR 4MM based on its 2020 turnover figures for Italy. The contribution as well as such a heavy data disclosure is something unique to Italy, as no other agencies across the EU are asking for similar obligations.

Ex-ante Platform Regulation

In March 2021, the Italian Competition Authority (ICA) has come forward with proposals to the IT government to reform Italian competition law to tackle more effectively anticompetitive conducts by digital platforms. The IT government could include the ICA's proposals into a draft bill called Annual law on Competition that will be in place by the end of 2022.

First, the ICA proposed to introduce a presumption of economic dependence in the commercial relationships of third-party business users with digital platforms that offer an intermediation service, where these platforms play a determining role in reaching end users and suppliers, including as a result of network effects and data accumulation. As this is a rebuttable presumption, digital platforms will have the opportunity to demonstrate that this relationship of economic dependence does not exist.

Second, the ICA proposes to introduce new legislation, based on Germany's 10th amendment to its competition law, which would designate certain companies as "undertakings of primary importance for competition in more than one market". These companies would be prohibited from pursuing certain conduct, unless they can demonstrate that it is objectively justified. Prohibited conduct listed in the proposed amendment includes: (i) self-preferencing; (ii) strategically using data to erect barriers to entry; (iii) providing third party business users with insufficient information on their performance on the platform; and (iv) making the provision or quality of a service conditional upon data transfer. Failure to comply with these rules could lead the ICA to impose behavioral or structural remedies.

Implementation of the EU Audiovisual Services Directive

Italy is implementing EU Audiovisual Media Services Directive ("AVMS-D"). The implementing measure in question envisages a significant increase in the mandatory investment quotas in local productions endangering international and local investments. Italy is implementing EU AVMS-D (Directive 2018/1808) through a Legislative Decree (Dlgs) which delegates the Government to adopt the implementing measures. The Dlgs provides, among other things, the introduction of a mandatory investment quota in European works (a quota that includes Italian works) which would gradually (until 2025) grow up to 25 percent of the given company's net revenues of the previous year. Such a high investment quota would jeopardize Italy's attractiveness for the audio-visual sector and create an environment hostile to investments in general. If the measure is approved in the current text, in 2025 Italy would have the highest mandatory investment quota in the whole of the EU.

W. Japan

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

The Japanese Ministry of Communications (MIC) expanded the application of its telecommunications law to foreign services in 2021.[294] 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. Industry reports that the MIC is also considering changes to existing privacy guidelines under the TBA, focusing on cross-web, device tracking in digital ads. The Personal Information Protection Commission (PPC), the data protection authority in Japan, has amended the Act on the Protection of Personal Information (APPI) in May 2020, which will come into effect from April 2022.[295]

Market-Based Platform Regulation

Following various reports and consultation CCIA has cited in previous NTE submissions,[296] the Headquarters for Digital Market Competition released its final report in 2021 on "Competition in the Digital Advertising Market." The report concluded that the Platform to Business Act (P2B) should be applied to digital advertising and organic search. The applicability of P2B to organic search is also being considered by the Cabinet Legislation Bureau. There are concerns on whether a wholesale application of the P2B to organic search is feasible given the unique nature of the product and potential algorithmic change disclosers.

In May 2021, the Japanese Consumer Affairs Agency (CAA) enacted "Act on the Protection of the Interests of Consumers Using Transaction Digital Platforms".[297] Industry is monitoring discussion on the draft of the Cabinet Office ordinance. The law aims to impose certain obligations on platforms regarding resolution of disputes between merchants and consumers, and requires platforms to disclose information to consumers about merchants upon request.

Copyright Policy

In 2020, Japan revised its Copyright Act. Part of the new amendments expand the scope of what constitutes illegal downloading to include digitized print media, in part to address illegal downloads of manga. There are exceptions for "minor offenses" and "special instances" such as education, news purposes, small clips for social media networks (GIFs), unintentional capture, parody, and minor uses of frames from a manga or lines out of a book "where it is recognized

---

[294] Morrison & Foerster, *Japan's Efforts to Strengthen the Effectiveness of Enforcement Against Foreign Telecommunications Operators* (May 7, 2020), https://www.jdsupra.com/legalnews/japan-s-efforts-to-strengthen-the-8593184/.

[295] Personal Information Protection Comm'n Japan, Act on the Protection of Personal Information, https://www.ppc.go.jp/en/legal/ (last visited Oct. 25, 2021).

[296] *CCIA 2020 NTE Comments*, *supra* note 36.

[297] *New Regulation of Digital Platforms in Japan* (Apr. 1, 2021), https://www.omm.com/resources/alerts-and-publications/alerts/new-regulation-of-digital-platforms-in-japan/.

that [the use] does not unduly harm the interests of the copyright holder."[298] The changes took effect on January 1, 2021.

Deductive Value Definition for Inventory Transfer by Non-resident Importers at Importation

In Japan, when importers declare their import customs by deduction method, on which the declaration value is calculated by deducting domestic costs from its own domestic price, it is unclear whether marketing expenses paid by non-resident importers are deductible, unlike EU import custom procedure. The Uniform Customs Code in the EU states that, when using the deduction method on imports into the EU, direct and indirect costs of marketing must be deducted from the unit price when they are made about sales in the EU. The lack of clarity complicates declaration procedure and imposes unnecessary burdens on importers.

Nutritional Supplements

In Japan, nutritional supplements are regulated as a part of a loosely defined "health food" subcategory of foodstuffs, unlike in the United States, where nutritional supplements are regulated independently. However, a supplement which includes specified raw materials categorized as medicine like aloe leaf extract can no longer be sold as a "health food" and are required to go through a time-consuming approval process as pharmaceuticals for sale. This discriminates against many nutritional supplements approved in the US, which contain materials defined as medicine in Japan.

X. 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".[299] The policy proposes an increase to 30 percent of the local ownership rules, currently set at 20 percent. The requirement would take effect by 2023. 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.

In 2021, the new Office of the Data Commissioner issued draft regulations proposing that data processed for "actualising a public good" shall be processed in a server and data center based in Kenya. This would include, but not limited to, data related to civic registration and national

[298] *Japan Enacts New Copyright Laws to Curb Illegal Manga Downloading*, CRUNCHYROLL (June 11, 2020), https://www.crunchyroll.com/anime-news/2020/06/11/japan-enacts-new-copyright-laws-to-curb-illegal-manga-downloading; *Japan's New Anti-Piracy Law Goes Live*, TORRENT FREAK (Jan. 1, 2021), https://torrentfreak.com/japans-brand-new-anti-piracy-law-goes-live-heres-how-it-will-work-210101/.

[299] *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/.

identification systems; primary and secondary education; elections; health; electronic payments and public revenue administration.

Such data localization mandates are a barrier to cross-border digital trade, and the forced local equity ownership requirement limits market access opportunities for U.S. companies operating in Kenya.

Digital Taxation

Kenya implemented the following tax laws in 2020: (1) a 20 percent withholding tax on "marketing, sales promotion and advertising services" provided by non-resident persons; (2) a 1.5 percent digital service tax on income from services derived from or accruing in Kenya through a digital marketplace, and (3) a revision to the VAT liability of exported services from zero-rated to exempt, so that the services provided by the local entity to overseas entities would no longer be classified as services for export and the local entity would no longer claim VAT refunds on its costs for those services.

Y. Korea

Network Management Mandates for Value-Added Telecommunications Service Providers

The Ministry of Science & ICT is currently considering regulations made pursuant to amendments to the Telecommunications Business Act passed in 2020.[300] 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.

Network Fee Legislation

Several proposals have been made by the Korean National Assembly to mandate "network use fee" payments by certain content providers. This is motivated largely by the need to help fund the costs of extending and adding capacity to local broadband markets, but is posed to distort incentives and leads to discriminatory treatment of content providers.[301] This follows years of

[300] 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.

[301] Kyung Sin Park & Michael Nelson, *Afterword: Korea's Challenge to the Standard Internet Interconnection*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (Aug. 17, 2021),

conflict among U.S. content providers operating in the region and local telecommunication providers.[302]

Restrictions on Cloud Services

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).

Through these requirements that depart from international standards, the CSAP effectively serves as a technical barrier to trade and prohibits global cloud service providers from accessing the Korean public sector market. U.S. firms are unable to meet some components of the certification program without creating a separate Korea-unique product, including physically segregating facilities for exclusive use for government-owned customers. Such an approach undermines the economies of scale of cloud computing. Industry cites that the four main technical requirements that has prevented global cloud service providers 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.

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 unlevel playing field for companies who are unable to obtain the CSAP.

While CSAP is currently an administrative guideline, Korea's National Assembly is currently considering an amendment to the 2015 Cloud Computing Promotion Act, which would institutionalize the CSAP as a statutory requirement.

Amendments to the Telecommunication Business Act on Mobile Application Marketplaces

In August 2021, the Korean National Assembly passed legislation that requires mobile application marketplaces to permit users to make in-application purchases through payment platforms not controlled by the marketplace itself. The scope of the law effectively creates a band on a predominately used U.S. model, at the exclusion of local equivalents. Further, policymakers supportive of the bill have made clear their intent to single out specific U.S. companies with the new law.[303] The targeting of U.S. firms could conflict with Korea's trade

https://carnegieendowment.org/2021/08/17/afterword-korea-s-challenge-to-standard-internet-interconnection-model-pub-85166.

[302] *Korean Court Sides Against Netflix, Opening Door for Streaming Bandwidth Fees from ISPs*, TECHCRUNCH (June 28, 2021), https://techcrunch.com/2021/06/28/korean-court-sides-against-netflix-opening-door-for-streaming-bandwidth-fees-from-isps/.

[303] Reason for Proposal and Main Contents, New regulations on prohibited acts of app market operators, etc. (Agenda No. 2102524), *available at* https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_B2C0H0N7Z3O0I1Y5X3Q0Z3Y1D1U2L3.

commitments under the Korea-U.S. Free Trade Agreement, as well as commitments under Article XVII (National Treatment) of the WTO General Agreement on Trade in Services (GATS).

U.S. operators of application marketplaces are disincentivized to operate in a region where it is unclear how the application distributor could recover the costs it incurs in maintaining the mobile application marketplace.

Further, the lack of sufficient deliberation and input from parties, both domestic and foreign, on the merits and possible implications of the bill including potential harmful effects on a nascent and thriving ecosystem that countless Korean developers utilize to reach a global market.

Location-based data restrictions

Korea's restrictions on the export of location-based data have led to a competitive disadvantage for international suppliers seeking to incorporate such data into services offered from outside of Korea. For example, foreign-based suppliers of interactive services incorporating location-based functions, such as traffic updates and navigation directions, cannot fully compete against their Korean rivals because locally-based competitors typically are not dependent on foreign data processing centers and do not need to export location-based data. Korea is the only significant market in the world that maintains such restrictions on the export of location-based data.

While there is no general legal prohibition on exporting location-based data, exporting such data requires a license. To date, Korea has never approved a license to export cartographic or other location-based data, despite numerous applications by foreign suppliers. U.S. stakeholders have reported that Korean officials, citing security concerns, are linking such approval to a separate issue: a requirement to blur certain integrated satellite imagery of Korea, which is readily viewable on other global mapping sites based outside of Korea. Korean officials have expressed an interest in limiting the global availability of high-resolution commercial satellite imagery of Korea, but have no ready means of enforcing such a policy since most imagery is produced and distributed from outside of Korea. It is unclear how limiting such availability through specific services (e.g., online mapping) of a particular supplier addresses the general concern, since high-resolution imagery, including for Korea, is widely available as a stand-alone commercial product (and is often available free of charge), and offered by over a dozen different suppliers.

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.[304] While in the pursuit of

[304] 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"],

enforcing existing laws regarding illegal content, some have raised concern that it follows authoritarian models of Internet regulation.[305]

Z. Malaysia

Cabotage Policy on Submarine Cable Repairs

In November 2020, the new Minister of Transport abruptly revoked an exemption from 2019 to the Merchant Shipping Ordinance 1952 that permits non-Malaysian ships to conduct submarine cable repairs in Malaysian waters.[306] The exemption was key in reducing the time required to conduct submarine cable repairs. Submarine cables are the global backbone of the internet, carrying around 99 percent of the world's Internet, voice and data traffic, including the backhaul of mobile network traffic and data for digital trade.[307] The revocation was reportedly a means to protect the domestic shipping industry from foreign competition.

Restrictions on Cloud Services

In October 2021, the Malaysian Communications and Multimedia Commission (MCMC) announced that data centers and cloud service providers would be subject to licensing obligations under the Communications and Multimedia Act 1998 (CMA 1998) starting January 2022.[308] Traditionally, and pursuant to global best practices, these licensing requirements are tailored to telecommunications and services providers, rather than a broader class of technology services.

Under the new obligations, cloud service providers may be required to: (1) incorporate locally in Malaysia; (2) appoint local shareholders, including a fixed percentage of shareholders from the Bumiputera ethnic group; (3) comply with the provisions of the Communications and Multimedia Act 1998, including requirements on content removal; (4) allow interception of communications subject to the discretion of the Communications and Multimedia Minister; and (5) make mandatory payments to the Universal Service Fund.

---

[305] *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/.

[306] *Tech Giants Seek Meeting with New Malaysian PM on Foreign Ship Cable Waiver,* REUTERS (Sep. 4, 2021), https://www.reuters.com/technology/tech-giants-seek-meeting-with-new-malaysian-pm-foreign-ship-cable-waiver-2021-09-04/.

[307] *Inside the Cables Carrying 99% of Transoceanic Data Traffic*, https://99percentinvisible.org/article/underwater-cloud-inside-cables-carrying-99-international-data-traffic/ (last visited Oct. 25, 2021).

[308] MALAYSIAN COMM. & MULTIMEDIA COMM'N, Cloud Service Regulation Introduced to Increase Accountability for User Data Security and Sustainability of Services (Oct. 16, 2021), https://www.mcmc.gov.my/en/media/announcements/cloud-service-regulation.

AA. 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,[309] 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 to force compliance. The measure was approved by Congress in November 2020, and entered force on January 1, 2021.[310] The regulation empowers tax authority to work with the telecom regulator to non-resident Internet platforms, removing them from accessibility to Mexican users. At time of filing, the provision hasn't been used as the vast majority of U.S. Internet companies have already been registered and have been complying with fiscal obligations.

Nevertheless, the implementation of this blocking could fragment the Mexican Internet and lead to technical problems that will likely impact third parties. Likewise, the provision likely violates USMCA Articles 15.3 of National Treatment for Services and Service Suppliers; Article 15.6: Local Presence; Article 18.3: Access to and Use of Public Telecommunications Networks or Services; Article 19.10(a): Principles on Access to and Use of the Internet for Digital Trade; and most importantly Articles 17.17 and 19.11 regarding Free flow of data across borders.

Copyright Liability Regimes for Online Intermediaries

Mexico reformed 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.

Likewise, the provision implemented through the amendment of in Article 232 Quinquies fr. II of the Copyright Law establishes administrative offenses and a fine, when ISPs: do not remove, take down, eliminate or disable access to content upon obtaining a notice from the right holder; or do not provide to a judicial or administrative authority information that identifies the alleged

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

[310] Income Tax Law http://www.diputados.gob.mx/LeyesBiblio/pdf/LISR_310721.pdf, VAT Law http://www.diputados.gob.mx/LeyesBiblio/pdf/77_310721.pdf, Tax Code http://www.diputados.gob.mx/LeyesBiblio/pdf/8_310721.pdf.

offender. This provision contravenes Article 20.89 (9) of the USMCA, and other provisions of the Bill, since the impossibility of applying the measures provided in the treaty do not *per se* originate a responsibility for ISPs.

Currently, the Supreme Court is analyzing an unconstitutionality action presented by the National Human Rights Commission against these amendments, arguing that in some respects it breaches USMCA and freedom of expression.

Restrictions on Cloud Services

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 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 also conflict with the localization principles established in USMCA digital and financial commitments.

In September 2021, the "ICT Cloud Policy" was published and includes concerning provisions regarding data localization.[311] Industry reports concerns that the requirements could result in Federal Government cloud procurement to favor providers with data centers located in Mexico.

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

[311] *Available at* https://www.dof.gob.mx/nota_detalle.php?codigo=5628885&fecha=06/09/2021. See also https://www.itmastersmag.com/noticias-analisis/la-administracion-publica-federal-pone-orden-en-sus-tic/.

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.

A second bill also proposed by Senator Ricardo Monreal establishes amendments to the Cinematography Law that similarly set a 10 percent to 15 percent national content quota requirement for OTT services.

Additional E-Commerce Barriers

The U.S.-Mexico-Canada Agreement (USMCA) entered into force on July 1 and included positive outcomes for US Companies in the Customs Chapter, including streamlined, simplified, and expedited border processing to help speed border clearance times and lower costs for low-value shipments. This included commitments by Mexico to implement new *de minimis* and informal clearance thresholds.

On May 27, 2021, Mexico's Tax Administration Service (SAT) published revised General Foreign Trade Rules that raised the informal clearance threshold to $2,500. The increase to $2,500 went into effect on June 26 for shipments valued at >$117. However, the Secretary of Economy still needs to harmonize its own regulations to allow for this change to be fully implemented which has not happened to date. Specifically, the SE needs to update Section IX, Article 10 of the Annex 2.4.1, which still requires compliance with all applicable NOMs for those courier shipments with a value of $1,000 or more, which in line with the recent changes to the SAT rules and the USMCA, should be updated to $2,500.

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). For non-USMCA shipments, the import rate was also increased by 3 percent (from 16 percent to 19 percent) for shipments between US$50-1000. 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 Customs Chapter, including eliminating the new import rates and implementing an informal clearance threshold for shipments up to USD $2,500.

Proposed Regulation Applicable to E-payment Institutions (IFPEs)

Mexican financial sector regulators - National Banking and Securities Commission (CNBV) and the Central Bank of Mexico (Banco de Mexico) - have issued Draft Provisions Applicable to Electronic Payment Fund Institutions (IFPEs). The particular articles of concern in the draft regulation are Articles 50 and 49.[312] Article 50 would impose the obligation of data residency

[312] Provisions Applicable to Electronic Payments Institutions, Referred to in Articles 48, Second Paragraph; 54, First Paragraph; and 56, First and Second Paragraphs of the Law to Regulate Financial Technology Institutions.

and multi-scheme provider to E-Payment Institutions (IFPEs) that use 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 draft requirements to localize data run counter to the spirit, if not the letter, of USMCA's landmark digital and financial services provisions. These draft regulations undermine U.S. financial services providers, which already face lengthy and uncertain approval processes from CNBV or Banco de Mexico in order to use secure U.S.-based cloud computing services. Additionally, the regulation could negatively affect the adoption of cloud computing in the country and create an uneven playing field, where U.S. cloud computing companies would be at a disadvantage with respect to local data center companies.

Most 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 shall 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 be participate in Mexico's national payments system (SPEI), regulated and operated by the Central Bank. Overall, there is information that Mexico's 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. In addition to Article 50, the provisions proposed in Article 49 establish an authorization model with a high degree of discretion and an absence of clear approval processes.

BB. 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.[313] 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.

The controlling Labour Party included in its policy platform "to proactively work with the OECD to find a workable solution to the issue of multinational corporations not paying their fair

[313] 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/.

share of tax."[314] CCIA urges New Zealand to abandon plans for a national DST in light of the October agreement.

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.[315] There are concerns that the draft legislation includes an overly broad definition of "objectionable content". The bill also contemplates government-imposed content blocking mechanisms.

The Bill is currently before Parliament. The Bill, which is framed in response to the Christchurch attacks of 2019, proposes 2 main changes: 1) the establishment of a notice and take down scheme for 'objectionable' online content backed by civil penalties; and 2) a new criminal offence for the act of livestreaming objectionable content. A parliamentary committee has just reported on the Bill, recommending (among other things) to make the Bill's claim of extraterritorial application more explicit, such that international services accessible by New Zealand citizens will be obligated to remove content that fits in the notably broad and subjective category of 'objectionable', 'regardless of whether an online content host is resident or incorporated in New Zealand or outside New Zealand'. This approach would create a significant burden on internationally accessible services.

Data Sovereignty

The NZ Government has pursued 'Cloud First' policies[316] that are promising in regards to enabling digital trade, and has recently joined a Digital Partnership Agreement with Chile and Singapore with supportive provisions that affirm DEPA "partners' levels of commitments relating to transmission of information and location of computer facilities" and "recognise the value of information flows and the development of new technologies and services."[317] Industry is monitoring some calls for restrictions which may have implications for the free flow of data across borders.[318]

[314] Our Manifesto To Keep New Zealand Moving, 2020, p10 Labour_Manifesto_2020.pdf

[315] 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).

[316] Digital Government New Zealand. Cloud Services, https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/ (last visited Oct. 26, 2021).

[317] New Zealand Foreign Affairs & Trade, DEPA Modules, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-modules/#bookmark2 (last visited Oct. 26, 2021).

[318] Co-designing Maori Data Governance, https://data.govt.nz/toolkit/data-governance/maori/ (last visited Oct. 26, 2021).

CC. Nigeria

Government-Imposed Content Restrictions and Related Access Barriers

Nigeria announced an "indefinite ban" on Twitter in the country following the company's decision to remove posts from political leaders that violated its abusive behavior policy. Cases like this illustrate the challenges online businesses face with respect to proactively removing content that violates their terms of service, crafted to ensure harmful content is quickly removed. As reported, most telecommunications providers quickly complied, even though the policy was not passed through legislation and could be subject to court litigation on the basis of free speech.[319]

A Bill for Protection from Internet Falsehoods and Manipulation was introduced in the Senate in December 2019. Beyond hate speech, the proposed law broadly criminalizes statements that may prejudice the country's security, public health, public safety, or friendly relations with other countries; or that may diminish confidence in the government. Online content service providers would also be subject to orders to disable access to the offending content or to issue 'correction notices' to all end users that may have had access to the content. If passed the law would significantly limit freedom of speech and could also be used to suppress content from political opposition.[320]

Data Protection Bill

Nigeria's 2013 Guidelines for Content Development in Information and Communication Technology establish local hosting requirements for government (sovereign), consumer and subscriber data, unless express approval has been obtained from the technology regulator (NITDA) for a crossborder transfer.[321] This is in addition to 2011 Guidelines from the telecoms regulator requiring local hosting of subscriber data and from the Central Bank Guidelines requiring domestic routing of card transactions; the Central Bank Guidelines do not envisage the possibility of cross-border transfers.

More recently, a Data Protection Bill, which looks to create a Data Protection Commission, seeks to regulate the collection, storage and use of personal data of data subjects in Nigeria.[322] It requires that personal data be processed lawfully based on a legal basis. The Bill applies to entities in the private and public sector as well as data controllers and processors operating within and outside the country. It extends its applicability to personal and biometric data of data subjects; personal banking and accounting records; academic transcripts; medical and health records; telephone calls; messages, among other things. The application of the Bill exempts from its scope the processing of personal data by a data subject while carrying out purely personal or household activities.

---

[319] *Nigeria's Twitter Ban is Another Sign Dictatorship is Back*, FOREIGN POLICY (June 7, 2021), https://foreignpolicy.com/2021/06/07/nigeria-twitter-ban-dictatorship/.

[320] *Nigerians Should Say No to Social Media Bill*, HUMAN RIGHTS WATCH (Nov. 26, 2019), https://www.hrw.org/news/2019/11/26/nigerians-should-say-no-social-media-bill.

[321] Available at: https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf.

[322] Available at: https://www.ncc.gov.ng/documents/911-data-protection-bill-draft-2020/file.

While this current draft version has moved well beyond data localization as well as requiring adequacy for international transfers, there remain concerns over provisions that give life to its extraterritorial application which is often difficult to manage/litigate and gives rise to ambiguities in the operations of data controllers/processors. Another concern is on the identification of a DPO - appointments should focus on the DPO as an "office" and not as a specific "individual."

Digital Taxation

The 2020 Finance Act introduces income tax obligations for non-resident companies providing digital goods and services in Nigeria.[323] While the law applies to all non-resident companies earning above a certain threshold, extensive media coverage and analysis by experts has repeatedly mentioned the targeting of U.S. multinationals. The law specifically references non-resident companies with a 'significant economic presence' in the country which is defined by a number of factors including: a minimum amount of revenue generated from users in Nigeria, transmitting data about Nigerian users, or the availability of local websites or local payment options. Exceptions have been built into the law for companies that are covered by a multilateral agreement to which the Nigerian government is a party.

DD. Pakistan

Government-Imposed Censorship and Content Restrictions

In February 2020, the Ministry of Information Technology and Telecommunication (MoITT) released the Citizens Protection (Against Online Harm) Rules.[324] After civil society and industry groups expressed widespread concerns, the government announced in March 2020 that a committee led by the Pakistan Telecommunication Authority (PTA) would conduct an "extensive and broad based consultation process with all relevant segments of civil society and technology companies."[325] However, the Cabinet approved and published on Oct. 20, 2020 substantially similar rules. After another round of consultation, MoITT published a third version of the Rules on June 18, 2021.[326]

The current version, titled "Removal and Blocking of Unlawful Content (Procedure, Oversight and Safeguards) Rules" retains the problematic provisions of the previous drafts. These include: mandatory local office presence and registration by the entity providing the service; obligations

---

[323] KPMG, *Nigeria: Tax Provisions in Finance Act, 2019*, https://home.kpmg/us/en/home/insights/2020/01/tnf-nigeria-tax-provisions-in-finance-act-2020.html.

[324] *See Newly Published Citizens Protection (Against Online Harm) Rules are a Disaster for Freedom of Expression in Pakistan*, YLS INFORMATION SOCIETY PROJECT (Feb. 29, 2020), https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blog/newly-published-citizens-protection-against-online-harm-rules-are-disaster-freedom-expression.

[325] ARTICLE 19, *Pakistan: Online Harms Rules Violate Freedom of Expression* (Aug. 13, 2021), https://www.article19.org/resources/pakistan-online-harms-rules/.

[326] Available at: https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Rules%20-%20RULES%20FOR%20REMOVAL%20AND%20BLOCKING%20OF%20UNLAWFUL%20ONLINE%20CONTENT%20(PROCEDURE%2c%20OVERSIGHT%2c%20AND%20SAFEGUARDS)%20RULES%2c%202020.pdf .

to appoint a local "compliance officer" to liaise with the PTA on content removal requests, obligations to appoint a local "grievance officer" and post their contact details online (the grievance officer would be required to redress complaints from the public within 7 days of receipt); impose strict timeline for content removal (48 hours or 12 in case of an emergency); require for companies to "comply with the user data privacy and data localization provisions" of a forthcoming Data Protection Law, and require firms to provide user data to investigative authorities in accordance with existing federal law.

Restrictions on Cross-Border Data Flows and Localization Mandates

In May 2020, the Ministry of Information Technology and Telecommunication (MoITT) released a draft Data Protection Bill that contained provisions on data localization (including an undefined "critical personal data" category), a powerful regulator in a newly established data protection authority, extraterritorial application, and criminal liability.

After multiple rounds of public consultation, MoITT released a new version of the bill in August 2021.[327] While some of the provisions around criminal liability and data localization are slightly improved, significant concerns remain regarding impediments to the cross-border flow of "sensitive" and "critical" data. Furthermore, these terms – "sensitive" and "critical" – are ill-defined, with "unregulated e-commerce transactions" falling within the definition of critical data.

Pakistan is also in the process of finalizing a "Cloud First Policy." This policy also imposes data localization requirements on wide and open-ended classes of "sensitive" and "secret" data. In the financial sector, the State Bank of Pakistan (SBP) prohibits financial sector institutions from storing and processing core workloads on offshore cloud.

EE. Panama

Restrictions on Cross-Border Data Flows and Data Localization

The Government Innovation Authority (AIG) of Panama published (09/10) resolution No. 52 ordering all cloud services, mission-critical, or state-security databases, or sensitive institutional data of all Government Entities must be held in Panamanian territory by December 31, 2022.

FF. 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.

[327] Revised draft available here: https://moitt.gov.pk/SiteImage/Misc/files/25821%20DPA%20Bill%20Consultation%20Draft_docx.pdf.

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.[328] The proposal appears to give preferential 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 abilities 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.

Local Content Requirements

On July 11, 2021, the Secretary of the Peruvian Congress published the report of a bill that proposes to modify the Audiovisual and Cinematographic Activity Promotion Law—attached. The document unifies two bills, the first (6257) creates screen quotas, while the second (7465) proposes the creation of a Film Commission and the promotion of audiovisual productions. The published text is now prepared to be discussed by the plenary of Congress, which is expected to happen in the coming weeks at time of filing.

Among the bill's provisions, there are local content requirements and the creation of a new incentive regime. Specifically, Article 20 states that the Ministry of Culture may set "annual rules on minimum percentages of exhibition and commercialization of Peruvian cinematographic works in any medium or system. This percentage must not exceed 20 percent of the total commercial and cultural works exhibited in the country during the same period of time."

If these policies are enacted, Peruvian audiences and creators would have fewer legitimate options for film and television content. In addition, these polices are likely to violate Peru's free trade agreement obligations.

[328] *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. 26, 2021).

GG. Philippines

Additional Restrictions for E-Commerce

The Philippines Department of Trade and Industry (DTI) is issuing a Joint Administrative Order (JAO) that regulates the e-commerce industry.[329] Industry expects it be passed by November 2021, and implemented as soon as it takes into effect 15 days after publication. The JAO reiterates enforcement of various laws aimed at consumer protection, and purports to also impose new obligations and liabilities on platforms which are not supported by existing laws. New obligations include proactive monitoring of content, TDR requirements, and direct and solidary liability. There is strong support under Philippine jurisprudence to render administrative regulations beyond the scope of existing laws invalid. Industry has expressed concern over the draft JAO.

HH. Poland

Government-Imposed Content Restrictions and Related Access Barriers

In January 2021, the Ministry of Justice announced the Draft Act on the Protection of Freedom of Expression in Online Social Networks.[330] The law aims to prevent companies from removing content posted by its users if it is not illegal under Polish law. The law would also establish a "Freedom of Speech Council" to oversee complaints issued by users who has content removed by a social media platform. There are concerns that through the implementation of the proposed legislation, freedom of speech would be threatened by expanding government control over online speech.

Draft Act on Book Market Protection

Poland is considering draft legislation on "book market protection" which would introduce an obligation for the publisher and importers to set a fixed price for books, ebooks and audiobooks.[331] The fixed price would be valid for a period of 6 full calendar months. If adopted, this requirement would significantly limit the free pricing of these products and can be problematic for websites that provides access to ebooks and audiobooks for a specific monthly subscription.

---

[329] *See* DEP. OF TRADE AND INDUSTRY, Calls for Inputs on the Draft Joint Administrative Order on Guidelines for Online Businesses Reiterating the Law and Regulations Application to Online Business and Consumers, https://www.dti.gov.ph/advisories/jao-online-business/ [Philippines].

[330] Ministry of Justice, Protection of the Freedom of Speech of Users of Social Networking Sites (Jan. 1, 2021), https://www.gov.pl/web/sprawiedliwosc/ochrona-wolnosci-slowa-uzytkownikow-serwisow-spolecznosciowych.

[331] Available at http://www.pik.org.pl/komunikaty/876/ustawa-o-ochronie-rynku-ksiazki-d-uojck-i-uzasadnienia-do-ustawy-konsultacje-dla-branzy-wydawniczo-ksiegarskiej-do-18-maja-2021-r. *See also Polish Book Industry Eyes Fixed Book Price Proposal*, PUBLISHING PERSPECTIVE (May 17, 2021), https://publishingperspectives.com/2021/05/polish-book-industry-players-eye-fixed-book-price-proposal-covid19/.

Digital Taxation

As part of its broad tax reform initiative, the Polish Government has proposed the introduction of a minimum corporate tax levy.[332] The tax is of a supplementary nature, and applies to entities subject to CIT and Tax Capital Groups, whose share of income in revenues (other than from capital gains) will be less than 1 percent, or which will incur a loss for a given tax year.

There is also a proposal for introduction of a media advertisement tax, which would be applied to all broadcasts, publishers, and large tech companies.[333]

II. Russia

Government-Imposed Content Restrictions and Related Access Barriers

Russia continues to serve as a model of government-imposed control of Internet services and speech online. As detailed below, in recent years Russia has passed many new laws that grant Russian authorities greater control over online communications and services, as well as impose several obligations on services to comply with government demands. The most recent laws include Federal law N482-FZ and Federal law N511-FZ, which came into effect in 2021.[334]

Under Federal law N482-FZ, certain platforms can be fined or blocked (through explicit blocking or throttling of Internet traffic) for censoring "socially significant information". A platform will be liable for censorship by the Russian government if it restricts access to such information, such as termination of Russian accounts as well as other content restrictions including for trade compliance purposes. The definition of censorship is extremely broad, potentially covering every single restriction applied to content such as termination of Russian accounts as well as other content restrictions including for trade compliance purposes. The law, which was introduced as a response to removals of Russian media content by international platforms channels and other content restrictions[335], targets foreign companies, U.S. digital services providers, and severely constrains their ability to operate and offer their services in the Russian market.

Federal law N511-FZ imposes fines for services that do not remove banned information, which has included political protest content. As per previously adopted legislation, digital platforms targeted by the law are all U.S. digital services companies, which are required to forward the government's content removal requests to their users. If the reported content is not promptly

---

[332] *Poland Proposes Minimum Corporate Levy to Curb Tax Avoidance*, BLOOMBERG TAX (Sep. 8, 2021, https://news.bloombergtax.com/daily-tax-report-international/poland-proposing-minimum-corporate-levy-to-curb-tax-avoidance.

[333] KPMG, *Poland: Proposed Levy or Advertising Contribution Would Apply for Traditional and Online Advertising* (Feb. 4, 2021), https://home.kpmg/us/en/home/insights/2021/02/tnf-poland-proposed-levy-advertising-contributions-traditional-online-advertising.html.

[334] *The Putin Regime Will Never Tire of Imposing Internet Control: Development in Digital Legislation in Russia*, COUNCIL ON FOREIGN RELATIONS (Feb. 22, 2021), https://www.cfr.org/blog/putinregime-will-never-tire-imposing-internet-control-developments-digital-legislation-russia.

[335] *New Law Would Expand Internet Censorship in Russia*, HUMAN RIGHTS WATCH (Nov. 23, 2020), https://www.hrw.org/news/2020/11/23/new-law-would-expand-internet-censorship-russia.

taken down by the user, the onus is on the platform to block access to such content. Non-compliance could mean the blocking of the platform altogether by the Internet Service Provider (ISP). The new law introduced fines for violations that are astronomically high - reaching 10 to 20 percent of revenue by the infringer for repeat violations.

In recent months, U.S. firms have experienced an increase in demands by the *Roskomnadzor*, which regulates Internet services, to take down content, including through requests pursuant to these new rules.[336] These have included threats to prosecute their local employees, which make it extremely challenging for US digital companies to operate and compete on a reasonable basis in Russia. Firms that Russian authorities determine have not sufficiently complied with demands have experienced an uptick in throttling and restriction in services.[337]

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.[338] 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[339] and the Federal Law on Amending the Code of Administrative Violations,[340] establish penalties for "knowingly spreading fake news" and establish a framework for ISPs to block access to websites deemed to be spreading "fake news."

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.[341] The law took effect in early 2021.[342] The scope of devices includes smartphones, computers, tablets, and smart TVs, and the scope of applications includes the default pre-installation of the local search engine, navigation tools, anti-virus software, software that provides access to e-government infrastructure, instant messaging and social network software, and national payment software. This has impacted U.S. companies' ability to compete on a level playing field in the Russian

---

[336] *Russia Raises Heat on Twitter, Google and Facebook in Online Crackdown*, N.Y. TIMES (May 26, 2021), https://www.nytimes.com/2021/05/26/technology/russia-twitter-google-facebook-censorship.html.

[337] *How Russia is Stepping Up Its Campaign to Control the Internet*, TIME (Apr. 1, 2021), https://time.com/5951834/russia-control-internet/; *New Russia Bill Would Expand Internet Censorship, HRW Warns*, RADIO FREE EUROPE (Nov. 24, 2020), https://www.rferl.org/a/hrw-warns-new-russian-bill-would-expandinternet-censorship/30966049.html.

[338] *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-disconnectthecountry-from-the-world-wide-web/

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

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

[341] *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-smartphoneslaptops.

[342] *Russian Law Requires Smart Devices to Come Pre-Installed with Domestic Software*, REUTERS (April 1, 2020), https://www.reuters.com/article/us-russia-technology-software/russian-law-requires-smart-devices-to-come-pre-installed-with-domestic-software-idUSKBN2BO4P2.

market, with broader implications for continued market access, consumer choice as well as industry development.

As noted above, Russia is also a country that imposes restrictions on the use of tools to circumvent censorship methods and access restricted content or services. Pursuant to a 2018 law, search engines are fined for providing access to "proxy services" including VPNs.[343]

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

Russia Law N236-FZ was signed into force in July 2021, and provides that companies owning any website/app which is accessed daily by more than 500K users from Russia have to "land" by establishing a local unit that will represent its interests in Russia and will be liable for its activities.[344] The law applies to foreign companies which own websites/apps accessed daily by more than 500,000 users from Russia and meet at least one of the following conditions: (i) it is in Russian or a Russian local language; (ii) it has ads targeted at Russian users; (iii) the website/app owner processes Russian user data; (iv) websites/apps receive money from Russian individuals and legal entities. Amongst other requirements, foreign companies will also be required to install Russian Government-provided software which will be counting the users of the website or app.

Some provisions of the Law are already in effect but await secondary legislation to become fully operational. The core part of the Law which requires a direct local presence takes effect on January 1, 2022. Failure to comply may result in significant penalties, including possible bans for Russian companies and/or users to advertise with such foreign platforms and/or transfer money and make payments, and potential full or partial blocking or throttling of the incompliant website or application. Such local presence requirements, coupled with onerous compliance requirements and harsh penalties, severely constrain the ability of U.S. companies to operate in Russia.

JJ. 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.[345] The rules contain a provision on data localization that may restrict access to the Saudi market for foreign

[343] HUMAN RIGHTS WATCH, *Russia: Growing Internet Isolation, Control, Censorship* (June 18, 2020), https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship. The Human Rights Watch identified all the following laws from 2017-2020 that "collectively empower the Russian government to exercise extensive control over the internet infrastructure and online activity in Russia" which include: 2016 "Yarovaya amendments" on forced data retention; 2017 law prohibiting VPNs and internet anonymizers from providing access to banned websites and follow-up 2018 amendments to the Code of Administrative Offenses; 2017 law on identification of messaging application users and a follow-up 2018 government decree; 2019 "Sovereign internet" law; and 2019 law on pre-installed Russian applications.

[344] *New Requirements for Localisation of Major Internet Companies in Russia*, DEBEVOISE & PLIMPTON (Aug. 23, 2021), https://www.debevoise.com/insights/publications/2021/08/new-requirements-for-localisation-of-major.

[345] *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.

Internet services.[346] 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.[347] 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.[348] 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).[349]

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

[346] *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.").

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

[348] *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.

[349] 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.

electronic devices require additional permits from the Saudi telecom regulator. Industry also reports extensive documentation requirements that depart from global practice in developed countries.[350]

KK. Singapore

Government-Imposed Content Restrictions and Related Access Barriers

The Protection from Online Falsehoods and Manipulation Bill became effective starting on October 2, 2019.[351] The law empowers any Minister to issue direction on online services to remove content or carry 'corrections' on their platforms in response to claims from the government that content is false or misleading.[352] 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.[353] Stakeholders have raised concerns with enforcement of these laws since it went into effect.[354]

Foreign Interference (Countermeasures) Act

The Foreign Interference (Countermeasures) Act (FICA) was passed on October 4, 2021.[355] It is expected to come into force in Q1 of 2022. Similar to the earlier content legislation, the Protection from Online Falsehoods and Manipulation Bill (POFMA), FICA empowers the Minister for Home Affairs (MHA) to issue directions to online services to remove content or carry "corrections" on their platforms in response to claims from the government or from individuals that content is being covertly influenced by a foreign actor. The Minister is also empowered to request information from online services which according to MHA is "required for the authorities to determine if harmful communications activity is being undertaken by or on behalf of a foreign principal". Given the broad powers granted to FICA under the bill, it will be important that its power is only used judiciously to weed out coordinated influence campaigns

[350] 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.

[351] 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.

[352] *See 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/.

[353] *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.

[354] *Singapore: 'Fake News' Law Curtails Speec*h, HUMAN RIGHTS WATCH (Jan. 13, 2021), https://www.hrw.org/news/2021/01/13/singapore-fake-news-law-curtails-speech.

[355] Ministry of Home Affairs, Countering Foreign Interference, https://www.mha.gov.sg/what-we-do/managing-security-threats/countering-foreign-interference [Singapore].

rather than a tool of targeting critical political speech.[356] Industry is closely monitoring how the law will influence similar measures in the region, due to concerns with the use of broad-ranging powers to moderate content on internet platforms and its impact on free speech.

LL. Spain

Digital Taxation

On October 7, 2020, the Senate approved legislation to impose a digital tax of 3 percent of revenue online advertising services, online intermediary services, and data transfer services.[357] 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.[358]
While the most appropriate action would be an immediate withdrawal of existing DSTs in exchange for terminating the Section 301 investigations, CCIA is supportive of the compromise reached by the United States, Austria, France, Italy, Spain, and the United Kingdom regarding existing measures.[359] CCIA encourages policymakers to continue work on swift implementation of the global framework and removal of the DST.

Royal Decree – Law 7/2021 - Sales of Goods and Supply of Digital Content Directives

Spain rushed through transposition of the EU Sales of Goods and Supply of Digital Content Directives under an emergency procedure involving no consultation, impact assessment, or other stakeholder involvement.[360] It was directly approved by the Council of Ministers, without being previously announced, despite the implementing act diverging significantly from the text of the

---

[356] *See Singapore Passes 'Most Powerful' Foreign Interference Law Amid Fears of Ever-Shrinking Space for Dissent*, WA. POST (Oct. 5, 2021), https://www.washingtonpost.com/world/2021/10/05/singapore-fica-foreign-interference-law/.

[357] Available at: https://boe.es/boe/dias/2020/10/16/pdfs/BOE-A-2020-12355.pdf.

[358] 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).]).

[359] *Unilateral Measures Compromise*, *supra* note 41.

[360] See HOGAN LOVELLS, *Directive for the Supply of Digital Content and Digital Services to Consumers: Spain Update* (May 12, 2021), https://www.jdsupra.com/legalnews/directive-for-the-supply-of-digital-9657688/.

directives. Apart from this approach being incompatible with the general principles of transparency and stakeholder involvement to which member states signed up to under the better regulation initiative, the divergence from the EU texts risks creating barriers to trade, fragmenting the Single Market, and undermining legal certainty.

Industry reports that the government justified the use of such an omnibus RD-L as they were late in meeting the implementation deadlines of the directives. However, they went beyond what was required in the Directive text.[361] In most cases, the government observed the usual obligation to conduct a public consultation and publish an impact assessment. This obligation was not observed. Implementing such divergent rules without a proper impact assessment will create major legal uncertainty for especially smaller cross-border players and more generally create a market barrier for traders and manufacturers, requiring them to operate differently in Spain in comparison to other markets.

While Directive (EU) 2019/771 should not impose an obligation on sellers to ensure the availability of spare parts throughout a period of time as an objective requirement for conformity, the national law sets that Producers must ensure the existence of (i) an adequate technical service, as well as (ii) spare parts for a minimum period of 10 years from the date on which the good ceases to be manufactured.

RTVE (national public service media organism) levy

The Spanish government is aiming at using the transposition of the AVMSD as an instrument to mandate video on demand services and video-sharing platforms to finance the public broadcaster RTVE by paying a levy equal to 1.5 percent of their Net Annual Revenue. The obligation to finance RTVE was first introduced following the government's decision to prohibit publicity on RTVE, resulting in a need to obtain funds from other sources. This levy is currently paid by the following players with varying rates: (1) Local free TV: 3 percent of net revenue, (2) Pay TV: 1.5 percent of net revenue and Telecoms: 0.9 percent of net revenue. Telecommunications companies will be exempt from this obligation with the new law.

MM. 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.[362]

[361] *See* Digital industry concerns with the Spanish transposition of the Sales of Goods Directive, https://www.digitaleurope.org/resources/digital-industrys-concerns-with-the-spanish-transposition-of-the-sales-of-goods-directive-2019-771/.

[362] *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.

NN. Taiwan

Digital Communications Act

Taiwan's National Communications Commission (NCC) is contemplating a content regulation titled the Digital Communications Act (DCA), which is likely to closely model after EU's DSA.[363] The DCA contains measures to allow government authority to censor online content, control misinformation and impose mandatory third-party consultations on content removal and community guidelines. While the NCC has not shared the draft at time of filing, industry worries that over-extensive content regulations and data-related requirements may reinforce censorship and add friction to cross-border digital trade.

Targeted Application of Competition Regulations

Taiwan's Fair Trade Commission (TFTC) is in preparatory status for investigations to be launched against only U.S. digital platform companies, but provides little to no insight into what issues are under investigation or research. The questionnaires for market research often carry unsubstantiated claims, misleading narratives, suggestive questions, and biased selection of examples. These procedural deficiencies are compounded by the fact that TFTC decisions are not stayed on appeal.

Ancillary Copyright

Industry reports that the Taiwan government is under pressure from news media publishers to impose a mandatory news media bargaining code to regulate commercial relations between news publishers and digital platforms.[364] While the Taiwan government has not released a draft, industry worries that the Code may be in tension with longstanding international trade principles of national treatment and most favored nation (MFN), by unfairly discriminating against foreign digital service suppliers and providing preferential treatment to local advertising and other digital service suppliers.[365]

Restrictions on Cloud Services

In 2019, the Financial Supervisory Commission (FSC) issued amendments to the Regulation Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, requiring financial institutions to obtain FSC's permission prior to using cloud computing services. However, the approval process imposes additional compliance costs and security risks for both the financial institutions and cloud service providers. The process requires submitting up to 17 documents, duplicated audit requests and a lengthy review process, which may discourage financial institutions from using cloud computing services, and thereby limiting market access for U.S. cloud services providers.

---

[363] *NCC Pushes Draft Communications Act*, TAIPEI TIMES (Oct. 1, 2021), https://www.taipeitimes.com/News/taiwan/archives/2021/10/01/2003765334.

[364] *News Media Bargaining Code Considerer*, TAIPEI TIMES (Sep. 3, 2021), https://taipeitimes.com/News/taiwan/archives/2021/09/03/2003763729.

[365] *See* page 17 of this submission.

Cloud Outsourcing for Financial Services

In Q4 2019, FSC issued an amendment to the Regulation Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, and the Directions for Operation Outsourcing by Insurance Enterprises, the first management guidance on the use of cloud computing services by financial and insurance institutions. The amendments include several requirements that would make it difficult for financial institutions to use cloud computing services. These include extensive documentary requirements, ambiguous approval criteria, an unclear approval timeline, and excessive duplicated audit requirements which increase compliance costs for financial institutions and Cloud Service Providers. In addition, there's currently no similar regulations addressing cloud outsourcing needs. Instead, institutions are requested to discuss with FSC on case-by-case basis regarding the Securities and Futures sector, e-Payment service providers, and fintech start-ups. The lack of sufficient guidelines ads to entry barriers for cloud adoption.

Data Localization

Industry reports a that through regulators' stated preferences for data localization, there is a de facto data localization requirement for cloud services.

While Taiwan's sectoral regulations, such as financial services, health records and public sector, allow institutions to outsource workloads to overseas cloud, there are wordings explicitly expressing regulator's preference of data localization, such as "in principle, where customer data is outsourced to a cloud service provider, the location for processing and storage shall be within the territories of the R.O.C.," and, in the case of overseas outsourcing, "except with the approval of the competent authority, backups of customer important data shall be retained in the R.O.C."

When an institution contemplates the outsource location, it's clear that the regulator prefers domestic destination; if the institution decides to get approved for overseas outsourcing, it has to bear the over-burdensome documentary requirements which may cause unnecessary compliance cost; even though FI is willing to bear the burden, the review process is very likely to be lengthy and unpredictable; and, the institution still need to maintain a local copy of "important" data.

Restrictions on Over-the-top (OTT) Services

Taiwan's National Communications Commission is considering a draft bill (Internet Audiovisual Service Management Act) that would impose registration requirements on over-the-top (OTT) services. The bill would introduce new requirements for certain internet services, including disclosure of subscriber numbers, appointment of a local representative, and membership of a self-regulatory body.[366] The new rules would present barriers to foreign-based OTT services, including by requiring the disclosure of commercially sensitive data.

[366] *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.

OO. 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.[367] The government has also issued emergency decrees in relation to the global pandemic that further restrict online and press freedom.[368]

In 2019, Thailand passed a controversial Cybersecurity Law following amendments in 2018. Industry has criticized the law due to provisions that enable government surveillance.[369] Under the new law, officials are granted authority to "search and seize data and equipment in cases that are deemed issues of national emergency."[370] This could "enable internet traffic monitoring and access to private data, including communications, without a court order."[371]

Government-Imposed Content Restrictions and Related Access Barriers

The Thailand Electronic Transactions Development Agency (ETDA) introduced the Draft Royal Decree on the Supervision of Digital Platform Services in August 2021. The draft decree is overly broad beyond the authority of ETDA and does not recognize different platforms' business models. It also imposes burdensome obligations and liabilities on businesses, such as local representative with unlimited liability, reporting requirement, and prescriptive ad mandatory requirement for platforms to display how to list, display, rating, collect information, terms, dispute, appeal, and broad authority for ETDA to further prescribe any additional requirement in the future. The Royal Decree sets out a requirement for each operator to have a Code of Conduct which includes merchant ID verification, but it lacks details. The government specifically mentioned this in the meeting, public forum and iterated by the Minister. Therefore, there is a very high possibility that this requirement will be further prescribed. The decree is expected to go to cabinet for approval by the end of October 2021 and go to the council of state for review afterwards.

---

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

[368] *Id.*

[369] *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.").

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

[371] *Id.*

PP. 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.[372] CCIA has previously identified laws that preemptively block websites on vague grounds, and specific instances of blocking by Turkish authorities.[373]

In recent years, the market conditions have worsened.[374] 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" [375]) in July 2020 that grants the government sweeping new powers to regulate content on social media.[376] The law went into effect October 1, 2020, and authorities were quick to take action against U.S. firms, imposing fines,[377] advertising bans, and bandwidth restrictions within months.[378] The law requires social network providers with more than one million daily users to: establish a representative office in Turkey, respond to individual complaints in 48 hours or comply with official takedown requests of the courts in 24 hours, report on statistics and categorical information regarding the requests every six months, and take necessary measures to ensure the data of Turkish resident users is kept in country. Social network providers face serious monetary fines and significant bandwidth reduction to their platform in cases of noncompliance.

Further to the 2020 Amendment to the Internet Law 5651, the Turkish government is expected to introduce a social media disinformation bill in Q4 of 2021. While a draft law has not yet been

---

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

[373] 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.

[374] *See* FREEDOM HOUSE, Freedom on the Net 2021, Turkey, https://freedomhouse.org/country/turkey/freedom-net/2021 ("Internet freedom continued to decline for a third year in a row in Turkey. During the coverage period, hundreds of websites were blocked, in some instances under a new social media law.").

[375] Available at https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm

[376] *Turkey Passes Law Extending Sweeping Powers Over Social Media*, N.Y. TIMES (July 29, 2020), https://www.nytimes.com/2020/07/29/world/europe/turkey-social-media-control.html.

[377] *Turkey Fines Social Media Giants for Breaching Online Law*, AP NEWS (Nov. 4, 2020), https://apnews.com/article/business-turkey-media-social-media-560de2b21d54857c4c6545c1bd20fc25.

[378] *Turkey Slaps Ad Ban in Twitter Under New Social Media Law*, REUTERS (Jan. 19, 2021), https://www.reuters.com/article/us-turkey-twitter/turkey-slaps-ad-ban-on-twitter-under-new-social-media-lawidUSKBN29O0CT.

released, the new bill will likely require a Turkish citizen to be appointed as a representative (rather than a legal entity per the 2020 amendment) and introduce fines and penalties for organized spread of disinformation.

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.[379] 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".[380] 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.[381]

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.[382] 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-ups) information systems within the country.[383] The Regulation establishes a framework for use of cloud services as an outsourced service, but only applies for services located in Turkey.[384]

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

---

[379] 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.

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

[381] *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.

[382] *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.

[383] *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.

[384] *Id.*

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.[385] 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.

QQ. 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 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.

The newly presented bill on Copyright and Related Rights №5552-4 (registered June 9, 2021) in its Article 58 keeps the norm on 24- and 48-hour "shot clocks" for online intermediaries to act on demands to remove content for them to avoid liability.

RR. United Arab Emirates (UAE)

Licensing Requirements for Social Media Influencers

The National Media Council Content Creators law applies to UAE residents and influencers operating in the UAE, including all social influencers who use their social media channels to promote and/or sell products.[386] The law requires "social media influencers" to obtain a license at the cost of 15,00 dirhams that is valid for one year, and covers a broad scope, including "any paid or unpaid form of presentation and/or promotion of ideas, goods or services by electronic means, or network applications".[387] Such onerous licensing requirements covering a broad scope of social influencing activities poses unnecessary trade barriers and inhibit new social

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

[386] General Framework of the UAE Media Strategy, https://u.ae/en/media/media-in-the-uae/media-regulation (updated on Oct. 25, 2021).

[387] *Want to Be An Instagram Influence in Dubai? That'll Cost You £3,000*, WIRED (May 24, 2018), https://www.wired.co.uk/article/instagram-influencer-dubai-fee-advertising-social-media.

influencers, particularly those based outside of the UAE from promoting their services to the UAE market. Though industry reports that the law has not been widely enforced, there is a risk that the rules could be enforced on a selective basis to target certain influencers.

SS. United Kingdom

As the U.S. looks to negotiate with the UK following its exit from the EU, it should consider several regulations and policies that deter U.S. digital exports.[388]

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.[389] The White Paper is incredibly wide-ranging, and includes several 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.[390]

[388] *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.

[389] 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.

[390] 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; Online Harms White Paper: Full Government Response to the Consultation (Dec. 2020), *available at* https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response.

In December 2020, the UK government released its response to the Online Harms consultation.[391] Based on the Report, it suggests that the regulation is designed to specifically target U.S players, twisting the notion of "proportionality" into protectionism. Further, as presented in the White Paper, the upcoming legislation will establish different categories of content and activity on platform services, then attribute different duties to each. There have been reports that officials will finalize the legislation by the end of 2021.[392]

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. While the proposal document itself purports to have a non-discriminatory intent, statements from policymakers suggest otherwise.[393]

While the most appropriate action would be an immediate withdrawal of existing DSTs in exchange for terminating the Section 301 investigations, CCIA is supportive of the compromise reached by the United States, Austria, France, Italy, Spain, and the United Kingdom regarding existing measures.[394] CCIA encourages policymakers to continue work on swift implementation of the global framework and removal of the DST.

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

---

[392] *UK To Speed Up Legislation to Tackle Harmful Digital Content*, POLITICO (Oct. 20, 2021), https://pro.politico.eu/news/141696.

[393] 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.").

[394] *Unilateral Measures Compromise*, *supra* note 41.

data.[395] The UK also recently joined the United States and Australia in a concerning request to Facebook regarding undermining the security of user communications.[396]

Restrictions on Cross-Border Data Flows

The EU's General Data Protection Regulation (GDPR) went into effect in 2019, 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.[397] It is critical that there remain clear rules for U.S. exporters offering services in the UK and that there remains a valid mechanism for companies to legally transfer the data of UK citizens.

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 non-discrimination 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 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.

TT. 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. The localization rules as contemplated indicate that the Government is creating barriers for foreign services to favour local telecommunications and cloud service providers.[398]

---

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

[396] 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/.

[397] *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.

[398] 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.

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. Drafts include requirements for all companies to comply with data requests, content takedown, and domain name seizures.[399] 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.

The Vietnamese government is currently finalizing a Decree on Personal Data Protection, with the intent for it to become effective in December 2021.[400] The current draft prescribes conditions that a personal data processor must fully satisfy regarding the treatment of personal data of Vietnamese citizens, including 'registration' of transfer of such data of Vietnamese citizens overseas, impacting cross-border data flows. A related draft Decree on Administrative Penalties for cybersecurity contains high penalties for violations of the PDP - up to 5 percent of total revenue.[401] There are also so-called "additional penalties" in the form of withdrawing licenses, information or video takedown, confiscation of evidence, equipment, public apologies and correction.

Government-Imposed Content Restrictions and Related Access Barriers

The Law on Cybersecurity also includes 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.[402]

Besides regulatory roadblocks, U.S. companies face challenges from technical intervention such as throttling or limiting server access. These technical interventions are part of the government's effort to influence and control content, and undermine U.S. company competitiveness in the marketplace. At the end of 2020, Vietnamese authorities threatened to shut down Facebook in

---

[399] *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.

[400] KPMG, *Legal Alert – Draft Decree on Data Protection in Vietnam* (June 2021), https://assets.kpmg/content/dam/kpmg/vn/pdf/Legal-Update/2021/Legal-Update-21-Draft-Decree-on-Personal-data-protection-EN.pdf.

[401] *Ministry of Public Security Completes Draft Decree on Cybersecurity Fines*, VIETNAM NEWS (Sep. 27, 2021), https://vietnamnews.vn/economy/1048670/the-ministry-of-public-security-completes-draft-decree-on-cybersecurity-fines.html.

[402] *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 country if the U.S. firm did not censor certain political content on its platform at the request of the government.[403]

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 because of these changes include licensing requirements, local content quotas, local presence mandates, and translation requirements.

In July 2021, the Vietnamese government proposed amendments to the Ministry of Information and Communication Decree 72/2013. Multiple new rules were proposed relating to localization and content removal.[404] Under the amendments, all foreign enterprises providing cross-border services with over 100,000 Vietnamese unique visitor access per month must store data locally, set up a branch or representative office in Vietnam, and enter into a content cooperation agreement with Vietnamese press agencies when providing information cited from the Vietnamese press. Requirements for content removal are also onerous and sweeping, especially considering the broad definitions of what "prohibited acts" could entail. For example, any act that the Vietnamese government considers to be "adversely affecting social ethics, social order and safety and the health of the community" would be in scope. In addition, digital platforms, including cross-border providers, are required to take down violating content within 24-hours.

Additional Restrictions on E-Commerce

On September 25, 2021, the government issued Decree 85 on E-commerce, broadening its scope to include cross-border platforms without a local presence in Vietnam (including websites in Vietnamese language or exceeding 100,000 transactions per year).[405] The Decree also requires local and cross-border e-commerce platforms to provide vendors' information to authorities upon request and take-down information on goods that violate Vietnamese laws within 24 hours. The Decree will take effect January 1, 2022.

On July 21, 2021, the Government approved the *Draft Decree Amending & Supplementing Several Articles of Decree No. 181/2013/ND-CP dated 14 November 2013* implementing the Law on Advertising.[406] The rules regulate advertising content, and expanded the scope of these rules to applications and social media. The law took effect on September 15, 2021.

---

[403] *Vietnam Threatens to Shut Down Facebook Over Censorship Requests*, REUTERS (Nov. 19, 2020), https://www.reuters.com/article/vietnam-facebook-shutdown/exclusive-vietnam-threatens-to-shut-down-facebookover-censorship-requests-source-idUSKBN28007K.

[404] *See Vietnam Proposes Draft Decree Tightening Control Over Social Networks*, VIETNAM BRIEFING (Aug. 10, 2021), https://www.vietnam-briefing.com/news/vietnam-proposes-draft-decree-tightening-control-over-social-networks.html/.

[405] Decree 85/2021/ND-COP amending and supplementing Decree 53/2013/ND-CP on e-commerce, https://english.luatvietnam.vn/decree-no-85-2021-nd-cp-dated-september-25-2021-of-the-government-amending-and-supplementing-a-number-of-articles-of-the-governments-decree-no-53-210029-Doc1.html [Vietnam].

[406] BAKER MCKENZIE, *Vietnam: Cross-border Ad Decree* (July 22, 2021), https://viewpoints.bakermckenzie.com/post/102h3j2/vietnam-cross-border-advertising-decree-what-is-new

Restrictions on Cloud Services

On June 3, 2020, Vietnam's Prime Minister signed Decision 749/QD-TTg, announcing the country's National Digital Transformation Strategy by 2025.[407] 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.[408] 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.[409] 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.[410] The Ministry of Finance issued Circular 80[411] providing guidance on Law on Tax Administration and its Decree 126 in September 2021. The Circular added a requirement for foreign digital service/e-commerce suppliers without a permanent establishment in Vietnam, to directly register and pay tax to the tax authorities. If the foreign service providers do not register, service buyers (or commercial banks in case of individual buyers) will withhold tax from their payment to foreign suppliers at deemed tax rates. The legislation prescribes the above digital suppliers to file dossiers for applying Double Tax Treaty at the same time as filing quarterly tax returns, but it is unclear how the suppliers, of whom the sales revenue is withheld by their buyers or commercial banks in the country would claim the tax treaty's benefits. This onerous procedure coupled with the deemed tax rates (Corporate Income Tax and Value Added Tax) will further complicate tax obligations for cross-border service providers and conflict with international taxation rules.

---

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

[408] *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.

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

[410] *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/.

[411] Available at: https://thuvienphapluat.vn/tintuc/vn/thoi-su-phap-luat/chinh-sach-moi/37945/thong-tu-80-2021-tt-btc-huong-dan-luat-quan-ly-thue-nd-126-2020.

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.