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

In re Request for Comments on Significant Foreign Trade Barriers for the 2023 National Trade Estimate Report	Docket No. USTR–2022–0013

COMMENTS OF THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION REGARDING FOREIGN TRADE BARRIERS TO U.S. EXPORTS FOR 2023 REPORTING

October 28, 2022

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 87 Fed. Reg. 56,741 (Sept. 15, 2022), 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 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 annually, 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 of development, enabling small and medium-sized businesses to reach new markets and serve customers around the world. During the COVID-19 pandemic, digital technologies have empowered millions of U.S. businesses to increase their resiliency and continue serving and communicating with customers around the world. Several studies of small businesses have reported that the increased adoption of digital services served as a critical factor for these small businesses surviving during the pandemic.[2]

As economies globally continue to navigate a new phase of uncertainty and economic headwinds, digital tools are a critical resource for businesses to become more productive and to adapt to inflationary pressures. Digital services and goods also represent a key driver of U.S. export power, with the technology industry now delivering a hefty digital trade surplus of $262 billion for the United States. They will continue to play an important role in the economic recovery.

However, U.S. strategic trade and technology interests face growing threats from countries that continue to adopt discriminatory or unbalanced regulations that extract value and hinder the growth and cross-border delivery of Internet services. Under the guise of promoting domestic champions or addressing public concerns, countries are adopting discriminatory policies that disadvantage, and often target, U.S. technology companies and their users. These measures include digital services taxes, mandated payments to local industry incumbents, expropriation of IP and data, targeted restrictions on innovation not applicable to rivals, data localization requirements, censorship and surveillance demands as well as measures targeting local workers, and restrictions on U.S. investment and ownership.

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

[2] SHRM, Small Businesses Get Creative to Survive Pandemic (Sept. 2020), https://www.shrm.org/hrtoday/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.

Unfortunately, some foreign governments are increasingly overt in their efforts to discriminate against U.S. enterprises with a stated goal of supporting domestic rivals. Using the "techlash" or opposition to a handful of U.S. technology companies, foreign policymakers have leveraged a narrative that has given rise to a complex array of restrictions on U.S. innovation, one-way wealth and knowledge transfer obligations, market access restrictions, and selective enforcement against U.S. digital services in foreign markets or otherwise extracting revenue for local industry players.

Further, these measures coincide with a rise in efforts by authoritarian governments to control Internet services, restrict speech, compel the carriage of propaganda and disinformation, and undermine the 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 these barriers are becoming increasingly common in emerging digital markets as well as some traditional large trading partners that are accomplished through using different tools and methods. Because the business community has a limited technical capacity to assess and respond to interference with the 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, non-discriminatory regulation and governance of technologies, and open digital trade principles. The U.S. government has made commendable strides in this effort by launching and advancing initiatives such as the U.S.-EU Trade and Technology Council, the Indo-Pacific Economic Framework, the U.S.-Taiwan Initiative on 21st Century Trade, the U.S.-Kenya Strategic Trade and Investment Partnership, and the Declaration for the Future of the Internet over the past year. CCIA urges USTR and the U.S. government writ large to strengthen the capacity of these plurilateral platforms to prevent emerging trade barriers and advance tangible commitments from countries to adhere to democratic digital norms such as due process, non-discrimination, safeguards for privacy and security, and support for the free and open Internet that has enabled vast societal advances and billions of dollars in trade benefits.

As the Internet has grown more essential to international commerce, communications, competitiveness, and security, it has become equally essential that such barriers are identified and quelled. For the 2023 National Trade Estimate report, CCIA has identified significant barriers to trade facing U.S. Internet and digital exporters in the following areas: (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) taxation of digital services, (4) discriminatory platform regulation, (5) copyright liability regimes for online intermediaries, (6) forced revenue transfers in digital news, (7) telecommunications-related barriers, (8) restrictions on cloud services, and (9) backdoor access to secure technologies. In the comments below, CCIA highlights countries whose current and proposed regimes pose a serious threat to digital trade and U.S. strategic interests regarding innovation, technology, investment, and economic strength.

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. Addressing foreign barriers to Internet-enabled international commerce and communications has taken on new urgency considering the increased usage of Internet-enabled products and services by all sectors of the American economy as well as a wide range of consumers. Internet-enabled commerce represents a significant sector of the global economy.

From 2012 to 2020, the digital economy in the U.S. grew at an annual rate of 4.8 percent between 2012 and 2020.[3] According to U.S. Department of Commerce estimates, the digital economy generated $2.14 trillion of value added to U.S. GDP, or 10.2% of total U.S. GDP. The digital economy accounts for 7.8 million jobs, which generated almost $1.09 trillion in total compensation. Considering that large technology companies earned 58% of their revenue through their exports abroad, digital trade is driving broad benefits to U.S. companies and domestic workers, resources, and economic value in turn.[4] The United States generates $683.86 billion globally in ICT and Potentially ICT-Enabled Services, with a trade surplus of $300.6 billion.[5] Digitally-deliverable services are an essential part of U.S. export strength, as they represented 77% of *all* U.S. services exports in 2021.[6] Foreign markets bring vast benefits to U.S. firms and represent a significant source of revenue for CCIA's members—at least half of CCIA's U.S.-based members' revenue, a total of roughly $676.5 billion, came from abroad in 2021.[7] One firm estimated that the larger technology companies earn 58% of their revenue abroad.[8]

This was made more apparent during the global pandemic, which continues to restrict many traditionally powerful industries. Internet services around the world have enabled communications across borders, facilitated the continued communication between loved ones, and empowered business activity to continue remotely.[9]

---

[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] *Tech Stock Faces New Blow As Strong Dollar Threatens Earnings*, W.S.J. (Oct. 4, 2022), (https://www.wsj.com/articles/tech-stocks-face-new-blow-as-strong-dollar-threatens-earnings-11664837715.

[5] BUREAU OF ECONOMIC ANALYSIS, U.S. Trade in ICT and Potentially-ICT Services, https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=6&isuri=1&tablelist=359&product=4.

[6] UN Conference on Trade and Development, Data, https://unctadstat.unctad.org/wds/ReportFolders/reportFolders.aspx?sCS_referer=&sCS_ChosenLang=en

[7] Analysis of 10-K filings for FY 2021 for Meta, Google, Amazon, Intel, Apple, Twitter, eBay, Uber, Shopify, Cloudflare, Vimeo, and Pinterest. Some companies categorized these as net sales, some as net revenue. Some companies do not break out revenue or sales earned in the U.S. and Canada, so the percentage could be slightly higher.

[8] *Tech Stock Faces New Blow*, *supra* note 4.

[9] *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.

International markets continue to present the most significant growth opportunities for major U.S. companies, even as international competition has grown. However, challenges for U.S. businesses to reach these markets have also grown, and these changing dynamics are not only driven by competitive market forces. Countries recognize the immense value that a strong digital industry contributes to the national economy, and with the predominance of U.S. companies in this sector, governments are increasingly adopting policies designed to favor domestic innovation and specifically target U.S. companies, ushering in a new form of discrimination.

Trading partners' pursuit of "technological sovereignty," often with heavily protectionist features, continues to be a concerning trend. Regulatory frameworks and policy agendas imposed as part of this pursuit threaten to systematically extract value from U.S. firms while undermining U.S. leadership in the digital economy and the global nature of the free and open Internet.

In its 2022 *Freedom on the Net* report, Freedom House highlighted how "[r]ising digital repression in many countries mirrored broader crackdowns on human rights over the past year" with online censorship at "an all-time high" due to a "record number of governments blocking political, social, or religious content, often targeting information sources based outside of their borders." This has resulted in a situation where, as Freedom House highlights, over "three-quarters of the world's internet users now live in countries where authorities punish people for exercising their right to free expression online."[10] The fragmentation of the Internet—even when the physical connectivity is left intact—is well underway, as *Freedom on the Net 2022* reported that 47 of the 70 countries that they surveyed have restricted individuals' access to information sources outside of their jurisdictions.[11] It is no longer regimes such as China and Russia that are pursuing an isolationist and protectionist digital environment, as Freedom House in 2021 warned of the potential "negative repercussions that [the European Union's] laws could have on internet freedom in more closed environments" in reference to the Digital Services Act and Digital Markets Act.[12] The current trajectory of nations seeking increasing amounts of control over digital services and the online ecosystem risks unprecedented fragmentation of the open Internet and delivery of digital services.

While National Trade Estimate reports from prior years have acknowledged concerns regarding the European Union's regulatory agenda for digital services, a series of persisting and developing bilateral concerns continue to surface as the EU aggressively seeks progress on its goal of digital sovereignty. Ongoing efforts advancing in the EU include policies related to cloud certification requirements, the Data Act, and mandatory network usage fees. Meanwhile, the EU has proactively promoted its regulatory efforts to mutual trading partners, especially those in the APAC region.

---

[10] FREEDOM HOUSE, *Freedom on the Net 2022*, https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet.

[11] *Id*.

[12] FREEDOM HOUSE, *Freedom on the Net 2021*, https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.

The United States should pursue a robust 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 has already set a strong 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. As the United States pursues agreements such as the Indo-Pacific Economic Framework, the U.S.-Taiwan Initiative on 21st-Century Trade, and the U.S.-Kenya Strategic Trade and Investment Partnership, the digital trade barriers identified in these comments—both in these markets and those that may influence them—should be addressed through the enforcement of existing rules and robust new commitments where necessary. CCIA also encourages the United States to pursue a gold standard agreement at the WTO in the context of ongoing e-commerce discussions, which present 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 2022 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. Globally, the transfer of digitally-deliverable services—which is reliant on cross-border data flows—generated $3.81 trillion in 2021.[13] As CCIA has noted in previous NTE filings, countries continue to pursue data localization policies including mandated local presence, infrastructure, and data storage. In a 2017 report, the U.S. International Trade Commission (USITC) included estimates that localization measures have doubled in the previous six years.[14] Since that time, industry continues to see countries pursue policy and regulatory frameworks that restrict the free flow of information across borders, leading to losses in output and productivity along with an increase in prices for industries reliant on these data transfers.[15]

[13] United National Conference on Trade & Development Data, *available at* https://unctadstat.unctad.org/wds/ReportFolders/reportFolders.aspx?sCS_referer=&sCS_ChosenLang=en (last visited Oct. 28, 2022).

[14] 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.

[15] 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-

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.[16] 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.[17]

Rather than promote domestic industry, data localization policies are likely to hinder economic development and restrict domestic economic activity,[18] and impede global competitiveness.[19]

---

cost ("In 2017, 35 countries had implemented 67 such barriers. Now, 62 countries have imposed 144 restrictions—and dozens more are under consideration.").

[16] 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.

[17] 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.

[18] *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).

[19] 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),

Data localization policies also frequently violate international obligations, including GATS commitments, which require, where a country has made specific commitments, that a cross-border supplier not be put at a disadvantage vis-à-vis a local supplier. To remain compliant with international trade rules, measures that restrict trade in services must be for a bona fide national security purpose or necessary to achieve specific legitimate 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.[20] 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 consistently implement in a non-arbitrary manner.[21]

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.[22] More recently, industry has tracked advances in the EU towards an EU-wide cloud that would localize data within EU borders and preclude U.S. suppliers from participation.[23]

Continued opposition from the U.S. and likeminded allies is needed at the multilateral stage in light of these growing trends.[24]

---

http://online.wsj.com/articles/SB10001424052702304868404579194290325348688. *See also* U.N. CONFERENCE ON TRADE AND DEVELOPMENT, DATA PROTECTION REGULATIONS AND INTERNATIONAL DATA FLOWS at 3 (2016), http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ("[I]f data protection regulations go 'too far' they may have a negative impact on trade, innovation and competition."); Nigel Cory, *Cross-Border Data Flows: What Are the Barriers, and What Do They Cost?*, INFORMATION TECHNOLOGY & INFORMATION FOUNDATION (May 2017), https://itif.org/publications/2017/05/01/crossborder-data-flows-where-are-barriers-and-what-do-they-cost at 6-7 ("At the firm level, barriers to data flows make firms less competitive, as a company will be forced to spend more than necessary on IT services. Companies will likely have to pay more for data-storage services, especially those in 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.").

[20] 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).

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

[22] 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.

[23] Under Annex I NIS2 Directive, "essential entities" include among others airlines, banks, railway companies, energy companies, Securities Exchanges, pharmaceutical companies, healthcare providers, digital infrastructure providers including those providing online communications tools, ICT managed services, and public administration entities.

[24] 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.

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.[25] In a survey of the past year, Freedom House reported that government officials in at least 22 countries blocked social media or communications services to the public and that an estimated 51% of individuals with access to the Internet lived in a jurisdiction where the ability to use social media services were temporarily or permanently blocked.[26]

In just the past year, Russia has all but isolated itself from the global Internet and executed sweeping actions to stop the dissemination of any news and opinion critical of the government and its invasion of Ukraine;[27] Turkey has pursued expanded limitations on the use and operation of social media services;[28] and India has intensified its campaign to push social media services such as Twitter to remove political content.[29] Starting June 2021, 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, a block which ended in January 2022 and was later ruled unlawful by the Economic Community of West African States Court.[30]

---

[25] *See, e.g.*, Google Transparency Report, Traffic and Disruptions to Google, https://transparencyreport.google.com/traffic/overview; Government Requests to Remove Content, https://transparencyreport.google.com/government-removals/overview (last visited October 20, 2022); Twitter Transparency Removal Requests Report, https://transparency.twitter.com/en/reports/removal-requests.html#2021-jul-dec (published July 28, 2022); https://transparency.fb.com/data/internet-disruptions/; *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. (Showing that Facebook notes that its services were interrupted 38 times in 12 countries in the second half of 2021, compared to 62 disruptions in 17 countries that took place during the first half of the year).

[26] *Freedom on the Net 2022*, *supra* note 10.

[27] *See, e.g.*, *War Accelerates Russia's Internet Isolation*, BLOOMBERG (Mar. 10, 2022), https://www.bloomberg.com/news/articles/2022-03-10/russia-internet-isolation-accelerates-after-ukraine-invasion#xj4y7vzkg; *Russia, Blocked from the Global Internet, Plunges Into Digital Isolation*, N.Y. TIMES (Mar. 7, 2022), https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html.

[28] *AKP, MHP Propose Amendment to Press Law Introducing Prison Sentences for 'Disinformation'*, BIANET (May 27, 2022), https://bianet.org/english/freedom-of-expression/262461-akp-mhp-propose-amendment-to-press-law-introducing-prison-sentences-for-disinformation.

[29] *Twitter Seeks Judicial Review of Indian Orders to Take Down Content*, REUTERS (July 6, 2022), https://www.reuters.com/world/india/twitter-pursues-judicial-review-indian-content-takedown-orders-source-2022-07-05/ , Twitter, Removal Requests, https://transparency.twitter.com/en/reports/removal-requests.html#2021-jan-jun (last visited Oct. 28, 2022).

[30] *Nigeria Lifts Twitter Ban Seven Months After Site Deleted President's Post*, THE GUARDIAN (Jan. 13, 2022), https://www.theguardian.com/world/2022/jan/13/nigeria-lifts-twitter-ban-seven-months-after-site-deleted-presidents-post; *Nigeria's Twitter Ban Unlawful: W. African Court*, FRANCE 24 (July 14, 2022), https://www.france24.com/en/live-news/20220714-nigeria-s-twitter-ban-unlawful-w-african-court.

Access Now reported there were 182 Internet shutdowns in 34 countries in 2021, an uptick in the 159 shutdowns documented in 29 countries in 2020.[31] The U.S. International Trade Commission detailed the economic losses associated with governments blocking and throttling services as well as executing Internet shutdowns:

> Temporary internet shutdowns and throttling can have a significant effect on digital product and services providers since user access to one or more of their services is reduced or eliminated. This can result in foregone revenue when consumer purchases are paused and/or advertisements are not viewed by users during the course of a shutdown. These disruptions can also reduce the income of businesses and individual users that rely on those sites to disseminate content.[32]

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. Unbalanced 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.[33]

---

[31] *Internet Shutdowns in 2021: The Return of Digital Authoritarianism*, ACCESS NOW (Apr. 28, 2022), https://www.accessnow.org/internet-shutdowns-2021/ [hereinafter "Internet Shutdowns 2021"].

[32] U.S. INT'L TRADE COMM'N, Foreign Censorship Part 2: Trade and Economic Effects on U.S. Business (July 2022), https://www.usitc.gov/publications/332/pub5334.pdf at 66 [hereinafter "Foreign Censorship Part 2"].

[33] 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-data-collection-and-challenge-democracy ("Citing fake news, governments curb online dissent: At least 17 countries

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 often on unreasonable timelines;
- carry, promote, or bar from moderating speech or news content that is positive of local political leaders while simultaneously removing content that opposes those leaders;[34]
- adhere to broadly defined "duties of care" or "responsibilities" that require general monitoring of all user content posted to an Internet service;
- 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;
- require disclosure of automated processes or algorithms used for online platforms;
- 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; designed to limit unintended consequences, especially those that impact online speech; and 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 dangerous 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 should be modernized in a manner that promotes liability rules that are consistent, clear, and work for Internet companies at 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. Predictability in and interoperability between international liability rules is increasingly important to the functioning of cross-border services. Further growth and maturity are dependent on the ability to access and export to international markets.

---

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.").

[34] *Russia Threatens to Block YouTube After Suspension of German RT Channels*, THE GUARDIAN (Sept. 29, 2021), https://www.theguardian.com/technology/2021/sep/29/russia-threatens-to-block-youtube-after-suspension-of-german-rt-channels.

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.

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.[35] Access Now documented 182 Internet shutdowns in 34 countries in 2021, an increase from 159 shutdowns identified across 29 countries in 2020.[36] Internet shutdowns are also costly, with one study finding that countries lose $23.6 million (per 10 million in population) for every day that the Internet is shut down.[37] The USITC estimated that $549.4 million was lost in India due to repeated Internet shutdowns impacting Facebook, Instagram, YouTube, and Twitter between 2019-2021; $82.2 million was lost in Indonesia due to the shutdown of the Internet in 2019; and $14.6 million was lost in Turkey after it blocked several U.S. services in 2020. All of these actions were taken to destabilize protests and/or halt political dissent. Despite these costs, governments continue to filter and block Internet content, platforms, and services for various reasons. For example, the Islamic Republic of Iran has completely shut off access to the Internet in response to protests in the past.[38] In September and October 2022, the government blocked access to Instagram and WhatsApp, and has periodically shut down the Internet across the country,[39] all while activists within and outside of the country leveraged online services such as Instagram to mobilize and publicize events in real-time.[40] In this way, these actions reflect both the harms of Internet shutdowns and the importance of social media services to freedom of expression. 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.

---

[35] *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.

[36] ACCESS NOW, *Internet Shutdowns 2021*, *supra* note 31.

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

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

[39] U.S. DEP'T OF TREASURY, *Treasury Sanctions Iranian Leaders Responsible for Internet Shutdown and Violent Crackdown on Peaceful Protests* (Oct. 6, 2022), https://home.treasury.gov/news/press-releases/jy0994.

[40] *As Unrest Grows, Iran Restricts Access to Instagram, WhatsApp*, REUTERS (Sept. 21, 2022), https://www.reuters.com/world/middle-east/iran-restricts-access-instagram-netblocks-2022-09-21/; *The Challenge of Cracking Iran's Internet Blockade*, WIRED (Sept. 30, 2022), https://www.wired.com/story/subvert-iran-internet-blackout/; *Despite Iran's Efforts to Block Internet, Technology Has Helped Fuel Outrage*, N.Y. TIMES (Sept. 29, 2022), https://www.nytimes.com/2022/09/29/world/middleeast/iran-internet-censorship.html.

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.[41]

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

With respect to the General Agreement on Tariffs and Trade (GATT) obligations that govern trade in physical goods, there is also 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, qualify as "services," analyzed with reference to the General Agreement on Trade in Services (GATS), not the 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 more rational approach is that the digital versions of goods remain goods subject to the GATT."[42] In any event, physical goods may be purchased through digital means, and thereby implicating the objectives embodied in the GATT, which disciplines discriminatory measures relating, for example, to the distribution of goods. The GATT generally requires a contracting party to afford goods supplied from abroad similar status to like products originating from domestic suppliers.[43] Yet in many cases, for example in China, platforms and services through which digital products can be obtained are subjected to specific censorship that provides a competitive advantage to similar domestic products.

The 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."[44] 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 the GATS, numerous provisions discipline the filtering, blocking, and censorship that is applied to Internet services. The GATS imposes considerable obligations on WTO Members, mandating transparency, impartiality, and non-discrimination 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

[41] 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.

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

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

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

obligations exist, such as for "public morals/order,"[45] GATS derogations are only permissible when necessary to achieve the stated objective; where no reasonable, less restrictive alternative exists; and when applied without prejudice.[46] Where nations implement filtering, blocking, and censoring of online services, these standards are rarely met. It is necessary to note that whereas the GATT imposes blanket commitments, the GATS governs sectors and "modes" where a contracting party has made specific commitments. China, however, for example, has made specific commitments pertaining to various web-based service sectors, as well as to value-added telecommunications.[47] As with the GATT, the 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.[48] 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 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.[49] 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 in relation to domestic Internet content.[50]

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

C. Taxation of Digital Services

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.[51]

---

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

[46] GATS Art. XIV. *See also The World Trade Law of Censorship and Filtering*, *supra* note 42, at 13.

[47] 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/.

[48] GATS Art. XVII:1.

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

[50] 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/.

[51] 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,

Further, 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 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.[52] 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.[53]

Pursuant to this commitment, the 141 countries that have agreed to this framework cannot introduce any new unilateral measures and CCIA encourages countries to abandon any national plans to implement.[54] 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.[55]

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.

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

[53] OECD/G20 Base Erosion and Profit Shifting Project, Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation 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.

[54] *Mauritania Joints the Inclusive Framework on BEPS*, OECD (Apr. 4, 2021), https://www.oecd.org/tax/beps/mauritania-joins-the-inclusive-framework-on-beps-and-participates-in-the-agreement-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy.html.

[55] U.S. DEP'T 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

Often based on inaccurate estimates, some countries assert that digital services fail to pay adequate taxes and should be subject to additional taxation.[56] 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 retaliatory action may be helpful to hasten the removal of existing measures pursuant to commitments under the OECD framework. However, insofar as governments globally continue to pursue DSTs in spite of the OECD deal, the U.S. government should continue to push back on these policies as they arise.

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.[57] 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.[58]

---

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.

[56] 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/.

[57] *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.

[58] 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"].

Further, many jurisdictions have either imposed our sought the power to impose customs duties on electronic transmissions to extract fees from digital services providers. 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 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 a number of requirements created that would accompany such an approach, many of which would be extremely difficult to comply with. For instance, data points required for compliance include the description of underlying electronic transfer, end-destination of the transmission, value of transmission, and the country of origin of the transmission — all of which do not exist for most electronic transmissions, especially in the cloud services market.

The moratorium is facing threats within the WTO by pressure primarily from 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 that this is not supported.[63] The United States should continue to advocate for the permanent

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

extension of the moratorium at the WTO at the upcoming Ministerial Conference expected in early 2023, and discourage countries and the World Customs Organization from furthering the inclusion of electronic transmission in their domestic tariff codes.

D. Discriminatory Platform Regulation

A general but ill-defined desire for "platform regulation", unsupported by evidence of consumer harm, is spurring digitally-focused ex-ante regulation around the world, including the EU, Japan, and Australia. In some cases, platform regulation serves as a backdoor for industrial policy dressed up as competition policy, and often employs thresholds designed specifically to target 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.[64] Often, policymakers are clear in public that they are targeting a handful of U.S. companies, but use the narrative of competition policy without robust market analysis to retain the ability to state the policies are not discriminatory.

E. Copyright Liability Regimes for Online Intermediaries

Countries frequently impose penalties on U.S. Internet companies for the conduct of third parties. This is especially true in the context of copyright enforcement. Countries are increasingly using outdated Internet service liability laws that impose substantial penalties on intermediaries that have had no role in the development of the content. These practices deter investment and market entry, impeding legitimate online services. Countries that have imposed copyright liability on online intermediaries contrary to the laws of the United States include France, Germany, India, Italy, and Vietnam. Another concerning trend is the failure of current U.S. trading partners to fully implement existing carefully negotiated intermediary protections in free trade agreements.[65] 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.

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, and such provisions have been a defining aspect of U.S. trade policy for decades, with every modern U.S. trade agreement

[64] 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.")

[65] *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.

since those struck with Chile and Singapore in 2003 including some assurances of copyright balance.[66] That commitment was reiterated by USTR in 2017.[67]

F. Forced Revenue Transfers for Digital News

A concerning trend is developing whereby governments are circumventing free market dynamics to force a select few U.S. online platforms to enter negotiations to pay news publishers for content the publishers allow or actively place on their platforms. These forced payments vary in structure and design, but rather than negotiating for and requiring payment for reproduction of full articles (a common commercial practice), news organizations are seeking to extract revenues from digital firms for quotes, snippets, headlines, and links of news content. The policies share a dangerous set of negative externalities and harms for online services providers as well as for the broader Internet ecosystem.

One form of this effort has come through 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.[68] A USITC report also observed that these laws tend to have "generated unintended consequences" to small online publishers.[69] Service providers of online search, news aggregation, and social media platforms are compelled to pay for the "privilege" of quoting from news publications. This is often referred to as a "snippet tax." It is also at times formally described as "ancillary copyright" in that it is allegedly an "ancillary" IP right — yet it is in fact inconsistent with international IP law, violates international trade obligations, and constitutes a TRIPS-violating barrier to trade.[70] CCIA would encourage U.S. policymakers to carefully evaluate the trade implications of

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

[67] OFFICE OF THE U.S. TRADE REP., *The Digital 2 Dozen* (2017), https://ustr.gov/sites/default/files/Digital-2-Dozen-Updated.pdf. ("the commitment of our free trade agreement partners to continuously seek to achieve an appropriate balance in their copyright systems, including through copyright exceptions and limitations.").

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

[69] 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 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.").

[70] 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.

imposing ancillary rights in the United States.[71] The EU Digital Single Market Copyright Directive creates an EU-wide version of this right.

Meanwhile, other jurisdictions are pursuing regulations forcing these revenue transfers that are unrelated to copyright policy. Australia recently passed the News Media Bargaining Code law that assumes a right to payment in a similar vein to those reliant on ancillary rights. However, Australia relied on an ill-fitting market analysis of news sharing rather than copyright as the basis for granting itself the power to compel digital platforms—namely Google and Facebook—to negotiate payments with news publishers. These two companies have not yet been designated under the law for forced negotiations, but the government retains the threat to do so, should their paid agreements with any news publishers be questioned.

Australia's example is now spreading to other jurisdictions, as Canada has introduced similar legislation to force U.S. companies to pay news publishers for content shared through their platforms. The bill, C-18, would force "digital news intermediaries"—targeted at two U.S. companies based on testimony from Parliament and analyses from the Parliamentary Budget Officer—to pay Canadian news publishers for *any* content of theirs reproduced in *any* way. This would include brief quotes and snippets, headlines, and links. Meanwhile, similar discussions have spread to Taiwan, where interest is brewing to enact Australia-style legislation to force Meta and Google to pay news publishers. Momentum is growing in India to adopt similar rules as well.[72]

Rooting out this problematic and discriminatory policy is key, as its spread could result in billions lost for U.S. firms operating in these countries if left unchallenged. For example, Canada's Parliamentary Budget Office estimated that—under the assumption that only Google and Meta would be included under Canada's legislation—an annual monetary exchange of $329.2 million would be made from those two companies to the news publishers.[73] If this number were to spread to other OECD countries, this could result in billions lost from U.S. industry, summarily transferred, as an effective subsidy to foreign firms. 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.[74]

G. Telecommunications-Related Barriers

U.S. digital services exports are often hindered by foreign jurisdictions adopting telecommunications-related rules and obligations. These policies include engrossing over-the-top (OTT) communications and content services into telecommunications regulations, despite the

[71] U.S. COPYRIGHT OFFICE, *Study on Ancillary Copyright Protections for Publishers* (2022), https://www.copyright.gov/policy/publishersprotections/.

[72] *India Plans to Make Google, Facebook Pay News Publishers For Using Their Content*, INDIA TODAY (July 18, 2022), https://www.indiatoday.in/technology/news/story/india-plans-to-make-google-facebook-pay-news-publishers-for-using-their-content-all-you-need-to-know-1976399-2022-07-16.

[73] Office of the Parliamentary Budget Officer, Cost Estimate for Bill C-18: Online News Act (Oct. 6, 2022), *available at* https://distribution-a617274656661637473.pbo-dpb.ca/cc009955611c336af6d46f82af210ac3445e6c551b3841adae30c1088f487b41.

[74] *Id.*

fundamental differences in their makeup and use, and regulation of telecommunications services upon which digital services are reliant to reach their customers.

A worrying trend is spreading globally, shaped by South Korea's prior and ongoing efforts to force online services suppliers—also called content and application providers (CAPs)—to pay Internet service providers (ISPs) for the traffic of their services, driven by consumer demand. Such policies are allegedly justified by a purported need for ISPs to preserve the resilience of their networks that they argue is burdened by large U.S. CAPs' traffic. This has led policymakers to call for U.S. online services providers to pay "fair contribution" or "level the playing field" with ISPs, resulting in policies and proposals that have proliferated and are now in discussion both in South Korea and the European Union, with industry concerned that Australia and the Caribbean Telecommunications Union could pursue similar policies.

In Korea and the EU, the efforts to force CAPs into paid contracts with ISPs for their services' traffic—demanded by users, not the CAPs themselves—have focused on U.S. services through arbitrary thresholds of subscribership and traffic volume, two metrics which experts suggest have negligible bearing on the strain on the network.[75] These discriminatory mandatory monetary exchanges between CAPs and ISPs—effectively taxes on U.S. online services providers to subsidize incumbent local ISPs—threaten digital trade between the U.S. and key export markets; undermine the Internet ecosystem both locally and globally by establishing sender-party-pays mandates in the mold of telephony; and result in vast inefficiencies for consumers and CAPs alike by disincentivizing the investments online companies make to improve traffic delivery, such as caching servers and data centers.[76]

These fees result in revenue extraction from CAPs for local incumbents, seeking to leverage their bottleneck control over access to their subscribers. CCIA urges vigilance regarding such policies as they move forward in the countries identified below and to contextualize calls for "fairness" with the value content and other online services providers generate for telecommunications networks.

Further, there is a growing effort globally to implement regulations over online services by imposing additional requirements on over-the-top (OTT) communications and content providers that bring them under similar regulatory regimes as traditional telecommunications providers. This developing view—to treat applications operating using the Internet such as OTT communications services, email services, and other Internet-enabled applications and websites the same as legacy telecommunications services—threatens to undermine the model that brought

[75] ANALYSYS MASON, *The Impact of Tech Companies' Network Investment on the Economics of Broadband ISPs* (Oct. 2022), https://www.incompas.org//Files/2022%20Tech%20Investment/FINAL%20Analysys%20Mason%20Report%20-%20Impact%20of%20tech%20companies'%20network%20investment%20on%20the%20economics%20of%20broadband%20ISPs.pdf.

[76] CCIA, Proposal to Mandate by Content and Application Providers (CAPs) Undermine the Future of U.S.-Korea Trade (Sept. 2022), https://www.ccianet.org/wp-content/uploads/2022/09/CCIA-Trade-Analysis-of-Korean-Network-Usage-Fee-Proposals.pdf; INTERNET SOCIETY, Internet Impact Brief: South Korea's Interconnection Rules (May 11, 2022), *Sender Pays: What Lessons European Policy Makers Should Take From the Case of South Korea*, INTERNET SOCIETY (Sept. 30, 2022), https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-south-koreas-interconnection-rules/.

forth the success of the global Internet. These efforts, such as those being pursued in India and Turkey, fail to account for the fact that OTT communications services and those provided by traditional telecommunications providers such as mobile carriers and broadband services are fundamentally different in the services that they provide consumers and their structure. Telecommunications providers operate on the layer of the network which connects different networks and therefore serves as the foundation of the Internet's functioning, whereas OTT providers are applications that operate above the network layer and use the network of networks (*i.e.*, the Internet) to move data between users. While these policy prescriptions undermine the Internet model broadly, insofar as they target U.S. services providers for more stringent requirements than those from other jurisdictions, they could prove an unreasonable hindrance to U.S. services exports as well.

H. Restrictions on Cloud Services

The provision of cloud services drives billions of dollars in economic value, as cloud computing supports a plethora of subsequent industries, applications, and services reliant on cloud infrastructure and suppliers.[77] U.S. cloud service providers (CSPs) are global leaders and represent a remarkable U.S export success, supporting a trade surplus while sustaining tens of thousands of high-paying jobs for U.S. individuals. Increasingly, jurisdictions are seeking to impose onerous and targeted requirements on cloud providers—many of the most prominent representatives of which are from the United States—that limit their ability to operate in these markets. The regulations and policies pursued globally range from traditional protectionist goals to preference local upstarts at the expense of foreign rivals, to measures seeking greater ability to conduct surveillance over individuals.

Examples include rules that mandate security standards preferential to local firms in France that are being considered for the entire EU bloc, certification standards aimed at keeping out foreign competitors in Korea and Vietnam, data localization requirements in Indonesia and Mexico, restrictions on virtual private networks in India, obligations regarding content and possible interception of messages in Malaysia, and a collection of intrusive measures related to intellectual property and business operations imposed in China.

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,

[77] PRECEDENCE RESEARCH, *Cloud Computing Market Size to Hit US$1,614.1 Billion by 2030* (May 13, 2022), https://www.globenewswire.com/en/news-release/2022/05/13/2443081/0/en/Cloud-Computing-Market-Size-to-Hit-US-1-614-1-Billion-by-2030.html.

or compliance with otherwise infeasible judicial orders. There is growing international hostility to encryption.[78]

These exceptional access regimes run contrary to the consensus assessments of security technologists because they are either technically or economically infeasible to develop and effectively implement.[79] Companies already operating in countries that have or are considering anti-encryption laws will be required to alter global platforms or design region-specific devices, or face fines and shutdowns for noncompliance. Companies that might have otherwise expanded to these markets will likely find the anti-encryption requirements to be barriers to entry. Further, given that technology is sold and used on a global basis, introduction of vulnerabilities as required by a number of these regulations risks the privacy and security of users worldwide. The United States should recognize these concerns and address them in future trade agreements, incorporating provisions that prevent countries from compelling manufacturers or suppliers to use a particular cryptographic algorithm or to provide access to a technology, private key, algorithm, or other cryptographic design details.

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.[80] 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.[81] However, industry reports that there are still limits within the "express" regime that make it difficult to export to Argentina and some U.S. companies have had to stop exporting to the Argentinian market completely.

There is another concerning trend regarding tax policies taking place in Latin America where many countries in the region are departing from international best practices and OECD principles through indirect taxes (VAT/GST) on cross-border supplies of electronically supplied services. For example, Argentina implemented a "Financial Intermediary" Tax Collection Model that creates an unlevel playing field. Argentina should be encouraged to instead employ the "Non-

[78] 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/.

[79] 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.

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

[81] 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.

resident Registration" Tax Collection model. Countries including Chile, Colombia, and Costa Rica are considering following Argentina's approach. U.S. suppliers of these cross-border electronically supplied services report instances of double taxation in the region.

Capital Controls

The Argentine government has applied a series of capital controls and new tax measures to the consumption of imports over the past year that make it more challenging for Argentine citizens to import goods and services. On October 28, 2019, the Central Bank established a limit of $200 per month that citizens were able to access through their bank accounts, limiting the amount of money those citizens could use to import goods and services.[82] 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.[83] 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."[84] Combined, these controls and taxes are making it increasingly difficult, and at times impossible, for foreign companies to sell to Argentine customers.

Draft Data Protection Bill

In September 2022, a new Draft Law on the Protection of Personal Data was published in the country's Official Gazette, with a public consultation period running through the end of the month.[85] The law largely tracks with the EU's General Data Protection Regulation (GDPR), although deviates in some key ways, including several requirements for the transfer of data outside of Argentina such as an assurance that the third-party country in question can adequately protect the personal data in the opinion of the data protection authority; that the entity exporting the data offers certain protections for the data processing conditions; or that the exportation of the data falls under another specific situation, such as user consent.[86] The implementation of this law and its final form will prove crucial in determining whether or not the update to the country's data protection laws serve to be a barrier to the free flow of cross-border data.

---

[82] *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.

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

[84] *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.

[85] Resolution 119/2022, https://www.boletinoficial.gob.ar/detalleAviso/primera/271369/20220912 (Sept. 12, 2022).

[86] *New Draft Bill on Personal Data Protection in Argentina*, LEXOLOGY (Sept. 16, 2022), https://www.lexology.com/commentary/tech-data-telecoms-media/argentina/ojam-bullrich-flanzbaum/new-draft-bill-on-personal-data-protection-in-argentina.

B. Australia

Regulation of Digital Markets

In February 2021, the Australian Government passed the News Media and Digital Platforms Mandatory Bargaining Code.[87] 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 also disclose proprietary information related to private user data and algorithms.[88]

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.

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 – both American – have been identified at this time. There are significant concerns from a procedural,[89] competition,[90] trade,[91] and intellectual property[92] 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.

---

[87] Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2021, *available at* https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r665.

[88] *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/.

[89] *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/.

[90] *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/.

[91] *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/.

[92] *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/.

At time of filing, no platform has been officially designated, but it is clear from the Treasury's consultation paper reviewing the code, published in April 2022, that the main targets of the law are Google and Meta.[93] The law continues to be of concern to industry due to its targeting of these two companies.

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.[94] The legislation authorizes the Australian government to use three new tools to compel assistance from technology companies in accessing information within electronic communications. These tools are technical assistance requests (TARs), which seek voluntary assistance from communications providers; and technical assistance notices (TANs) and technical capability notices (TCNs). These tools call upon providers to do one or more specified acts which could include building new technical capabilities as required by the Attorney General. While the legislation specifically forbids a notice to provide a "systemic weakness or vulnerability" into an encrypted system, it does provide sufficiently broad authority to undermine encryption through other technical means with little oversight. Over the past year, technology companies have called for amendments to the bill citing the broad language and failure to address concerns during the drafting process.[95] As of the most recent annual report from the Australian Government Department of Home Affairs, published in February 2022, New South Wales Police was granted a TAN for the first time, which empowers agencies to "compel designated communications providers to give assistance where they already have the technical capability to do so."[96]

Copyright Liability Regimes for Online Intermediaries

Failure to implement obligations under existing trade agreements serves as a barrier to trade.[97] 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

[93] Review of the News Media and Digital Platforms Mandatory Bargaining Code Consultation Paper (Apr. 2022), https://treasury.gov.au/sites/default/files/2022-04/c2022-264356_0.pdf at 10 (showing only deals struck by Google and Meta).

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

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

[96] Telecommunications (Interception and Access) Act 1979 Annual Report 2020-21, https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-20-21.pdf at 2 and 70.

[97] *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.

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.[98] This oversight was not addressed by the recent passage of amendments to Australia's Copyright Act, which expanded intermediary protections to some public organizations but pointedly excluded commercial service providers including online platforms.[99] 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.[100] Criticism for the legislation was widespread, with particular concern about the rushed nature of the drafting and legislative process.[101] The legislation applies to a broad range of technology and Internet services, including U.S.-based social media platforms, user-generated content and live streaming services, and hosting services. However, the law does not take into account the varying business models of these services in scope of the law and their varying capabilities or roles in facilitating user-generated content. CCIA encourages governments to enact policies affecting online content only after consultation by all stakeholders.[102] Australian

[98] 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.

[99] 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/.

[100] 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.

[101] *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.

[102] *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.").

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.[103]

The Online Safety Act which was passed in July 2021 gives the eSafety regulator the power to demand the removal of adult cyber abuse and other content that is deemed "harmful".[104] This legislation also compels eight different sectors of the online industry 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.[105] Industry has mobilized around the scope of services caught by this legislation (social media services, user generated content platforms, search engines, app distribution marketplaces and enterprise hosting services), concerns that turn-around times for content removal are too short (24 hours), lack of transparency and accountability of decisions made by the regulator and that the ill-defined concept of "harm" will lead to lawful content being censored. Industry has developed Codes of Practice in eight different sectors: social media services; websites; search engines; app stores; broadband providers; device manufacturers; hosting services; and miscellaneous electronic services such as email, messaging, gaming, and dating services.[106] The eSafety regulator will assess the Codes of Practice and rule on their adequacy following a review of a public comment period that ran between September 1, 2022, and October 2, 2022.[107] Additionally, the eSafety Commissioner issued legal notices to five companies, all of which are U.S.-based and of varying sizes, demanding disclosures of measures taken to combat child sexual exploitation on their services, with potential fines of $555,000 daily for companies failing to comply.[108]

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

---

[103] 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.

[104] Parliament of Australia, Online Safety Bill 2021, https://perma.cc/637E-N5AF.

[105] *Australia: Online Safety Bill Pa*ssed (2021), Library of Congress Global Legal Monitor, https://www.loc.gov/item/global-legal-monitor/2021-08-10/australia-online-safety-bill-passed/.

[106] Consolidated Industry Codes of Practice for the Online Industry, Phase 1 https://onlinesafety.org.au/codes/.

[107] eSafety Commissioner, *Australians Encouraged to Comment on Draft Industry Codes* (Jan. 9, 2022), https://www.esafety.gov.au/newsroom/media-releases/australians-encouraged-comment-on-draft-industry-codes [Australia].

[108] eSafety Commissioner, *Tech Platforms Asked to Explain How They Are Tackling Online Child Sexual Exploitation* (Aug. 30, 2022), https://www.esafety.gov.au/newsroom/media-releases/tech-platforms-asked-explain-how-they-are-tackling-online-child-sexual-exploitation [Australia].

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

Critical infrastructure reforms

Australia passed a bill putting in place changes to its critical infrastructure framework, with the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 receiving Assent in April 2022.[110] 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'. The proposed legislation significantly expands the sectors considered critical infrastructure (including companies that provide 'data storage or processing' services) and will impose additional positive security obligations for critical infrastructure assets (like risk management programs and cyber incident reporting), enhanced cyber security obligations and, most concerningly, 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.

Hosting Strategy Certification Framework

In 2019, the Australian Government released the Hosting Strategy[111], 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[112] to operationalize the Hosting Strategy. 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.[113] 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. In February 2022, the Australian government published its Media Policy Statement with additional details of the

---

[110] Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6833. See text of bill https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6833_aspassed/toc_pdf/22006b01.pdf;fileType=application%2Fpdf at 10.

[111] Digital Transformation Agency, Whole-of-Government Hosting Strategy, https://www.dta.gov.au/our-projects/whole-government-hosting-strategy [Australia].

[112] Digital Transformation Agency, Whole-of-Government Hosting Strategy - Hosting Certification Framework, (Mar. 2021) https://www.dta.gov.au/sites/default/files/files/digital-identity/New%20Accreditation%20Templates/Hosting%20Certification%20Framework%20-%20March%202021.v2.pdf [Australia].

[113] Media Reform Green Paper (Nov. 2020), https://www.infrastructure.gov.au/sites/default/files/documents/media-reform-greenpaper-december2020_0.pdf [Australia].

policy proposal and next steps. In discussing the government's proposed ability to set content requirements, the Green Paper cites only U.S.-based firms: "The Minister for Communications would have a power to designate large SVOD services, such as Netflix and Amazon Prime, as Tier 1 services. These services would be required to report annually to ACMA on their expenditure on, and provision of, Australian content, and the steps they are taking to make Australian content prominent and discoverable on their services."[114] Mandatory preferences in favor of Australian content, with the exception of certain grandfathered measures, would be generally inconsistent with AUSFTA. CCIA urges USTR to actively monitor these developments and engage with Australia to avoid breaches of AUSFTA.

The government of Australia has committed to new legislation implementing a framework for ensuring streamlined accessibility to and visibility of Australian TV services on connected TV platforms. The government seeks to issue a final decision on the makeup of the regulatory framework by the middle of 2023, at which point lawmakers would begin drafting the legislation. Given the potential of such a framework to disadvantage U.S. content suppliers and connected TV platforms, CCIA urges the U.S. government to actively monitor developments and to engage with partners in Australia to ensure adherence to AUSFTA if the legislation preferences Australian content over foreign content.

Taxation of Digital Services

The Australian Taxation Office (ATO) issued a draft ruling in June 2021, dubbed TR 2021/D4, that would change the parameters for what is deemed a "royalty" in a manner that if finalized, could implicate digital exporters.[115] The delivery of software could be subjected to Australian withholding tax as a royalty and has been considered by the ATO as part of this update. This change to Australian tax code splits from both prior practice in the country and international norms. Under Australia's previous code TR 93/12, which stood in place until the introduction of the new proposal, distributors of software licenses were not deemed to be paying royalties for payments if the license was made to end-users to ensure no software copyrights were being violated. The OECD Model Tax Convention on Income and on Capital similarly recognizes this right, stating that "distributors are only paying for the acquisition of the software copies, not to exploit any right in the software copyrights."[116] The new approach, under TR 2021/D4, would classify distributors and resellers as engaging in an ancillary "authorization" copyright inherent in software programs, regardless of whether the owner of the software copyright has approved any rights to modification, reproduction, or other actions to the distributor in question. This would subsequently implicate traditionally typical aspects of a transaction between software distributors and resellers in engaging in copyright rights exchanges rather than simply exchanging a copyrighted article or supplying a service.

[114] Media Policy Statement: Green Paper Response and Next Steps (Feb. 2022), https://www.infrastructure.gov.au/sites/default/files/documents/media-policy-statement.pdf [Australia].

[115] Draft Taxation Ruling, TR 2021/D4, https://www.ato.gov.au/law/view/document?DocID=DTR/TR2021D4/NAT/ATO/00001.

[116] OECD, https://www.oecd.org/ctp/treaties/model-tax-convention-on-income-and-on-capital-condensed-version-20745419.htm

Industry is concerned that the ATO is seeking to release a second draft of these proposed rules ahead of finalizing the policy before the end of the year or at the start of 2023. Industry is concerned that in its current form, TR 2021/D4 fails to separate income tax applications on payments for gaining copyrighted software and those made to exploit copyright rights. The direction of the rules contravenes international norms on the taxation of software rights and payments that have persisted for years, which could have consequences for U.S. and global firms in Australia and internationally if other jurisdictions similarly abandon precedent. Particularly concerning for U.S. companies, the ATO does not see TR 2021/D4 as inconsistent with its Double Taxation Avoidance Agreements, including its DTAA with the United States.

C. Austria

Taxation of Digital Services

Austria implemented a 5 percent digital tax on revenues from digital advertising services provided domestically.[117] The global revenue threshold is 750 million euro, and domestic revenue threshold is 25 million euro. The tax, implemented in the Digital Tax Act 2020 (*Digitalsteuergesetz* 2020), became effective on January 1, 2020. "Online advertisement services" include advertisements placed on a digital interface, in particular in the form of banner advertising, search engine advertising and comparable advertising services.[118] 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."[119] 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."[120]

---

[117] 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.

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

[119] *Id.*

[120] 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

D. Bangladesh

Digital Security Act

The Digital Security Act of 2018 criminalizes a wide range of online activity, creating challenges for Internet-based platforms and digital media firms.[121] The Act criminalizes publication of information online that hampers the nation, tarnishes the image of the state, spreads rumors, or hurts religious sentiment. The Act provides for criminal penalties up to $120,000 and up to 14 years in prison for certain infractions. The law has come under scrutiny for harming civil liberties and human rights.[122]

Information and Communication Technology Act

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. 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.

Restrictions on Cross-Border Data Flows and Data Localization Mandates

In July 2022, the government of Bangladesh released a draft personal data protection bill dubbed the Data Protection Act.[123] The legislation would implement data localization requirements for sensitive data, user-generated data, and classified data. Industry has expressed concern that the

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.]).

[121] Digital Security Act, 2018, *available at* https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf [Bangladesh].

[122] *How Bangladesh's Digital Security Act is Creating a Culture of Fear*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (Dec. 9, 2021), https://carnegieendowment.org/2021/12/09/how-bangladesh-s-digital-security-act-is-creating-culture-of-fear-pub-85951; *Bangladesh: Scrap Draconian Elements of Digital Security* Act, HUMAN RIGHTS WATCH (Feb. 22, 2018), https://www.hrw.org/news/2018/02/22/bangladesh-scrap-draconian-elements-digital-security-act.

[123] Unofficial translation available at: https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/6c9773a2_7556_4395_bbec_f132b9d819f0/Data%20Protection%20Bill%20en%20V13%20Unofficial%20Working%20Draft%2016.07.22.pdf.

obligations contained within the draft legislation are confusingly defined and break from global norms and procedures.[124]

Government-Imposed Restrictions on Internet Content and Related Access Barriers

In February 2022, the Bangladesh Telecommunication Regulatory Commission proposed a draft of regulations that, if adopted, would grant the government broad-sweeping powers to dictate online content with the threat of extensive punishments for firms and employees deemed non-compliant.[125] The draft bill of the rules, which have been called the Regulation for Digital, Social Media and OTT Platforms, were presented in their final form to a subdivision of the Supreme Court of Bangladesh on October 19, 2022. Despite providing fora for public feedback to the draft legislation, the final draft of the bill appears to reflect none of the vast concerns raised by industry and free expression advocates to the Bangladesh government.[126] The bill empowers the government to demand online services providers remove content from a user or reveal information about a user if necessary to further the "unity, integrity, defence, security, or sovereignty of Bangladesh," is "offensive, false or threatening and insulting or humiliating" to any person, is harmful to "religious values," is "patently false" or belongs to another person, is seen as oppositional to the "Liberation War of Bangladesh, the spirit of the Liberation War, the Father of the Nation, the national anthem, or the national flag," or a wide range of other vaguely-defined violates, all of which would be determined by the government. Further, the bill would require the outright blocking of information in the case of an "emergency," as defined by the government. The demands for removal or blocking of content could be made with a 72-hour window for compliance, with the threat of blocking the content if a platform does not adhere to the demand—given that the bill is extraterritorial in nature, these provisions carry additional burdens for foreign services suppliers. Prior iterations of the bill have included criminal liability and possible prison sentences for local employees along with a $35 million fine, and although the most recent draft suggests the effort is moving towards liability for the firm and not individual employees, the lack of definitions in the bill render this a lingering concern.[127] Given the grave threat of this draft bill to U.S. online services suppliers operating in Bangladesh and the region writ large, CCIA urges USTR to monitor developments and actively engage with Bangladesh in communicating concerns as a final decision could be reached by the end of this year.[128]

---

[124] See Asia Internet Coalition, Industry Submission on Draft Data Protection Act 2022 (Aug. 24, 2022), *available at* https://aicasia.org/wp-content/uploads/2022/09/Industry-submission-by-Asia-Internet-Coalition-on-the-draft-Data-Protection-Act-2022_24-August-2022.pdf.

[125] Bangladesh Telecommunication Regulatory Commission, Regulation for Digital, Social Media and OTT Platforms, 2021, *available at* http://old.btrc.gov.bd/notice-board/bangladesh-telecommunication-regulatory-commission-regulation-digital-social-media-and; http://old.btrc.gov.bd/sites/default/files/u148664/The%20Bangladesh%20Telecommunication%20Regulatory%20Commission%20Regulation%20For%20Digital,%20Social%20Media%20And%20OTT%20Platforms%20%202021.pdf.

[126] *Stakeholders' Consultation Mostly Ignored in Final Draft of Social Media, OTT Regulation*, THE DAILY STAR (Oct. 28, 2022), https://www.thedailystar.net/news/bangladesh/news/it-was-eyewash-3148286.

[127] Global Network https://globalnetworkinitiative.org/wp-content/uploads/2022/03/GNI-BTRC-Submission.pdf and https://www.thedailystar.net/news/bangladesh/news/it-was-eyewash-3148286

[128] *BTRC Draft Rules on OTT: Govt Given Indemnity for Its Action*s, THE DAILY STAR (Oct. 28, 2022), https://www.thedailystar.net/news/bangladesh/news/btrc-draft-rules-ott-govt-given-indemnity-its-actions-3147256

Internet Shutdowns

According to data from Access Now and Meta, the Internet was shut off completely twice in Bangladesh throughout 2021,[129] for 3 days and 13 hours.[130] In addition to the strong human rights concerns associated with government shutdowns of the Internet, there are grave dangers to digital trade as well. As detailed by the U.S. International Trade Commission's two-part investigation into foreign censorship released in February and July 2022, Internet shutdowns can cause millions of dollars in losses for U.S. social media and user-generated-video services, representing a notable loss to U.S. services exports.[131]

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.

Taxation of Digital Services

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.[132]

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

---

[129] ACCESS NOW, *Internet Shutdowns 2021*, *supra* note 31.

[130] Meta, Internet Disruptions, https://transparency.fb.com/data/internet-disruptions/ (last visited Oct. 28, 2022).

[131] U.S. INTERNATIONAL TRADE COMMISSION, Foreign Censorship Part 1: Policies and Practices Affecting U.S. Businesses, https://www.usitc.gov/publications/332/pub5244.pdf (Feb. 2022); Foreign Censorship Part 2: Trade and Economic Effects on U.S. Businesses, https://www.usitc.gov/publications/332/pub5334.pdf (July 2022).

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

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

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.[134] 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.[135] 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.[136]

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 DPA will 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,[137] government procurement preferences for local ICT hardware and software,[138] and non-recognition of the results of conformity assessment procedures performed outside of Brazil for equipment connected to telecommunications networks.[139] 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. 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 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.[140] Industry reports that officials are considering what approach to take with respect to intermediary liability

[134] 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.

[135] 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).

[136] *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.

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

[138] 2014 Decrees 8184, 8185, 8186, 8194, and 2013 Decree 7903.

[139] ANATEL's Resolution 323.

[140] 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/.

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.

Taxation of Digital Services

Brazil is currently considering various digital tax initiatives, including the introduction of a DST through an expansion of its existing CIDE (*contribuição de intervenção no domínio econômico*) regime. The CIDE-Digital tax (PL 2,358/2020) would apply progressively from 1 percent to 5 percent on gross revenues derived from (1) digital advertising; (2) operating a digital service that permits users to interact with each other for the sale of goods and services; and (3) collection of user-generated data in the operation of a digital platform.[141] 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.[142] Brazil should be discouraged from introducing new taxes that discriminate against a specific class of digital companies for specialized taxation.

Additional E-Commerce Barriers

Brazil's *de minimis* threshold for duty-free importation remains at USD $50, which is applicable only to consumer-to-consumer transactions sent through post. This level is not commercially significant. The low threshold increases the time and cost of the customs clearance process for businesses of all sizes and serves as an e-commerce barrier. It also does not apply to business-to-consumer or business-to-business transactions.[143] 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

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

[142] *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.").

[143] 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.

Congressional approval. To compare, the average *de minimis* threshold among OECD members is USD $70 for taxes and USD $194 for duties.[144]

Government-Imposed Content Restrictions and Related Access Barriers

A law designed to address "fake news" was passed by the Senate in July 2020 - Internet Freedom, Responsibility, and Transparency Bill. While there were improvements from its initial draft,[145] concerns remain that some requirements would be used in a manner to pursue restrictions on speech.[146] A new version of that bill—which maintained many of the provisions causing concerns of content and speech restrictions—received a hearing in July 2022. Momentum on the legislation stalling due to the 2022 Presidential election.[147] Further, on September 21, 2021, President Jair Bolsonaro signed an Executive Order that—although temporary in nature and now lapsed—prevented social media companies from taking down content regarding the 2022 Brazilian election that violates their disinformation rules,[148] marking one of the first instances globally of a blatant use of such restriction.[149]

A new set of rules, adopted by the Superior Electoral Court on October 20, 2022, in the build-up to the Brazilian elections, would allow the leader of Brazil's electoral justice system to unilaterally demand online platforms to take down content perceived to be in violation of prior removal orders absent any other entity making such a request.[150] If the social media provider does not adhere to the takedown order within two hours, the platform would potentially have to suspend their operations in the country. The rules have been implemented with a stated interest of combating misinformation, but this brings an excessive amount of power to define false information for one person who subsequently can unilaterally compel compliance with a removal notice, especially with such a short timeline for review and adherence. This takedown regime

---

[144] 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.

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

[146] *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 ; *Joint Statement: Brazil: Disinformation Bill Threatens Freedom of Expression and Privacy Online*, FREEDOM HOUSE (June 29, 2020), https://freedomhouse.org/article/brazil-disinformation-bill-threatens-freedom-expression-and-privacy-online.

[147] PL 2630/2020, https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735.

[148] Provisional Measure No. 1,068, Sept. 6, 2021, https://www.in.gov.br/web/dou/-/medida-provisoria-n-1.068-de-6-de-setembro-de-2021-343277275.

[149] *Brazil's President Bans Social Networks From Removing Some Posts*, N.Y. TIMES (Oct. 19, 2021), https://www.nytimes.com/2021/09/09/world/americas/bolsonaro-social-networks.html.

[150] *TSE aprova resolução para dar mais efetividade ao combate à desinformação no processo eleitoral*, Tribunal Superior Electoral (Oct. 20, 2022), https://www.tse.jus.br/comunicacao/noticias/2022/Outubro/tse-aprova-resolucao-para-dar-mais-efetividade-ao-combate-a-desinformacao-no-processo-eleitoral. See also https://www.tse.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tse.jus.br/comunicacao/arquivos/resolucao-desinformacao/@@download/file/TSE%20-%20Resoluc%CC%A7a%CC%83o%20-%20Desinformac%CC%A7a%CC%83o%20-%20aprovada.pdf.

will hinder the ability of U.S. online services suppliers to operate in Brazil and obstruct freedom of speech as it incentivizes over-compliance to ensure continued operations in the country. The possibility of U.S. firms being forced to suspend operations in the country is deeply concerning as well.

Universal Charging Ports

In June 2022, the National Telecommunications Agency, Anatel, opened a public consultation for a proposal to mandate all cell phones sold in Brazil to require USB-C charging ports. In accompaniment to the blog post announcement, Anatel published documents suggesting the primary incentive for the proposal is to address the problems of e-waste, consumer convenience, and global standardization.[151]

G. Cambodia

Government-Imposed Content Restrictions and Related Access Barriers

Reports of censorship and mandated Internet filtering and blocking continue to rise in Cambodia.[152] Legislation passed in April 2020 grants extensive authorities to the government to restrict information online if a state of emergency is imposed.[153] This has prompted concern at the UN over possible human rights abuses.[154]

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.[155] 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.[156] An Internet Society report from February 2022 detailed how the law would "undermine three of five critical properties of the Internet Way of Networking and negatively impact all four of the qualities that maximize the Internet's potential as an open, globally connected, secure, and trustworthy

---

[151] Agência Nacional de Telecomunicações, Aberta consulta pública para padronização de carregadores de cellular,

https://www.gov.br/anatel/pt-br/assuntos/releases/aberta-consulta-publica-sobre-requisitos-usb-c-em-telefones-celulares. *See also*
https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO4gErf_h9Bj0UpNGsKPLVUml8h5Cufp8xpyuvmnh4zk-UBUiWRWVUTHhPFD9Loa_bNRoVA_2jJv-Il0hxES7s4P

[152] *Freedom on the Net 2022: Cambodia* (2022), https://freedomhouse.org/country/cambodia/freedom-net/2022.

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

[154] In Dialogue with Cambodia, Experts of the Human Rights Committee Ask about Freedom of Expression and Raise Issues Concerning COVID-19 Prevention Measures (Mar. 11, 2022), https://www.ohchr.org/en/press-releases/2022/03/dialogue-cambodia-experts-human-rights-committee-ask-about-freedom.

[155] *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.

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

resource for good."[157] The law was set to go into effect in February 2022, but has been postponed to an undetermined date due to the pandemic.[158] The Cambodian government confirmed its intention to implement the law while defending its legitimacy in a February 2022 statement, and foreshadowed two additional pieces of legislation to come—first one on cybersecurity, to be followed by a different law on personal data protection upon the cybersecurity law's completion.[159]

A draft Cybercrime bill has also been discussed by the Interior Ministry that could hold intermediaries liable for third party content.[160] The bill also contemplates new data localization mandates. In May, government officials reiterated the desire to adopt the legislation,[161] and on September 7, 2022, the Minister of Interior met with government stakeholders for a final discussion about the draft cybercrime bill prior to its submission for a review by the Council of Ministers, bringing it closer to enactment.[162]

H. Canada

Forced Revenue Transfers for Digital News

In April 2022, Canadian Heritage introduced Bill C-18, the Online News Act,[163] which would empower the Canadian Radio-television and Telecommunications Commission to compel large "digital news intermediaries"—namely Facebook and Google—to pay groups of news publishers for *any* reproduction of *any* piece of news content on their services, including headlines, quotes, and links. The legislation, heavily inspired by Australia's News Media Bargaining Code law, tasks the CRTC with devising a list of online platforms that would be designated as digital news intermediaries under the law based on their size *after* the legislation has been enacted. However, it is clear that Bill C-18 targets U.S. companies, namely Google and Facebook, based on the statements made by Canadian lawmakers in discussing the merits of the bill. In a House of Commons debate on C-18, U.S. companies were referenced 73 times, with no references to any non-U.S. company in the context of the debate.[164] Further, Canada's Parliamentary Budget Office, in responding to a request from a Member of Parliament, estimated that $329.2 million

[157] Internet Society: Internet Impact Brief: Cambodia National Internet Gateway (Feb. 18, 2022), https://www.internetsociety.org/resources/2022/internet-impact-brief-cambodia-national-internet-gateway/.

[158] United National Human Rights Office of the High Commissioner, State of Press Freedom in Cambodia (Aug. 2022), https://www.ohchr.org/sites/default/files/2022-08/press-freedom-cambodia-en.pdf at 11.

[159] Press Release, Clarification by the Spokesperson of the Ministry of Foreign Affairs and International Cooperation on the National Internet Gateway Establishment (Feb. 15, 2022), https://www.mfaic.gov.kh/posts/2022-02-15-Press-Release-Clarification-by-the-Spokesperson-of-the-Ministry-of-Foreign-Affairs-and-International-Cooperation-o-10-50-07.

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

[161] Cyberlaw to Address Security Concerns, KHMER TIMES (May 24, 2022), https://www.khmertimeskh.com/501080863/cyberlaw-to-address-security-concerns/.

[162] *Draft Cybercrime Law Nearing Completion*, PHNOM PENH POST (Sept. 7, 2022), https://www.phnompenhpost.com/national/draft-cybercrime-law-nearing-completion.

[163] Bill C-18, An Act respecting online communications platforms that make news content available to persons in Canada, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-18/first-reading [Canada].

[164] House of Commons Debates, May 13, 2022, https://www.ourcommons.ca/DocumentViewer/en/44-1/house/sitting-71/hansard#11685803

would be paid to news publishers annually under the assumption that only Google and Meta would be implicated under the legislation. Most of the money extracted from these two companies—roughly 75% of it—would go to large broadcasters that dominate the broadcast market, with only 25% of the share expected to go to newspaper organizations, according to estimates from the PBO.[165] The estimates perpetuate concerns that the law would forcibly transfer revenue from U.S. digital services firms to shore up local behemoths.

The legislation is in conflict with several of Canada's international trade obligations. These obligations include the U.S.-Mexico-Canada Free Trade Agreement Articles 14.4 (Investment) and 15.3 (Cross-border Services) regarding National Treatment; USMCA Articles 14.5 (Investment) and 15.4 (Cross-border Services) regarding Most-Favored Nation Treatment; USMCA Article 14.10 regarding Performance Requirements; USMCA Article 19.4 regarding Non-Discriminatory Treatment of Digital Products; and intellectual property obligations through the World Trade Organization's absorption of the Berne Convention and the right to quotation in the Agreement on Trade-Related Aspects of Intellectual Property Rights.[166] The Standing Committee on Canadian Heritage in the House of Commons has held several hearings and the legislation has significant support from the Canadian government.

Taxation of Digital Services

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 euro million or more per year, and in-scope revenue associated with Canadian users of more than $20 million per year.[167]

CCIA is concerned that despite the OECD agreement on a global solution, and the clear commitment not to proceed with any new measures, that Canada still intends to finalize this proposed legislation and policymakers have reiterated that they intend to move forward with the DST if the OECD framework is not in place by Jan. 1, 2024.[168] CCIA appreciates USTR's strong

[165] Office of the Parliamentary Budget Officer, Cost Estimate for Bill C-18: Online News Act, *supra* note 73.

[166] CCIA White Paper on Canada's Bill C-18, the "Online News Act" (Sept. 2022), https://www.ccianet.org/wp-content/uploads/2022/09/CCIA-White-Paper-on-Canadas-Bill-C-18-the-Online-News-Act.pdf

[167] CCIA provided comments on the specifics of the Canada DST, available here: https://www.ccianet.org/library-items/ccia-comments-on-canada-dst/

[168] 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-deputyprime-minister-on-new-international-tax-reform-agreement.html; *Will Canada Go It Alone on a Digital Tax?*, POLITICO (Julu 15, 2022),

https://www.politico.com/newsletters/ottawa-playbook/2022/07/15/will-canada-go-it-alone-on-a-digital-tax-00046024.

engagement to push back on the implementation of the tax and to instead steer towards the OECD agreement.[169]

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.[170] 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.[171]

In March 2022, Canadian Heritage announced the creation of a 12-person expert panel which would devise recommendations for a pending proposal aimed at addressing "harmful online content", after publishing a report in February surveying the feedback they had received on the framework.[172] The proposal would establish a digital safety commissioner that would implement rules specifically targeting the following categories of harm: "terrorist content; content that incites violence; hate speech; the non-consensual sharing of intimate images; and child sexual exploitation content" for all "online communication service providers," with penalties of 5% of a provider's gross global revenue or $25 million, whichever value is larger.[173] The February report concluded by saying that the government would "consider next steps and will announce further action shortly." The process has since stalled but is expected to renew once Parliament passes the government's two other major online legislative efforts for online news and online content (C-18 and C-11).

---

[169] OFFICE OF THE U.S. TRADE REP., USTR Opposes Canada's Digital Services Tax Act Proposal (Feb. 22, 2022), https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/february/ustr-opposes-canadas-digital-services-tax-act-proposal.

[170] 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.

[171] *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/.

[172] Government of Canada Announces Export Advisory Group on Online Safety (March 30, 2022), https://www.canada.ca/en/canadian-heritage/news/2022/03/government-of-canada-announces-expert-advisory-group-on-online-safety0.html; Technical Paper available at https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html

[173] *Ottawa Proposes New Rules to Crack Down on Harmful Online Content*, CBC (July 29, 2022), https://www.cbc.ca/news/politics/online-hate-facebook-youtube-social-media-1.6122894

The Canadian government also introduced Bill C-11, which extends Canada's broadcasting regulations to online platforms. Under Bill C-11, 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 would compel the service to give preferential treatment to Canadian content and creators.[174] The stated goal of the bill is to require foreign online streaming services to offer more Canadian content by "contribut[ing] in an equitable manner to strongly support the creation, production and presentation of Canadian programming, taking into account the linguistic duality of the market they serve." The House of Commons passed the legislation on June 21, 2022, and the Senate has conducted a series of hearings studying the bill. The government has so far failed to adequately clarify in amendments that the legislation would not impact user-generated videos on such services. This has profound censorship and digital trade implications, as it necessarily means non-Canadian audio and audio-visual communications will be demoted. Representatives from the content creation, academic, and public interest communities have opposed the bill in addition to the streaming industry.[175] Such preferences are inconsistent with core provisions of the US-Mexico-Canada Agreement and CCIA urges USTR to actively engage to oppose such discriminatory measures.

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.[176]

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.[177]

---

[174] Bill C-11 (Third Reading), June 21, 2021, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-11/third-reading.

[175] YouTube Creators, Canada's Bill C-11: What It Could Mean for Creators and Discoverability on YouTube, https://www.youtube.com/watch?v=pKEGnAo4Eqg; Michael Geist, Opening Statement on Bill C-11, https://www.youtube.com/watch?v=TovmyFfZqIU; What's Wrong with Bill C-11? An FAQ, Open Media (Apr. 4, 2022), https://openmedia.org/article/item/whats-wrong-with-bill-c-11-an-faq; An Update From YouTube Canada on the Online Streaming Act, Google (June 22, 2022), https://blog.google/intl/en-ca/company-news/outreach-initiatives/an-update-from-youtube-canada-on-the-online-streaming-act/.

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

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

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.[178] After industry concerns, the OPC determined that it would not amend the guidelines.[179] Rather, it intends to direct lawmakers to reevaluate existing law and determine whether legislative changes are needed. The Government of Quebec passed privacy legislation in September 2021 that, amongst other things, would make data transfers extraordinarily difficult.[180] The law entered into effect on September 22, 2022, with various provisions entering into effect in phases over three years.[181] The U.S. International Trade Commission identified the law as a barrier to digital trade in its "Year in Trade 2021" report published in August 2022.[182] Industry is following these proceedings. Abrupt changes to procedures that enable data transfer between the U.S. and Canada may conflict with provisions in the Digital Trade Chapter of USMCA and Canada's commitments under CPTPP, which both contain commitments for all parties to enable cross-border data flows.

Regulations on the Trade of Artificial Intelligence Systems

On June 16, 2022, the Canadian government introduced C-27, the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act.[183] The Artificial Intelligence and Data Act seeks to establish "common requirements, applicable across Canada, for the design, development and use" of AI systems.[184] Artificial intelligence systems are defined with a broad brush as any technological system that, "autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions." Many of its definitions are left excessively opaque or undefined, leaving interpretations that could lead to disclosure of trade secrets, excessive punishments for innovators, and restrictions on services trade for online

[178] 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"].

[179] 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/.

[180] *Quebec to Introduce the Most Punitive Privacy Laws in Canada – With Fines of up to $25 Miillion*, LEXOLOGY (June 19, 2020), https://www.lexology.com/library/detail.aspx?g=a42e22b1-ec2d-4a79-a9d3-74519ef6a3e8.; *Quebec's Updated Privacy Law Complicates Cross-Border Data Flows*, BLOOMBERG LAW (Nov. 12, 2021), https://news.bloomberglaw.com/privacy-and-data-security/quebecs-updated-privacy-law-complicates-cross-border-data-flows.

[181] *Canada Reforms Its Data Privacy Laws Through Enactment of Quebec Bill 64*, LEWIS BRISBOIS (Feb. 16, 2022), https://lewisbrisbois.com/blog/category/data-privacy-cyber-security/canada-reforms-its-data-privacy-laws-through-enactment-of-quebec-bill-64.

[182] U.S. INT'L TRADE COMMISSION, The Year in Trade 2021 – Operation of the Trade Agreements Program, https://www.usitc.gov/publications/332/pub5349.pdf at 184.

[183] Bill C-27 First Reading, June 16, 2022, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

[184] Id.

programs. "High-impact" AI systems are not defined in the bill, and are set aside for elucidation in future regulations, while also putting legal obligations on individuals or companies who "develop or make available for use the artificial intelligence system or manage its operation" to determine whether or not a system is "high-impact" or risk punishment of a fine. The lack of clarity regarding "high-impact" AI systems is concerning as it will inform the extent to which this legislation applies to firms currently developing technology given the scope and ability of the Minister of Innovation, Science and Industry to regulate them.

Further, the definition of "person responsible" is insufficiently delineated and wide-sweeping. The bill does not clarify whether individuals who design, develop, or use an AI system would be considered equivalent to a person who is "managing" that same system. A person or entity making a "high-impact" AI system available for use must also make a wide range of information available online, including "the types of content that it is intended to generate and the decisions, recommendations or predictions that it is intended to make," which could veer into revealing proprietary information. As such, Bill C-27 could undermine the development of a growing and innovative field by creating regulatory uncertainty.

Additionally, industry is watching the development of Bill C-27's data protection provisions to ensure that it remains aligned with provincial regulations as well as those governing U.S. firms in the United States and European Union.

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.

Government-Mandated Content Restrictions

In September 2021, five Senators introduced the Digital Platforms Regulation Bill, Nº 14.561-19, to put in place a series of rules for digital platforms that the bill defines as "all digital infrastructure whose purpose is to create, organize and control, through algorithms and people, a space for interaction where natural or legal persons can exchange information, goods or services."[185] The bill would implement convoluted requirements for online platforms to conduct

[185] Regula las plataformas digitales, https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15047&prmBOLETIN=14561-19. *See also International Civil Society Warns About the Dangers to the Exercise of Rights of the Bill to Regulate Digital Platforms Presented in Chile,* ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (Nov. 24, 2021), https://www.apc.org/en/pubs/international-civil-society-warns-about-dangers-exercise-rights-bill-regulate-digital-platforms.

proactive monitoring of user activity to take down illegal content to avoid punishment,[186] while also limiting their ability to remove harmful legal content.[187] The bill also includes concerning language that broadens the scope of the legislation outside of Chile's borders and expands the "right to be forgotten" to potentially include the contents of articles as well as user data.[188]

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, cloud services, data transfers and e-commerce 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.[189] 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 a number of localization and protectionist measures.[190] The United States International Trade Commission has estimated billions of dollars are being lost in the market as a result. The USITC estimates that Facebook loses anywhere from $3.1 billion to $13.3 billion every year, depending on the size its market share were if it could operate in the

[186] [186] Id. https://www.apc.org/en/pubs/international-civil-society-warns-about-dangers-exercise-rights-bill-regulate-digital-platforms ("The bill attributes "strict liability" for all damages caused by a platform (article 15), in contradiction with its own rules of exemption from liability (article 6), and empowering the courts to double the compensation for such damages, creating in Chile the figure of punitive damages that has no legal recognition or consistency with the Chilean legal system. At the same time, imposing strict liability is contrary to the recommendation of the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, by stating that "a strict liability scheme in the field of electronic or digital communication is incompatible with minimum standards regarding freedom of expression".")

[187] GNI Letter and Analysis: Draft Digital Platform Regulation in Chile https://globalnetworkinitiative.org/chile-digital-platforms-bill/ ; https://medium.com/wikimedia-policy/a-chilean-bill-would-prohibit-community-based-content-moderation-2488d84022f4 ("Article 6 actually creates contradictory obligations by stating that user-generated content "may not be removed unless they might be considered civilly injurious, libellous, or they constitute threats or constitute crimes established by other legal bodies or that incite to commit a crime."").

[188] *A Chilean Bill Would Prohibit Community-Based Content Moderation. It Could Outlaw the Work of Wikipedia Editors*, WIKIMEDIA POLICY (Mar. 10, 2022), https://medium.com/wikimedia-policy/a-chilean-bill-would-prohibit-community-based-content-moderation-2488d84022f4.

[189] 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/.

[190] 2019 CCIA NTE Comments, https://www.ccianet.org/wp-content/uploads/2019/10/USTR-2019-CCIA-Comments-for-NTE.pdf at 34-40.

country. YouTube would lose anywhere from $100 million to $7.5 billion and Google Search could have lost $2.6 billion if it had a small market share and $15.5 billion if it had a large market share in 2021 alone. 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.[191]

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.[192] There is confusion regarding how this draft affects prior draft legislation on cross-border data and localization mandates issued pursuant to the Cybersecurity Act.[193]

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.[194] "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."[195]

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.[196] 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

---

[191] 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.

[192] 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/.

[193] 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").

[194] 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/.

[195] *Id.*

[196] 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/.

by third parties and data integration, revised notification requirements for incident response, and requirements to maintain data processing records.[197]

The two draft Measures above are reportedly being submitted for deliberation during the National People's Congress term ending in 2023.[198]

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.[199] 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. Under the power of the Data Security Law, China's Ministry of Industry and Information Technology published its latest draft of the "Administrative Measures on Data Security in the Industry and Information Technology Sectors" on February 10, 2022.[200] The draft defines industry data, telecommunications data, and radio data; sets requirements for delineating risk factors for each set of data as either core, important, or ordinary; and establishes mandates for companies to comply with data security and protection requirements, including security assessments of the government for the exportation of data. MIIT is continuing to assess comments as it devises a final draft of measures.[201]

In August 2021, the Personal Information Protection Law was passed. The law went into effect on Nov. 1.[202] The PIPL includes requirements to notify and explicitly obtain consent from owners of data when their PII is sent abroad from China and when data is processed beyond a target set by the Cybersecurity Administration of China, they must pass a security assessment to send PII abroad. Data localization rules, required implementation of a data protection officer for firms, targeted advertising restrictions, and enhanced powers to the new CAC are all included as well. Its extraterritorial application of data protection requirements and strict restrictions on international

---

[197] 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/.

[198] 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/.

[199] 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/.

[200] Text at: https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20219/6b7e6d62a890492996225806cc530144.pdf.

[201] *China Issues Draft Measures on Data Security in the Industry and Information Technology Sectors*, WILMER HALE (Feb. 17, 2022), https://www.wilmerhale.com/en/insights/client-alerts/20220217-china-issues-draft-measures-on-data-security-in-the-industry-and-information-technology-sectors.

[202] Translation available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

transfer of personal information data will add burden to multinational companies and limit the ability of US companies to operate in China.

The PIPL implements security certification, standard contractual clauses, and an assessment of security by Cybersecurity Administration of China as the three avenues firms must undertake to export PII outside of China. On June 24, 2022, the final draft of *Cybersecurity Standard Practice Guideline—Specification for Security Certification of Personal Information Cross-Border Processing Activities* was issued by TC260. Due to the lack of administrative measures and a national standard, these guidelines are likely to represent the blueprint by which firms must abide for security certification and operations conduct.

Subsequently, on June 30, 2022, The Cyberspace Administration of China announced a new set of draft rules, the "Standard Contract Provisions for Personal Information Exit (Draft for Comment)," that provide detailed rules for firms engaging in cross-border data transfers.[203] The draft rules seek to strengthen a data security law established in September that mandates firms operating in China to categorize the data they process to determine how that data gets stored or transferred to other entities and followed a separate set of draft rules put forward in April which sought to reinforce data security checks for firms engaging in cross-border data flows.[204] The new draft rules would require firms handling personal data to implement a set of procedures for the signing of "Standard Contracts," such as determining the legal status of data, the scope of data, the necessity for collection, and the level of protection that personal data would receive once transferred abroad.[205] Under the proposed rules, PI processors will be required to meet certain conditions for permission to export PI and by signing a Standard Contract with the entity receiving the data abroad.

The CAC released its *Measures on Data Exit Security Assessment* on July 7, 2022, with an effective date of September 1, 2022. These rules delineate the obligations for firms to transfer data deemed important as well as PI by Critical Information Infrastructure operators as well as other firms of a certain size, defined by volume of data. Data processors are required to execute a data exit risk assessment and identify key assessment issues prior to issuing a data exit security assessment.

The measures described above will also compel companies from outside China to reveal the entirety of their corporate data mapping including the routes through which cross-border data is trafficked, implicating trade secrets and crucial IPR.

Critical Information Infrastructure entities were further shored up through the Critical Information Infrastructure Security Protection Regulation, which went into effect on September 1, 2021. The rules left several crucial aspects of the legislation—such as its scope and the obligations imposed on firms—unclearly defined. The procurement of "secure and trustworthy" services and products

[203] Text at: http://www.cac.gov.cn/2022-06/30/c_1658205969531631.html.

[204] *New Specifications for Cross-Border Processing of Personal Information for MNCs*, CHINA BRIEFING (May 11, 2022), https://www.china-briefing.com/news/china-cross-border-personal-information-transfer-new-clarifications-for-multinational-companies/.

[205] *Cross-Border Data Transfer – New Provisions Clarify Contract Procedure for Personal Information Export*, CHINA BRIEFING (July 4, 2022), https://www.china-briefing.com/news/cross-border-data-transfer-new-provisions-clarify-contract-procedure-for-personal-information-export/.

for networks are incentivized through the rules, which is likely to lead to companies from China being preferred to foreign firms. Companies labelled as a Critical Information Infrastructure operator are further submitted to additional requirements including certification and assessment obligations and cybersecurity reviews, providing undue burdens to U.S. and foreign companies and an obstacle to participation in the market.

National Treatment

Industry has expressed concern regarding China's Standardization Law, which are leveraged as regulations to impose China's security and technological requirements for participation in the market. The cryptographic standards adopted by China mandate that firms use technologies that are founded on cryptographic algorithms from China for security. This obligation represents a significant barrier to entry, as the standards that serve as the foundation for the rules were developed by a Chinese cryptographic industrial authority that excludes foreign companies from participation.

Restrictions on Cloud Services

China seeks to further restrain foreign cloud service operators, in concert with its national plan to promote the Chinese cloud computing industry. As CCIA have noted in previous submissions, U.S. cloud service providers (CSPs) are worldwide leaders and strong U.S exporters, supporting tens of thousands of high-paying American jobs and making a strong contribution toward a positive balance of trade.[206] While U.S. CSPs have been at the forefront of the movement to the cloud in virtually every country in the world, China has blocked them.

Draft Chinese regulations combined with existing Chinese laws will force U.S. CSPs to transfer valuable U.S. intellectual property, surrender use of their brand names, and hand over operation and control of their business to a Chinese company in order to operate in the Chinese market. Without immediate U.S. Government intervention, China is poised to implement fully these restrictions, effectively barring U.S. CSPs from operating or competing fairly in China.

China's Ministry of Industry and Information Technology (MIIT) proposed two draft notices – Regulating Business Operation in Cloud Services Market (2016) and Cleaning up and Regulating the Internet Access Service Market (2017). These measures, together with existing licensing and foreign direct investment restrictions on foreign CSPs operating in China under the Classification Catalogue of Telecommunications Services (2015) and the Cybersecurity Law (2016), would require foreign CSPs to turn over essentially all ownership and operations to a Chinese company, forcing the transfer of incredibly valuable U.S. intellectual property and know-how to China.[207]

[206] 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.

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

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

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

Export Controls

China finalized a new export law in October 2020 that took effect on December 1, 2020.[208] 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.

Online Intermediary Liability Restrictions

The Cyberspace Administration of China published draft rules in June 2022 outlining the obligations of online service providers and content creators regarding the management of comments and reply comments posted on platforms—including live-streaming services—as an update to the 2017 rules under the Provisions on the Management of Internet Post Comments Services.[209] The draft rules include requirements for "post comment service providers" to verify the identity of users posting comments; establishing measures through which they handle and process data; inspect comments in real-time, review all comments before posting them, and report "unlawful and negative information" to the relevant internet information departments; and hire a review and editorial team reflecting the scale of the services offered, thereby "increasing the professional caliber of review and editorial staff." Comments and replies reflected one of the key ways the public communicated about the COVID-19 pandemic with fellow residents and people abroad.[210] It is currently unclear when this law will go into effect, but the CAC accepted public comments on the draft rules until July 1.

The Cyberspace Administration of China announced in March 2022 the results of its QingLang Operation conducted throughout 2021 with a stated aim to "create a better internet ecosystem in

---

foreign CSPs and Chinese companies be disclosed in detail to regulators. These measures are fundamentally protectionist and anti-competitive.

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

[209] Text available at: http://www.cac.gov.cn/2022-06/17/c_1657089000974111.htm; https://www.chinalawtranslate.com/en/comment-service-restrictions-draft/.

[210] New Draft Rule Portend More Internet Censorship in China, AXIOS (June 21, 2022), https://www.axios.com/2022/06/21/china-internet-censorship-comments-social-media.

China," while also outlining its goals for 2022.[211] Over 22 million "illegal" pieces of information, over 2,160 "illegal" apps were eliminated, about 1.34 billion "illegal" accounts were forcibly closed, and over 3,200 websites were shut down, according to the CAC. In 2022, the department stated it plans to engage in crackdowns and asserting the Chinese Communist Party's vision for the internet including in the areas of live streaming, internet rumors through fact-checking, algorithm governance, and internet safety and appropriateness for minors during the summer holidays.[212]

Additional E-Commerce Barriers

China passed its first law regulating "e-commerce" in August 2018 which took effect in January 2019.[213] 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."[214] Requirements include the need to obtain a business license to operate.

China's State Administration of Market Regulation proposed amendments in October 2021 to its 2018 e-commerce law largely focused on intellectual property and counterfeits.[215] The proposed amendments would lengthen the waiting period following counter-notice, permit e-commerce providers to secure against losses in the midst of lengthy waiting periods, and implement fines in the case that a false claim that no infringement occurred leads to the intellectual property rights holder experiencing losses. Further, the proposed new version of the law would impose restriction or revoke licenses from e-commerce providers for serious cases if they fail to root out sellers pushing products that infringe on intellectual property rights.

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.[216] 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

---

[211] *China's Cyberspace Regulator Punishes Accounts Abusing Athletes like Gu Ailin*g, GLOBAL TIMES (Mar. 17, 2022), https://www.globaltimes.cn/page/202203/1255187.shtml; *Enforcement Trends From China's Cyberspace Regulator in 2022*, PERKINS COIE (Apr. 11, 2022), https://www.perkinscoie.com/en/news-insights/enforcement-trends-from-chinas-cyberspace-regulator-in-2022.html.

[212] *QingLang Regulations, More of Them and More Control on Chinese Social Media* (Mar. 23, 2022), https://bitterwinter.org/qinglang-regulations-more-control-on-social-media/.

[213] 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/.

[214] *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.

[215] U.S. DEP'T OF AGRICULTURE, China State Administration of Market Regulation Proposed Amendments to E-Commerce Law (Dec. 2021), https://apps.fas.usda.gov/newgainapi/api/Report/DownloadReportByFileName?fileName=China%20State%20Administration%20of%20Market%20Regulation%20Proposed%20Amendments%20to%20E-Commerce%20Law_Beijing%20ATO_China%20-%20People%27s%20Republic%20of_11-28-2021.pdf.

[216] *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.

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.[217] Revision to the legislation in 2018 that sought to implement the U.S.-Colombia FTA copyright chapter includes no language on online intermediaries.[218] 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,[219] a core component of its national strategy on AI. While the Framework adopted some good practices such as taking a 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.

Taxation of Digital Services

The third Commission of both Chambers of Congress passed a new tax bill that introduces new difficulties for U.S. exporters, called No. 118 of 2022, on October 6th, 2022, with a goal of final passage in November 2022.[220] The bill implicates U.S. firms operating in Colombia for both digital goods and services through Articles 57 and 61. Under the legislation, effectively all U.S. firms would be forced to make a choice between paying Colombian income tax paired with a 10% withholding tax at source or instead paying a 5% tax on *all* gross income from the sale of goods, the supplying of digital services, or both to consumers in Colombia.

---

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

[218] 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/.

[219] Presidential Advisory for Economic Affairs and Digital Transformation Presidency of the Republic of Colombia, Ethical Framework for Artificial Intelligence in Colombia (2021), https://dapre.presidencia.gov.co/dapre/SiteAssets/documentos/ETHICAL%20FRAMEWORK%20FOR%20ARTIFICIAL%20INTELLIGENCE%20IN%20COLOMBIA.pdf.

[220] Colombian Proposed Tax Reform 2022: Main Impacts on the Extractive Industry (Aug. 17, 2022), https://www.jdsupra.com/legalnews/colombian-proposed-tax-reform-2022-main-4687709/.

For companies providing goods to the Colombian market, the bill would implicate U.S. firms with a "deliberate and systematic interaction" to Colombia's market and earn "31,300 tax units" (which would translate to USD $300,000 currently) during the relevant tax year, a relatively low bar for inclusion. Digital services providers would be included regardless of their relation to or earnings in Colombia, the provision of select services defined in the proposed bill would trigger its obligations for such suppliers that are so wide sweeping they would likely include all online services offered in Colombia. The provision of online or downloadable mobile applications; electronic books, music, and movies; streaming services without charge; subscription-based audio-visual content; online education; as well as "[o]ther electronic or digital services" and "[a]ny other services provided through a digital market for users" in Colombia.

Along with these provisions, a new 10% withholding tax for entities selling goods or services would be applied where there is a significant economic presence in Colombia and other aspects of article 408 of the Colombian Tax Code do not apply.

These measures are inconsistent with global tax norms, which favor taxing income at the permanent establishment associated with income generation, as well as the evolving principles being developed at the OECD to address global tax fairness. In addition, since the U.S. does not have a tax treaty with Colombia, implementation of this measure would likely to result in double taxation for U.S. companies. To the extent that this measure results in the treatment of U.S. manufacturers, distributors, content creators, and service suppliers being treated less favorably than Colombian entities, it also raises serious issues of Colombia's compliance with its trade obligations under both the WTO and the United States-Colombia Trade Promotion 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.[221] Government ownership and 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. [222] In August 2021, the Cuban government adopted new regulations that ban dissent against the government on social media, making it illegal to criticize "the constitutional, social and economic" rules of the

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

[222] *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/

country or that provoke acts "that alter public order."[223] The definitions behind false information and public safety are extremely vague and left in the hands of the government authorities.[224]

M. Czech Republic

Taxation of Digital Services

Announced by the Ministry of Finance in July 2019,[225] the Czech Republic is currently finalizing its digital tax.[226] 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.[227] 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.[228] The effective date has been delayed. Policymakers have cited the need to tax U.S. companies despite support for an OECD solution.

Forced Revenue Transfers for Digital News

The implementation of the EU Copyright Directive in the Czech Republic is currently in the final stages ahead of final adoption with several amendments that would target U.S. firms, represent a marked shift away from other EU member states' implementation of the directive, and threaten U.S. companies' ability to combat misinformation and online harmful content. Amendment 1274 represents a particularly problematic interpretation of Article 15 of the EUCD for industry, as it seeks to target "dominant" firms by imposing discriminatory obligations from which local competitors would receive exemption. Provisions that would restrict or adjust U.S. firms' services would hinder their ability to fight disinformation. U.S. business operations in the Czech Republic would be further harmed through powers granted to the Ministry of Culture to set remuneration with no safeguards regarding values determined or methodology along with obligations for firms to provide "all data necessary" with the Ministry of Culture absent protections for IP or trade secrets. Punishments for not adhering to the mandates would be set at one percent of a company's turnover worldwide.

---

[223] Text available at https://www.gacetaoficial.gob.cu/sites/default/files/goc-2021-o92.pdf. *See also Cuba Spells Out Social Media Laws, Forbidding Content That Attacks the State*, NBC NEWS (Aug. 18, 2021), https://www.nbcnews.com/news/latino/cuba-spells-social-media-laws-forbidding-content-attacks-state-rcna1703.

[224] *Cuba Passes Regulations Criminalizing Online Content, Further Restricting Internet Access*, COMMITTEE TO PROJECT JOURNALISTS (Aug. 19, 2021), https://cpj.org/2021/08/cuba-passes-regulations-criminalizing-online-content-further-restricting-internet-access/.

[225] 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.

[226] Kathy Larsen & Jan Stojaspal, *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.

[227] 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 at 7.

[228] *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/.

Further, the Czech Republic government seeks to implement Article 17 of the EUCD through provisions, in Article 51a, which could empower Czech legal associations and business rivals the power to seek the blocking of U.S. firms' services in the country if the suppliers in question repeatedly block lawful content. If this provision is implemented as drafted, it would present a significant threat to online services suppliers' ability to moderate harmful content and fight disinformation. Further, the CJEU has previously ruled that Article 17 as drafted provides sufficient protections for user rights of freedom of expression and information, such that the Czech Republic's Article 51a is not only potentially harmful, but also unnecessary.

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.[229] This includes industrial and competition policy, platform regulation and increased platform liability, regulation of artificial intelligence and a range of technology-specific certification schemes. The pursuit of "technological sovereignty" will likely disadvantage U.S. exporters to the benefit of domestic competitors and will likely also undermine Europe's long-term prospects for digital innovation.

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

Raising concerns on key policy disagreements that hinder U.S. exports to the European Union through fora such as the EU-U.S. Trade & Technology Council will be key for U.S. policymakers.[230]

Restrictions on Cross-Border Data Flows and Data Localization

Industrial Policies and Technological Sovereignty

As part of the EU-wide push for "technological sovereignty," the EU has advanced industrial policy proposals 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 as a preferred alternative to successful U.S. suppliers.

The European Union Agency for Cybersecurity (ENISA) has built upon protectionist cybersecurity certification standards adopted in France in the EU's Cybersecurity Certification

[229] 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/.

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

Scheme for Cloud Services (EUCS).[231] A draft of the certification with "high assurance level" includes data localization requirements within the EU; prohibition for non-EU entities to own, in part or in whole, or operate cloud services in the EU; obligation for customer support employees to be located in the EU; and a stated objective of cloud services providers being "operated only by companies based in the EU, with no entity from outside the EU having effective control over the CSP, to mitigate risk of non-EU interfering powers undermining EU regulations, norms and values."

While the EUCS is not mandatory on its own, the NIS2 Directive allows national governments, national enforcement authorities, and/or the European Commission to mandate specified cloud customers, even in commercial sectors, to only use a certified EUCS cloud service.[232] Separately, national enforcement authorities under the proposed Data Act can arbitrarily require cloud vendors to obtain an EUCS certification before accessing parts or the whole of the EU market.[233]

Organizations which may be required, directly or indirectly, to use an EUCS certified cloud services include: public bodies, over 10,000 "essential entities" regulated under the NIS2 Directive,[234] any number of "important entities" regulated under said Directive,[235] and any other European companies using or contemplating using cloud services regulated under the Data Act. Since the EU has WTO obligations prohibiting discrimination with respect to both government procurement and purely commercial offerings of cloud services it is unclear how such measures could be legitimately justified.

The Data Act, introduced in February 2022, seeks to build on other digital market regulations such as the Digital Markets Act and Digital Services Act to establish restrictions on how companies can use personal, commercial, and industrial data generated within the EU as well as additional obligations for large firms operating in local data markets.[236] The Data Act proposal

[231] ENISA, Cybersecurity Certification: Breaking New Ground (June 6, 2022), https://www.enisa.europa.eu/news/enisa-news/cybersecurity-certification-breaking-new-ground; Key Organisations Express Concerns Over the Cybersecurity Certification Scheme for Cloud Services, https://amchameu.eu/news/key-organisations-express-concerns-over-cybersecurity-certification-scheme-cloud-services.

[232] Articles 21(1) and 21(2) NIS2 allow Member States and the European Commission to require essential and important entities to use an EU certified ICT product, service, or process.

[233] Under the Data Act proposal, any national enforcement agency may require cloud providers to obtain an EUCS certification complying with sovereignty requirements as a method to adhere to Article 27 the proposed Data Act, which requires companies to adopt "technical, legal and organisational measures" to prevent non-EU government access to non-personal data, regardless of whether the actor processes that data. The draft scheme makes an explicit reference to this possibility.

[234] Under Annex I NIS2 Directive, "essential entities" include among others airlines, banks, railway companies, energy companies, Securities Exchanges, pharmaceutical companies, healthcare providers, digital infrastructure providers including those providing online communications tools, ICT managed services, and public administration entities.

[235] Under Annex II NIS2 Directive, "important entities" include car manufacturers, electrical components manufacturers, medical device manufacturers, food production, processing and distribution companies, online marketplaces, search engines and social networking platforms, and public and private research organisation;

[236] Press Release, Data Act: Commission Proposes Measures for Aa Fair and Innovative Data Economy (Feb. 23, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

features new prescriptive rules on when, where, and how companies should be able to access, process, and share data with other companies and governments. This includes prohibiting U.S. companies from becoming third parties to receive IoT data—both personal and non-personal—in Europe if designated as "gatekeepers"; potentially creating a separate regime for non-personal data transferred internationally for cloud services providers regarding third party countries' requests for access to non-personal data; obligations to share data that contains proprietary information; and by potentially empowering national regulators to oversee aspects of the proposal, raising the possibility of duplicative enforcement throughout the 27 member states. Such regulation, if enacted could leave U.S. companies at a distinct disadvantage compared to European and other non-U.S. entities in a constantly innovating and growing IoT market.

The EU's Data Governance Act[237] implements restrictions to the transfer of certain non-personal data held by the public intermediaries to third-party countries, 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.[238] However, the GDPR governs restrictions for personal data, while the DGA extends these obligations to non-personal data. The Data Governance Act was published in the Official Journal of the European Union in June 2022, and the new rules will begin to be enforced on September 24, 2023.[239]

The updated cybersecurity legislation ('NIS2')[240] will impose 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). The legislation is at an advanced stage, with the European Parliament and EU Member States reaching a political agreement on the legislation in May 2022.[241] The legislation would include the obligation for such providers to be certified against an EU certification scheme to be developed under the EU Cybersecurity Act ('CSA').[242] The NIS2 Directive would also intensify reporting requirements and punishments. The first EU cybersecurity scheme under development relates to cloud services which feature discriminatory requirements against U.S. providers as described in the section above.

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

---

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

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

[239] Available at https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52020PC0767.

[240] Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN.

[241] Press Release, Commission Welcomes Political Agreement on New Rules on Cybersecurity of Network and Information Systems (May 13, 2022), https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985.

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

- In July 2022, a letter from primarily French cloud providers supports discriminatory requirements against U.S. companies in part to curb the marketshare of "three US-based companies which hold 70% of the European market."[243]
- In April 2022, the Franco-German-led GAIA-X cloud project published its own labeling scheme whose "level 3" assurance entails 'sovereignty' requirements similar to EUCS (data localisation, non-EU ownership restrictions, employee location restrictions, etc).[244]
- In February 2022, the European Commission stated in a Q&A document that the proposed Data Act will introduce "mandatory safeguards to protect data held on cloud infrastructures in the EU . . . . With these measures, the Data Act will support cloud adoption in Europe, which will in turn stimulate efficient data sharing within and across sectors."[245]
- In December 2021, several French Members of the European Parliament supported discriminatory requirements in the EUCS.[246]
- In November 2021, the European Data Protection Board wrote to ENISA and the European Commission in support of data localization and discriminatory requirements against U.S. cloud vendors, arguing that "strong guarantee that the cloud service provider is not subject to foreign access incompatible with the GDPR would facilitate the compliance of processing activities relying on cloud services certified with [EUCS high assurance level]."[247]
- In July 2021, the governments of France, Italy, Spain and Germany shared a non-public paper arguing that the transparency requirements of the draft certification scheme for cloud services (EUCS) "are not sufficient to face the concern of the lack of immunity to non-EU laws."
- 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 place "verified safeguards" to ensure that any foreign request to access EU (personal and non-personal) data is compliant with EU law.[248]

---

[243] European cloud providers call "not to give in to the pressure" over sovereignty requirements, Euractiv, 14 July 2022, *available at* https://www.euractiv.com/section/data-protection/news/european-cloud-providers-call-not-to-give-in-to-the-pressure-over-sovereignty-requirements/

[244] *See* criteria 54-61 under the "European control" section of Gaia-X labeling criteria, 21 April 2022 available on https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X-labelling-criteria-v22.04_Final.pdf

[245] European Commission, Data Act- Questions and Answers (Feb. 23, 2022), https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114.

[246] French Renew MEPs' letter to Commissioner Breton, Commissioner Schinas, and Commission Vice-President Vestager, *available at* https://twitter.com/GrudlerCh/status/1466448581997568005/photo/1

[247] Letter from 18 November, *available at* https://edpb.europa.eu/system/files/2021-11/edpb_letter_to_enisa_out2021-00157.pdf

[248] 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.

- 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."[249]
- French President Macron stated that Europe should not rely "on any non-European power" for data security.[250]
- 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.[251]

The discussion at the 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 are "SecNumCloud" certified - services which comply with a French cybersecurity certification requiring data storage in France or in the EU and restricting foreign ownership of the cloud supplier.[252] On 12 September 2022, the French government announced it would define when the "sensitive data" of private and public sector organizations must be processed by a SecNumCloud-certified vendor.[253] The French government also hinted it may require private sector companies at large to use SecNumCloud certified products.[254] To date, only a smaller number of French companies have obtained or are looking to obtain this certification.[255] Specific tenders, requiring SecNumCloud certification have begun to be issued, effectively precluding U.S. suppliers from participating, and calling into question France's compliance with its WTO Government Procurement Agreement obligations.
- The Italian Cloud Strategy (September 2021)[256] bears many similarities with the French strategy. However, it also explicitly requires the storage and processing of encryption keys in Italy for certain categories of data. This requirement will apply for any certified (or 'qualified') commercial cloud services that may be used to host local and central

[249] 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.

[250] *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.

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

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

[253] *Cloud: cinq nouveaux dispositifs pour soutenir le développement du secteur* (Sept. 9, 2022), https://www.economie.gouv.fr/cloud-cinq-nouveaux-dispositifs-soutenir-developpement-secteur#.

[254] Speech from Minister Lemaire, 12 September 2022, available at https://presse.economie.gouv.fr/12-09-2022-discours-de-bruno-le-maire-sur-la-strategie-nationale-pour-le-cloud/

[255] Cloud services and companies which are 'SecNumCloud' certified are available on page 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 on https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/

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

> 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 centers "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 have been decided by the Italian national cybersecurity agency and the Department for Digital Transformation through subsequent implementing regulations. Industry would benefit from the new Government and Cybersecurity Agency engaging with global cloud suppliers on sovereignty measures for the Italian Cloud Strategy.

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.[257] 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 Maire unveiled details on plans to create Europe's own cloud services, titled "GAIA-X".[258] 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."[259] The stated goal of European policymakers has not strayed from data sovereignty, as the most recent architecture documents released by the organization state a mission to "create a federated open data infrastructure based on European values regarding data and cloud sovereignty."[260] GAIA-X company members commit to letting customers demand that their data be processed and stored exclusively in the EU.[261]

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 using these ostensible concerns as a justification for supporting local industry players and excluding

---

[257] 2021 CCIA NTE Comments at 45 ("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.")

[258] 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.

[259] 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.

[260] Gaia-X Architecture Document (2022) https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-x-Architecture-Document-22.04-Release.pdf at 5.

[261] Gaia-X Policy Rules Document, https://www.gaia-x.eu/sites/default/files/2021-05/Gaia-X_Policy%20Rules_Document_2104.pdf.

U.S. industry from public procurements.[262] 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,[263] 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.

There are indications that 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 in the cloud sector.[264] Member States are expected to inject subsidies into several European cloud vendors while exempting them from EU state aid rules. France and Germany have 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.[265] This IPCEI would add to a 10 billion euros pledge that 25 Member States and the European Commission had already signed up to in late 2020.[266]

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.[267] The GDPR is intended to unify data protection methods for individuals within the EU and confront issues resulting from the export of personal data outside of the EU. Since taking effect, a number of small businesses and online services have ceased serving customers in the EU market due to compliance costs and uncertainty over obligations. Following the adoption of GDPR, there has been an observed increase in the number of apps exiting the market as well as a decline in the number of new breakthrough apps.[268]

---

[262] *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.

[263] 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/.

[264] 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.

[265] 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

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

[267] 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"].

[268] National Bureau of Economic Research, GDPR and the Lost Generation of Innovative Apps (May 2022), https://www.nber.org/papers/w30028 ("Using data on 4.1 million apps at the Google Play Store from 2016 to 2019, we document that GDPR induced the exit of about a third of available apps; and in the quarters following implementation, entry of new apps fell by half.")

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.[269] The ruling created immediate legal uncertainty for thousands of companies, a majority of 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 welcomed the Trans-Atlantic Data Privacy Framework to replace Privacy Shield announced in March 2022,[270] and applauded the signing of the Executive Order to enhance the privacy safeguards for signals intelligence activities.[271] CCIA encourages the European Commission to take the necessary steps to implement this new framework which will bring clarity and assuredness to businesses operating in both markets. The swift adoption of an EU adequacy decision and the formal extension of the Data Protection Review Court redress mechanism to EU residents under the Executive Order[272] are especially critical for all companies subject to on-going probes by local supervisory authorities.[273]

In the trade negotiation context, it is unfortunate that the EU's preferred approach on data flows, providing unbounded discretion to assert privacy concerns as a reason to restrict cross-border data flows could increase the likelihood of data localization rather than reduce barriers.[274] The

[269] 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

[270] Press Release, CCIA Applauds EU-US Agreement on Transatlantic Data Flows (Mar. 25, 2022), https://www.ccianet.org/2022/03/ccia-applauds-eu-us-agreement-on-transatlantic-data-flows/.

[271] Press Release, Transatlantic Data Flows: CCIA Welcomes Signing of Executive Order Enhancing Privacy Protections for Europeans and Facilitating Transfer (Oct. 7, 2022), https://www.ccianet.org/2022/10/ccia-welcomes-signing-of-executive-order-enhancing-privacy-protections-for-europeans-and-facilitating-transfers/.

[272] Section 3 (f), "Designation of qualifying state" of the Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities.

[273] Since the CJEU decision to invalidate the Privacy Shield adequacy decision, and several regulators have already imposed a quasi-data localization requirement in Europe, partly on the basis of the European Data Protection Board's Recommendations 01/2020. *See* Keir Lamont, *The Monkey's Pause: Mailchimp Data Transfers Halted in German Schrems II Inquiry*, DISRUPTIVE COMPETITION PROJECT (Apr. 2021), https://www.project-disco.org/european-union/040621-the-monkeys-pause-mailchimp-data-transfers-halted-in-german-schrems-ii-inquiry/. Some regulators even appeared to require U.S. companies to adopt "additional requirements" even if data stays in Europe. *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/.

[274] 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

EU has included such provisions in its FTA with the UK, and has presented comparable 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.[275] The proposal seeks to expand the existing Directive, which only applies to telecommunication services, to all "electronic communication services" including over the top services.[276] 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."[277] This is based on a flawed understanding of the services at issue and it is ignoring the fact that the Internet 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.[278] In June 2022, the Council and the European Parliament concluded a provisional political agreement for the proposal and it will be applicable from June/July 2023.[279] Under the new rules,[280] 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

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.").

[275] 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"].

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

[277] *Id*. at recital 6.

[278] Proposal for a Regulation of the European Parliament and of the Council on foreign subsidies distorting the internal market, https://ec.europa.eu/competition/international/overview/proposal_for_regulation.pdf.

[279] Council of the EU, Foreign Subsidies Distorting the Internal Market: Provisional Political Agreement Between the Council and the European Parliament (June 30, 2022) https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/foreign-subsidies-regulation-political-agreement/.

[280] Provisional Agreement Resulting From Interinstitutional Negotiations, *available at* https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/INTA/DV/2022/07-13/1260231_EN.pdf.

exemptions, film credits, preferential tax treatment, cash grants, and the broad category of "the provision of goods or services or the purchase of goods or services."[281]

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 business's complete financial records and details of business transactions for the last 5 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% of global turnover, exclusion from on-going and future procurement for up to 3 years, forced abstention from certain investments, 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 redressive 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.[282] The Commission is currently working on an Implementing Regulation that will seek to clarify the Regulation.

Network Usage Fee Proposal

In response to a campaign from incumbent European telecommunications providers, the European Commission announced its intention to launch a public consultation in December 2022 or early 2023 to consider a 'Sending-Party-Network-Pays' (SPNP) model for Internet traffic.[283] This is similar to the regulatory model being expanded upon in South Korea, the effect of which (as in the EU) would be additional fees assessed predominantly on successful U.S. firms, whose content and applications have attracted significant foreign demand. The United States and partner nations rejected this proposal when advanced by the European Telecommunications Network Operators' Association (ETNO) a decade ago. Similar to Korean operators, ETNO suggests that large U.S. content access providers (CAPs) should be required to pay fees to

[281] *Id.* at 22.

[282] See for example the U.S. and the UK being singled out where page 51 of the proposal explains the correlation between FDI origins and subsidy spenders. The proposal is available at https://ec.europa.eu/competition/international/overview/proposal_for_regulation.pdf.

[283] *EU's Vestager Assessing if Tech Giants Should Share Telecoms Network Costs*, REUTERS (May 2, 2022), https://www.reuters.com/business/media-telecom/eus-vestager-assessing-if-tech-giants-should-share-telecoms-network-costs-2022-05-02/.

European ISPs for the content demanded by the ISPs' customers. The telco incumbents estimate that total payments could amount to 20 billion euros annually, i.e., more than four times the amount discussed under the abandoned EU Digital Services Tax proposal.

The initial ETNO report spurred European lawmakers' encouragement for a proposal to force "Big Tech" companies to pay ISPs for receiving their traffic cites solely American companies as responsible for the traffic that requires subsidizing.[284]

ETNO's proposal is discriminatory by nature and in evident contrast with the net neutrality principle, as it leaves the door open to discriminatory behaviours of incumbent telcos, who could throttle or block internet users' access to specific services in case of lack of agreement with content providers. In addition, there is growing evidence that telcos have successfully accommodated growing traffic from content and application providers (the source of demand for their services) with relatively little additional network investment.[285] This suggests that this initiative is simply a strategic attempt to leverage anti-tech sentiment for commercial gain, by obtaining governmental sanction for creating a new tollbooth to access to their customers. Several EU member states have expressed backing for the telecoms' campaign; in foreshadowing the upcoming consultation, EU Commissioner for the Internal Market Thierry Breton said, "We also need to review whether the regulation is adapted with the 'GAFAs' (Google, Apple, Facebook, Amazon) for example, which use bandwidth (provided by) telecom operators."[286]

The proposal of the incumbent telecommunications providers has been challenged by some member states, seven of whom suggested slowing down the process to avoid unintended consequences of implementing a SPNP requirement.[287] In October 2022 the body of European telecom regulators (BEREC) stated that it "has found no evidence that such mechanism is justified" and warns that the proposal "could be of significant harm to the Internet ecosystem." BEREC, however, only has a consulting role in EU lawmaking.

CCIA urges USTR to engage early and firmly to dissuade the advancement of discriminatory and anticompetitive rules forcing network usage fee.

---

[284] ETNO, Europe's Internet Ecosystem: Socio-Economic Benefits of a Fairer Balance Between Tech Giants and Telecom Operators (May 2022), https://etno.eu//downloads/reports/europes%20internet%20ecosystem.%20socio-economic%20benefits%20of%20a%20fairer%20balance%20between%20tech%20giants%20and%20telecom%20operators%20by%20axon%20for%20etno.pdf.

[285] Analysys Mason, *supra* note 75.

[286] *EU To Consult on Making Big Tech Contribute to Telco Network Costs*, REUTERS (Sept. 9, 2022), https://www.reuters.com/technology/eu-consult-big-tech-contribution-telco-networks-by-end-q1-2023-2022-09-09/.

[287] *Seven EU Countries Warn the Commission Against Hasty Decisions on 'Fair Share'*, EURACTIV (Julu 25, 2022), https://www.euractiv.com/section/digital/news/seven-eu-countries-warn-the-commission-against-hasty-decisions-on-fair-share/.

Regulation of Digital Marketplaces

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. The European Commission reached a political agreement on implementation for the Digital Markets Act in March 2022 and the European Parliament formally adopted it in early July.[288] The rules are expected to enter into effect in early 2023. Under the rules, 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, reflecting some policymakers' intent to ensure that only U.S. firms fall under scope.[289] 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 will 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. In this sense the DMA represents a dramatic shift in competition enforcement, resulting in greater potential infringement on fundamental intellectual property rights and freedom to contract only in exceptional circumstances. Unlike traditional competition enforcement, the Commission will be able to impose these interventions without an assessment of evidence, without taking into consideration any effects-based defenses, and without considering procompetitive justifications put forth by the companies targeted. It is concerning that this DMA "gatekeeper" designation is now being extended into new EU regulations including the Data Act.[290]

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

[288] Press Release, Digital Markets Act: Commission Welcomes Political Agreement on Rules to Ensure Fair and Open Digital Markets (Mar. 25, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1978 and https://ec.europa.eu/commission/presscorner/detail/en/IP_22_4313.

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

[290] Press Release, Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy (Feb. 23, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

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.[291] The European Commission reached a political agreement on implementation for the Digital Services Act in April 2022, and the European Parliament formally adopted the rules in July 2022.[292] These new rules will police how providers moderate for illegal content, counterfeiting, collaborative economy services, or product safety. The DSA is expected to be published in the Official Journal of the European Union in November 2022.

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 recommendation systems, and appoint a compliance officer. Fines can reach up to 6% of annual turnover. Further, "very large online platforms"—defined as those with 45 million active users or more in the EU—will only have 6 months to comply with the new regulations, while most companies receive 15 months to prepare.[293]

The DSA was weaponized as a means to incorporate regulations on a variety of other topics not initially germane to the stated goal of online safety. For example, the inclusion of restrictions on personalized targeted advertising, undermines the horizontal normative purpose of the DSA proposal and harms European companies along with U.S. firms.

Online marketplaces, including a large number of U.S. companies, could become liable for every product sold through their channels. As such, 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 be incentivized to take down products, meaning fewer products would become available online. Some categories of products considered too risky, could even be dropped. CCIA has encouraged EU lawmakers to address sector specific concerns in a sector-specific bill, such as the June 2020 General Product Safety Regulation (GPSR) proposal.[294] This bill seeks to update the existing Product Safety Directive to respond to new challenges related to online purchases including via marketplaces.[295] Building on the DSA, the GPSR imposes further restrictions on online marketplaces by creating deadlines for responses to authorities' orders or users' notices

[291] 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/.

[292] Press Release, Digital Services Act: Commission Welcomes Political Agreement on Rules Ensuring a Safe and Accountable Online Environment (Apr. 23, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545.

[293] Victoria de Posson, *Will the DSA's Short Compliance Deadlines Set Some Companies Up to Fail?,* DISRUPTIVE COMPETITION PROJECT (June 14, 2022), https://www.project-disco.org/european-union/061422-will-the-dsas-short-compliance-deadlines-set-some-companies-up-to-fail/.

[294] The General Product Safety Directive, https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/consumer-product-safety_en.

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

regarding product safety or creating a stay down obligation forcing marketplaces to remove products identical to ones previously flagged by authorities.

Further, the European Commission proposed new rules "to prevent and combat child sexual abuse" in May 2022 that would direct online service providers to implement a mandatory series of measures to detect and report in real-time any known child sexual abuse material, new child sexual abuse material, and grooming or solicitation of children.[296] The rules apply to a range of providers including software application stores, but the most stringent mandates of scanning and monitoring private messages and content generated by users are imposed on providers of hosting service and interpersonal communications. The rules include obligations on risk assessment and mitigation, detection of material, reporting, takedowns, child restrictions on accessible content, and oversight measures. Concerns have emerged from a broad set of experts and stakeholders, including from the German privacy chief and government as well as civil society regarding the implementation of what could result in an oppressive surveillance system.[297] The European Commission opened a public consultation through September 5, 2022, which CCIA responded to.[298]

The EU's rules on "Preventing the dissemination of terrorist content online", passed in 2021, went into effect on June 7, 2022.[299] Among the requirements imposed through the rules, "hosting service providers" operating in the EU must take down terrorist content within one hour of notice of its presence and take "proactive measures commensurate with the level of risk and to remove terrorist material from their services, including deploying automated detection tools." The Member States determine penalties for failure to comply, which can range from warnings to fines of up to 4% of a company's global revenue for repeated failure to adhere to the rules.

Copyright Liability Regimes for Online Intermediaries

On May 17, 2019, the Copyright Directive was published in the Official Journal of the European Union.[300] The Member States had until June 7, 2021, to implement this new EU law. Only four countries (Germany, the Netherlands, Hungary and Malta) have implemented the new rules as of

[296] Press Release, Fighting Child Sexual Abuse: Commission Proposes Rules to Protect Children (May 11, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2976; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472.

[297] James Vincent, *New EU Rules Would Require Chat Apps to Scan Private Messages for Child Abuse*, THE VERGE (May 11, 2022), https://www.theverge.com/2022/5/11/23066683/eu-child-abuse-grooming-scanning-messaging-apps-break-encryption-fears; Letter to European Commission from EDRI (June 8, 2022) https://edri.org/wp-content/uploads/2022/06/European-Commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law.pdf

[298] CCIA Position Paper: The Proposed EU Regulation to Prevent and Combat Child Sexual Abuse (Sept. 2022), https://www.ccianet.org/wp-content/uploads/2022/09/CSAM-CCIA-Position-Paper-9-September-2022.pdf.

[299] Legislative Timeline available here: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0331(COD)&l=en.

[300] 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.

October 2021. The European Commission has opened an infringement procedure against the other 23 member states for not transposing the bloc's copyright rules in time.[301]

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.

The European Commission released guidelines on implementation of Article 17 only four days before the deadline, on June 17, 2021.[302] This article effectively requires online services to implement filtering technologies. While Article 17 avoids the word "filter", content-based filtering is the only practical means of achieving compliance. This upends longstanding global norms on intermediary liability. Absent obtaining a license from all relevant rightsholders, online services will be directly liable unless they: (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 "best efforts" standard does not mitigate other requirements, since "best efforts" is a subjective but still mandatory standard open to abuse and inconsistent interpretations at the member state level. In an April 2022 ruling, the Court of Justice of the European Union found that "the obligations established in this Directive should not lead to Member States imposing a general monitoring obligation."[303] However, despite this clarification, the ruling declined to exclude upload filters outright as a general obligation.

Despite claims to the contrary by EU officials, lawful user activities will be severely restricted. Some have noted that requirements would not affect lawful user activity such as sharing memes, alluding to the exceptions and limitations on quotation, criticism, review, and parody outlined in the text. However, while the text itself does not explicitly "ban memes," the resulting actions online services will have to take to avoid direct liability is the restriction of lawful content. Algorithms used to monitor content on platforms cannot contextualize specific content to determine whether it was lawfully uploaded under one of the exceptions listed. Additionally, the exceptions and limitations provided for only apply to users, not the sharing services themselves (¶ 5: "Member States shall ensure that users in all Member States are able to rely on the following existing exceptions and limitations when uploaded and making available content generated by users"). This makes the exceptions largely meaningless for services that have relied on it, and who no longer receive the same rights as users.

---

[301] *See* https://ec.europa.eu/commission/presscorner/detail/en/mex_21_3902?utm_source=POLITICO.EU&utm_campaign=14d27e1a3e-EMAIL_CAMPAIGN_2021_07_26_11_26&utm_medium=email&utm_term=0_10959edeb5-14d27e1a3e-190504281.

[302] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1625142238402&uri=CELEX%3A52021DC0288.

[303] Judgment available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=258261&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=758534.

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, or consumers will face 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.

CCIA remains concerned with the Copyright Directive's Article 15 and the creation of a press publishers' right.[304] Contrary to U.S. law and current commercial practices, Article 15 may effectively require search engines, news aggregators, applications, and platforms to enter into commercial licenses before including snippets of content in search results, news listings, and other formats. The exception for "short excerpts" and single words is highly unlikely to provide any real certainty for Internet services who wish to continue operating aggregation services, and conflicts with the current practice of many U.S. providers offering such services.

The Copyright Directive does not harmonize the exceptions and limitations across the EU. The freedom of panorama exception (the right to take and use photos of public spaces) was left out of the proposal entirely. Moreover, while a provision on text and data mining is included, the qualifying conditions are highly restrictive. The beneficiaries of this exception are limited to "research organizations," excluding individual researchers and startups.

As EU states implement the new copyright rules into their national law, some governments are re-interpreting key provisions leading to potentially far-reaching and problematic consequences for users, publishers and platforms alike. One example of this trend can be found in Croatia.[305] While the European Commission, and Commissioner Breton have specified "that Member States are not allowed to implement Article 15 . . . through a mechanism of mandatory collective management",[306] the Croatian draft law includes a provision which would make it mandatory for all publishers to license these rights collectively. This creates new barriers and challenges for U.S. companies when complying with national rules.

France has already started to implement this provision of the EU Copyright Directive as it created an analogous right for press publishers which entered into force in October 2019. News publishers can now request money from platforms when platforms display their content online.

---

[304] *Id*.

[305] *Croatia's Diverging Implementation of EU Copyright Rules*, DISRUPTIVE COMPETITION PROJECT (Sept. 15 2021), https://www.project-disco.org/european-union/091521-croatias-diverging-implementation-of-eu-copyright-rules/.

[306] Parliamentary Question, Answer Given by Mr. Breton on behalf of the European Commission (2020) https://www.europarl.europa.eu/doceo/document/E-9-2020-004603-ASW_EN.html.

Following this development, Google announced in September 2019 that it would change the way articles appear in search results instead of signing licensing agreements.[307] In October 2019, the French competition authority opened an investigation into Google's compliance with the French law transposing the Copyright Directive, and in April 2020, the competition authority ordered Google to pay French publishers under the new law.[308] In October 2020, Google and the "Alliance de la Presse d'Information Générale", which represents newspapers such as Le Monde, announced that future licensing agreements would be based on criteria such as the publisher's audience, non-discrimination and the publisher's contribution to political and general information.[309] Notwithstanding this offer, in July 2021, the French competition authority imposed a €500 million fine on Google as it considered that the company did not negotiate "in good faith" with the press industry over licensing fees.[310] Google appealed this decision, considering the fine disproportionate to their efforts to reach an agreement.

In the Czech Republic, an amendment was proposed in October 2022 regarding the implementation of Article 15 of the EU DSM Copyright Directive to introduce a new set of obligations which would restrict platforms' ability to offer and evolve their products. These proposals depart from other Member States' implementation of Article 15, particularly with respect to the classification of (undefined) "dominant" platforms and the targeted obligations on these select few companies. The proposal would prohibit "dominant" platforms from "arbitrarily restrict[ing] or adjust[ing] the service in a discriminatory manner"—effectively establishing a must-carry, must-pay obligation; introduce new arbitration procedures where either party can request the Ministry of Culture to determine remuneration following 60 days of negotiation; mandate the sharing of "all data necessary" with the Ministry of Culture to determine remuneration without including safeguards for the protection of IP and/or trade secrets; and empowers the Ministry with the ability to impose of up to CZK 500,000 or 1% of the total global turnover for the previous financial year (whichever is highest) for non-compliance.

A separate amendment proposed in the Czech Republic proposes to address Article 17 of the EUCD in a manner industry finds problematic as it is not prescribed by the Directive. As written, the provision, Article 51a, empowers both groups of users represented by a legal association and platforms' rivals themselves with the right to seek blocking of a platform's service if the supplier in question repeatedly is said to fail to block lawful content. This provision stretches beyond the purview of the EUCD and threatens to restrict online services providers' procedures aimed at decreasing the spread of disinformation and the harmful content online. Industry is concerned that this amendment simultaneously hinders business operations in the Czech Republic and

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

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

[309] *Google Poised to Strike Deal to Pay French Publishers for Their News*, REUTERS (Oct. 7, 2020), https://www.reuters.com/article/us-alphabet-france-publishing/google-poised-to-strike-deal-to-pay-french-publishers-for-their-news-idUSKBN26S33C.

[310] *Rémunération des droits voisins : l'Autorité sanctionne Google à hauteur de 500 millions d'euros pour le non-respect de plusieurs injunction* (July 13, 2021), https://www.autoritedelaconcurrence.fr/fr/article/remuneration-des-droits-voisins-lautorite-sanctionne-google-hauteur-de-500-millions-deuros.

violates basic competition law principles of equal treatment. Further, the CJEU has previously ruled earlier in 2022 that the framework of Article 17 included necessary safeguards for user information and freedom of expression while offering users' rights and rightsholders' intellectual property rights adequate support.

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.[311] 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.[312] 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.[313] 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.[314]

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.[315] 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

---

[311] 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.

[312] *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).

[313] *Id.* at ¶ 72.

[314] 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").

[315] GDPR art. 17.

burdensome. For example, popular U.S. services have fielded hundreds of thousands of requests since the policy went into effect.[316] 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.

A September 2022 opinion from the Advocate General on the topic of Meta's breach of GDPR provided sweeping advice to the Court of Justice of the European Union about the application of the law more broadly in the Internet ecosystem.[317] First, the Advocate General recommended that the CJEU rule that any authority in Europe has the ability to investigate and conclude a violation of GDPR *if* the authority informs the pertinent data protection authority of its action. Second, companies do not have the ability to process personal data for the provision of personalized services (such as an organic newsfeed), ad delivery, and integrated user experience for multiple products without user consent. Third, companies identified as dominant could be unable to process personal data even if users *do* consent.

Regulations on Artificial Intelligence

In April 2021, the European Commission proposed the AI Act to regulate artificial intelligence (AI) across all sectors. The objective is to support AI in the EU and protect EU citizensArtificial Intelligence. The EU Member States and European Parliamentarians are finalizing their respective positions and final negotiations and agreement is expected in 2023 and may apply as early as 2025 in all 27 EU Member States.

Lawmakers see AIA as an opportunity to set global norms: like GDPR, AIA would be a first-of-its-kind regulation, with the potential to carry soft influence worldwide as businesses adapt to EU-specific requirements, and to inspire AI regulation in other regions. The broad definition of AI in the AIA includes systems usually not considered AI. These systems are regulated by risk level: (1) low-risk systems are subject to transparency rules; (2) high-risk systems must comply with a comprehensive regulatory regime including 100+ requirements including a conformity assessment, auditing requirements, and post-market monitoring; and (3) prohibited systems pose unacceptable risk and are banned. The law will apply to both providers and users of AI systems where the "output" of that system is used in the EU. Fines can reach up to 6% of annual global turnover.

Various unclear definitions of AI, classification of high-risk and prohibited AI, and allocation of responsibilities for actions in the AI value chain could lead to harms for firms from both the U.S. and EU. The broad definition of so-called "high-risk" applications, cumbersome compliance requirements and steep fines, create new compliance burdens for U.S. companies doing business in the EU. Further, the definition of AI Systems and associated techniques is overly broad and

[316] 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.

[317] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021CC0252&from=en.

could include practically *any* current or burgeoning software systems, regardless of whether they perform actions associated with definitions commonly linked to AI. Additionally, the definition of a "provider" of high-risk AI systems includes any "person, public authority, agency or other body" that even has "a view to placing it on the market or putting it into service under its own name or trademark," a broad and highly prescriptive approach that could impair research and development.[318] Further, it is unclear how the legislation defines "physical or psychological harm" the basis for banning AI systems that use techniques "beyond a person's consciousness in order to materially distort a person's behavior in a manner that causes or is likely to cause . . . physical or psychological harm". Additionally, the expansive definition of "high-risk" in the proposal—in its current form—could dampen innovations and create legal uncertainty and new hindrances for the pre-approval processes for products and services that are already subject to a multitude of regulatory mandates.

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 data centers, content delivery networks, telecommunications services, Internet Exchange Points, DNS). The legislation is at an advanced stage, as the European Parliament and EU Member States reached a political agreement on the legislation in May 2022.[319] This will also include the obligation for such providers to be certified against an EU certification scheme to be developed under the EU Cybersecurity Act ('CSA').[320] One of the first EU cybersecurity schemes under development relates to cloud services and features overt discriminatory requirements against non-EU cloud providers.

In September 2022, the European Commission introduced a Cyber Resilience Act proposal (CRA)[321] which creates extensive approval processes that a wide range of digital products and services would have to undergo before they can be sold and used on the EU market. The draft rules set up an elaborate approval process for stand-alone software and "connected" products that consumers and businesses use, from mobile and desktop operating systems and antivirus software to smart meters. The CRA also has ramifications for all services which use software and hardware covered by the Act throughout their supply chain. This would affect cloud storage, messaging and email, online marketplaces, search engines, and even social networks. The European Parliament and Council are expected to start reviewing the proposal during the fall of 2022.

---

[318] CCIA Position Paper on the EU Artificial Intelligence Act (Jan. 2022), https://www.ccianet.org/wp-content/uploads/2022/01/CCIA-Position-Paper-on-the-EU-Artificial-Intelligence-Act.pdf.

[319] Press Release, Commission Welcomes Political Agreement on New Cybersecurity of Network and Information Systems (May 13, 2022), https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985.

[320] 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

[321] European Commission, Cyber Resilience Act, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

Mandatory Universal Charger

On June 7, 2022, the European Parliament and Council negotiators reached an agreement on legislation to require all mobile phones, tablets, and cameras to use USB-C chargers. On October 4, 2022, the European Parliament passed legislation enshrining the rules, to begin by the beginning of 2024, with the mandate being applicable to laptops by 2026. The rules undermine device makers with an existing market share that operate in Europe.

Media Freedom

The European Commission introduced the European Media Freedom Act in September 2022 with a dual goal of supporting media freedom and diversity and protecting journalists.[322] Given the several existing rules governing digital services with implementation codes under development such as the Digital Services Act, the Digital Markets Act, and the EU Code of Practice on Disinformation, industry harbors concern regarding a lack of clarity around how this set of rules interacts with these other regulations. The U.S. government should pursue engagement with European partners to ensure that the EMFA does not supersede or revise these legislations while their implementation is still under development and to instead await evidence of these other pieces of legislation's effect on business and Internet use. Given the proven ability of the Internet to connect individuals to a broader set of diverse news sources than ever before possible and the contribution of online services to promoting media plurality and small news organizations by lowering the barrier to entry, the goal of promoting free and fair trade and media freedom should be viewed as complementary.

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.[323]

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.[324] 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

[322] Press Release, European Media Freedom Act: Commission Proposes Rules to Protect Media Pluralism and Independence in the EU (Sept. 16, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5504.

[323] *Freedom on the Net 2022: Egypt*, https://freedomhouse.org/country/egypt/freedom-net/2022; *Egypt: End the Blocking of News Websites*, ARTICLE 19 (Aug. 1, 2022), https://www.article19.org/resources/egypt-end-the-blocking-of-news-websites/; Blocked Websites in Egypt, https://masaar.net/en/blocked-websites-in-egypt/ (last visited Oct. 28, 2022).

[324] *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.

conflict with the existing Media law of 2018). Companies must comply by November 16, 2020, extended from the previous date of September 16, 2020.

Additional E-Commerce Barriers

Industry reports a number of inconsistencies, subjectivity, and lack of clarity regarding import processes that pose a barrier to shipping in the region. For example, valuation during import processes is highly inconsistent, even after declaring the value of goods and following official processes. Further, firms that wish to import products into Egypt must register, but are required to have a permanent establishment in the region to register. This largely restricts smaller e-commerce sellers from expanding in the market.[325]

P. France

Copyright Liability Regimes for Online Intermediaries

France proposed legislation in October 2019 intending to implement the EU Copyright Directive, through the ongoing audiovisual reform.[326] Previously, French officials indicated that filters would be required under implementing legislation.[327] The proposal does not even appear to reflect the text of the Directive, omitting mention of protection of exceptions and limitations, the principle of proportionality, or that the actions required by the liability standard cannot amount to a duty to monitor. Specifically, the proposal replaces the prohibition on removal of safeguards that allow users to rely on exceptions granted in Article 17(7) of the Directive.[328] Instead, there is only an obligation to inform users about relevant exceptions in terms and conditions.

Government-Imposed Content Restrictions and Related Access Barriers

In March 2019, the National Assembly proposed a very broad law on combating hate speech ("*Lutte contre la haine sur internet*").[329] The law would require designated Internet services to take down hateful comments reported by users within 24 hours. The law targeted any hateful attack on someone's "dignity" on the basis of race, religion, sexual orientation, gender identity, or disability. If platforms in scope do not comply, they could face an administrative penalty of 4 percent of their global revenue and penalties could reach tens of millions of euros.

---

[325] *Egypt: Legal Framework of E-Commerce Business in Egypt* (Aug. 29, 2022), https://www.mondaq.com/telecoms-mobile-cable-communications/1225322/legal-framework-of-e-commerce-business-in-egypt.

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

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

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

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

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.[330] The Court determined the legislation "undermines freedom of expression and communication in a way that is not appropriate, necessary and proportionate to the aim pursued" making the text not compatible with the French constitution. The French law required platforms to take down manifestly illegal content upon notification within 24 hours. Among others, the law targeted any hateful attack on someone's "dignity" on the basis of race, religion, sexual orientation, gender identity or disability.[331] The Court also struck down the one-hour removal deadline for terrorist propaganda and child pornographic content as it contradicts the French Penal code (Art 227-3 and 421-2-5).

Taxation of Digital Services

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.[332] The tax was applied retroactive to January 1, 2019, with the first pay date in November 2019. The tax is based on 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.[333] 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.[334] Based on French officials' own admission, the majority of firms that will pay the tax will be American.[335]

---

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

[331] *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/.

[332] 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"].

[333] *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.

[334] *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.]).

[335] 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

CCIA supports USTR's decision to pursue a Section 301 Investigation under the Trade Act of 1974 regarding the French DST. CCIA acknowledges the political compromise reached by the United States, Austria, France, Italy, Spain, and the United Kingdom regarding existing unilateral measures as they relate to implementation of the OECD/G20 Inclusive Framework.[336]

Data Localization

France first indicated that it will direct resources to build a national "trusted cloud" in 2019.[337] 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.[338]

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

ANSSI, the French cybersecurity authority, has adapted its cybersecurity certification and labeling initiative, SecNumCloud, to explicitly discriminate against non-French cloud providers.[340] Problematic requirements include "[t]he registered office, central administration or main establishment of the service provider must be established within a member state of the European Union"; a cap of 24% individual and 39% collective share ownership for non-EU entities; and no veto power for non-EU entities.[341] The certification standard is no longer

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.].

[336] Joint Statement from the United States, Austria, France, Italy, Spain, and the United Kingdom, Regarding a Compromise on a Transitional 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.

[337] 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.").

[338] *Id.*

[339] 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.

[340] ANSSI, L'Anssi Actualise Le Referntiel Secnumcloud, https://www.ssi.gouv.fr/actualite/lanssi-actualise-le-referentiel-secnumcloud/.

[341] See unofficial translation, *available at* https://www2.itif.org/2021-secnumcloud-3.2.a-english-version.pdf at article 19.6.

entirely voluntary or preferred—tenders have been published with SecNumCloud verification as a requirement.[342] The only companies that are verified under SecNumCloud are French.[343] The Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique de France (the Ministry of the Economy, Finance and Industrial and Digital Sovereignty of France) has suggested that it could mandate its own SecNumCloud scheme to the broader private sector by defining "sensitive data", and subsequently declaring when SecNumCloud would be required.[344] This effort at "data sovereignty" was defended by French policymakers as justified due to grievances over the U.S. CLOUD Act, which clarified the extraterritorial effect of some U.S. laws relating to criminal activity.[345]

Q. 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.[346] The NetzDG law mandates removal of "manifestly unlawful" content within 24 hours, and provides for penalties of up to 50 million euros.[347] 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"[348] have led to companies removing lawful content, erring on the side of caution in attempts to comply.[349] 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

---

[342] Available at https://ted.europa.eu/udl?uri=TED:NOTICE:399127-2022:TEXT:EN:HTML&tabId=0.

[343] ANSSI, Liste des produits et services qualifies (Oct. 4, 2022) https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf.

[344] Ministere de l'Economie Dest Finances et de la Souverainete Industrielle Et Numerique, Cloud : Cinq nouveaux dispositifs pour soutenir le developpement du secteur (Sept. 12, 2022), https://www.economie.gouv.fr/cloud-cinq-nouveaux-dispositifs-soutenir-developpement-secteur; Discours de Bruno Le Maire sur la stratégie nationale pour le Cloud, https://presse.economie.gouv.fr/download?id=99457&pn=116%20-Discours%20de%20Bruno%20Le%20Maire%20sur%20la%20strat%C3%A9gie%20nationale%20pour%20le%20Cloud.pdf.

[345] *France Wants Cyber Rule to Curb U.S. Access to EU Data*, POLITICO (Sept. 13, 2021), https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/.

[346] 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.

[347] Id. § 3(2).

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

[349] *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.

repeatedly raised concerns regarding the law's specificity and transparency requirements[350] and groups have expressed concerns about its threats to free expression.[351]

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.[352] Cases arising under this law will also have implications on extraterritoriality.[353]

In a 2020 review of the law, the German government has acknowledged flaws and needs for improvement.[354] In June 2020, there were further amendments proposed.[355]

Amendments to the law that require identifying and removing certain hate speech within 24 hours at risk of fines of up to 50 million Euros went into effect in February 2022, although parts of the amendments were paused for violating EU laws on civil liberties, while the fines for Google and Meta were stayed as well as well as their obligations.[356]

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".[357] In April 2022, the Franco-German-led GAIA-

---

[350] Thomas Escritt, *Germany Fines Facebook for Under-Reporting Complaints*, REUTERS (July 2, 2019), https://www.reuters.com/article/us-facebook-germany-fine/germany-fines-facebook-for-under-reporting-complaintsidUSKCN1TX1IC.

[351] *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.").

[352] 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/.

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

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

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

[356] *Big Tech Takes on Germany*, POLITICO (Feb. 2, 2022), https://www.politico.eu/article/big-tech-takes-on-germany-over-demands-to-forward-illegal-content-to-federal-police/; *Germany Administrative Court Holds New Online Hate Speech Regulation Violates EU Law*, JURIST (Mar. 2, 2022), https://www.jurist.org/news/2022/03/germany-administrative-court-holds-new-online-hate-speech-regulation-violates-eu-law/; *Germany: Administrative Court of Cologne Grants Google and Facebook Interim Relief; Holds Network Enforcement Act Partially Violates EU Law*, U.S. LIBRARY OF CONGRESS (Mar. 30, 2022), https://www.loc.gov/item/global-legal-monitor/2022-03-30/germany-administrative-court-of-cologne-grants-google-and-facebook-interim-relief-holds-network-enforcement-act-partially-violates-eu-law/.

[357] 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-

X cloud project published its own labeling scheme whose "level 3" assurance entails 'sovereignty' requirements similar to the upcoming EU certification scheme for cloud services, *i.e.*, data localization, non-EU ownership restrictions, employee location restrictions, etc.[358]

Asymmetry in Competition Frameworks

Germany has recently reformed its competition rules to target companies of "paramount significance for competition across markets", which came into force in January 2021.[359] The intention of this reform is to make it easier to sanction large digital companies, with provisions that effectively reverse the burden of proof for finding the abuse of a dominant position against companies deemed to be of "paramount significance", and eliminates the Higher Regional Court of Düsseldorf from the appeals process which otherwise normally applies to defendants.

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 in 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 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.

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.

[358] See criteria 54-61 under the "European control" section of Gaia-X labeling criteria, 21 April 2022 available on https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X-labelling-criteria-v22.04_Final.pdf

[359] Amendment of the German Act Against Restraints of Competition (Jan. 19, 2021), *https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html*

Since 2021 the German Competition Authority has already initiated proceedings and/or made a finding of "paramount significance" against Apple[360], Amazon[361], Google[362], and Meta[363]. It is reported that Microsoft is also under scrutiny.[364] Like the EU's Digital Markets Act, these rules will prohibit or otherwise reduce the ability of the targeted companies to engage in pro-competitive behaviour that their rivals otherwise enjoy. It appears that the targets of this competition law reform will be exclusively US companies.

R. Hong Kong

National Security Law and Local National Security Legislation (Article 23 of Basic Law)

The national security law was promulgated in Hong Kong in June 2020.[365] 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,[366] and the list of blocked websites under the law, though not officially confirmed by the Hong Kong authorities, appears to be increasing on national security grounds.[367] Hundreds of people have reportedly been arrested under the law,[368] as human rights experts have alerted world leaders to

[360] Available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/21_06_2021_Apple.html.

[361] Available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/06_07_2022_Amazon.html.

[362] Available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/05_01_2022_Google_19a.html.

[363] Available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/04_05_2022_Facebook_19a.html.

[364] Samuel Stolton, *Microsoft to face new antitrust scrutiny in Germany*, *Politico* (Aug. 11, 2022), https://www.politico.eu/article/microsoft-to-face-new-antitrust-scrutiny-in-germany/.

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

[366] *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.

[367] *As 'Great Firewall' Looms, Fears for Hong Kong's Free Internet*, ALJAZEERA (Feb. 17, 2022), https://www.aljazeera.com/economy/2022/2/17/as-great-firewall-looms-fears-for-hong-kongs-free-internet; *Hong Kong Rights Group Says Website Not Accessible Through Some Networks*, REUTERS (Feb. 15, 2022), https://www.reuters.com/world/china/hong-kong-rights-group-says-website-not-accessible-through-some-networks-2022-02-15/.

[368] *Hong Kong National Security Law; What Is It and Is It Worrying*?, BBC (June 28, 2022), https://www.bbc.com/news/world-asia-china-52765838; *Dismantling a Free Society*, HUMAN RIGHTS WATCH (2021), https://www.hrw.org/feature/2021/06/25/dismantling-free-society/hong-kong-one-year-after-national-security-law.

the harms of the law.[369] As noted elsewhere in these comments further, website blocks are barriers to maintaining a free and open internet which is critical to digital trade.

Industry is also concerned about the Hong Kong Government expressing that it has advanced efforts to develop local security legislation under Article 23 of the Basic Law to support the national security legislation passed in 2020. This effort could subsequently provide further basis for broader blocking of websites as well as other powers that could limit digital trade and foreign online services suppliers from operating in Hong Kong.

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".[370] The government began preparatory work on the bill in May 2022,[371] with a consultation expected to begin towards the end of the year.[372] Details on the specific entities to be designated as critical information infrastructure have yet to materialize, however due to prior suggestions that ISPs would be implicated, USTR should monitor developments to 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 US companies at a competitive disadvantage vis-à-vis their Chinese and Hong Kong competitors.

Cybercrime Legislation

Hong Kong's Cybercrime Subcommittee of the Law Reform Commission published a consultation paper on July 20, 2022, which issued initial proposals for "bespoke cybercrime" legislation.[373] The paper on Cyber-Dependent Crimes and Jurisdictional Issues outlined a proposal to render an act of knowingly making available or possessing a device or data that was made or adapted to commit a violation of law as a crime itself. As the legislation advances, electronic service providers should be clarified to not be determined as "making available or possessing a device or data" for the purposes of criminal or financial liability if such an act is due to the action of an individual using the service. Such clarifications would reduce the possibility the final set of rules could pose burdensome restrictions for online intermediaries and other digital services suppliers operating in Hong Kong.

[369] *Top Rights Experts Urge Repeal of Hong Kong's National Security Law,* UN News (July 27, 2022), https://news.un.org/en/story/2022/07/1123432.

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

[371] Cyber Security Legislation Proposed (May 25, 2022), https://www.news.gov.hk/eng/2022/05/20220525/20220525_125433_066.html.

[372] *Bill Strengthening Hong Kong's Cybersecurity Underway*, HONG KONG BUSINESS (2021), https://hongkongbusiness.hk/information-technology/news/bill-strengthening-hong-kongs-cybersecurity-underway.

[373] Press Release, Consultation Paper on Cyber-Dependent Crimes and Jurisdictional Issues published (with photo/video), https://www.info.gov.hk/gia/general/202207/20/P2022072000144.htm.

Privacy Law Anti-Doxxing Provisions

Hong Kong's privacy law—Personal Data (Privacy) (Amendment) Ordinance of 2021—entered into force on October 8, 2021, with anti-doxxing provisions that industry finds concerning.[374] The provisions empower the Office of the Privacy Commissioner for Personal Data of Hong Kong with the ability to demand that online platforms take down doxxing content, the definition of which could include blocks of entire websites or platforms. The application of these demands could extend beyond Hong Kong for content posted anywhere and foreign suppliers are expected to adhere to these demands regardless of where the content was posted. Insofar as these new rules could lead to the blocking of websites or platforms, the U.S. government should seek to ensure that U.S. business operations in Hong Kong are not hindered and that the makeup of the open and global Internet is not harmed through blocking-induced fractures.

S. 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.[375] The Indian Government has set ambitious goals for the country's digital future. However, the government has continued to pursue a digital agenda that undermines this growing potential while advancing harmful practices intimidating local employees of online platforms that hinder operations in the country as well as free expression. New regulations on data localization, protectionist policies that would mandate data access to competitors, and taxation plans ultimately hinder global trade flows.

Taxation of Digital Services

In March 2020, the Indian Parliament expanded the scope of India's existing "equalization levy" in its amended national 2020 Budget.[376] 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-

---

[374] Office of the Privacy Commissioner for Personal Data, Hong Kong, Media Statement, The Personal Data (Privacy) (Amendment) Ordinance 2021 Takes Effect Today to Criminalise Doxing Acts (Oct. 8, 2021), https://www.pcpd.org.hk/english/news_events/media_statements/press_20211008.html.

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

[376] *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.

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.[377]

The new equalization level 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" in 2018, but deferred implementation until there was international consensus on this question.

The Indian government has explicitly stated that the country will not stop enforcing their digital taxes until there is more clarity and assurance about the OECD global agreement and its impact.[378] The uncertainty of this status quo has resulted in U.S. digital firms continuing to pay the taxes.[379] This is despite the agreement struck between the U.S. and India in November 2021 for the Indian government to transition "from the existing India equalization levy to the new multilateral solution" and a commitment between the two parties to "working together through constructive dialogue on this matter."[380] The U.S. International Trade Commission included India's DSTs in its 2021 Year in Trade Report,[381] and CCIA urges USTR to continue to monitor developments on DSTs in India to ensure U.S. firms are not targeted for extractionary fees in this growing market.

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

---

[377] *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.

[378] *Equalisation Levy on Facebook, Amazon, May Go Only in 2-3 years*, THE ECONOMIC TIMES (Oct. 11, 2021), https://economictimes.indiatimes.com/tech/technology/equalisation-levy-on-facebook-amazon-google-may-go-only-in-2-3-years/articleshow/86926126.cms?from=mdr.

[379] *Big Tech Firms Play It Safe, Await Clarity Before Adjusting India Taxes*, THE ECONOMIC TIMES (Feb. 10, 2022), https://economictimes.indiatimes.com/tech/technology/big-tech-firms-play-it-safe-await-clarity-before-adjusting-india-taxes/articleshow/89463122.cms.

[380] Press Release, Treasury Announces Agreement on the Transition from Existing Indian Equalization Levy to New Multilateral Solution Agreed by the OECD-G20 Inclusive Framework (Nov. 24, 2021), https://home.treasury.gov/news/press-releases/jy0504.

[381] OFFICE OF THE U.S. INT'L TRADE COMMISSION, The Year in Trade 2021, https://www.usitc.gov/publications/332/pub5349.pdf at 204-205

domestic businesses.[382] 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.[383] 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), first introduced in December 2019, included concerning provisions that have remained throughout various drafts in the previous three years: 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).[384]

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

The Personal Data Protection Bill (PDP) was finally tabled on December 16, 2021,[385] after two years of review, with recommended changes that include a strict approach to data localization with the requirement that all data involving Indian citizens be kept within India's territorial

---

[382] 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.").

[383] *2020 CCIA NTE Comments.*

[384] 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.

[385] Report of the Joint Committee on Personal Data Protection Bill, 2019 https://www.ahlawatassociates.com/wp-content/uploads/2021/12/17-Joint-Committee-on-the-Personal-Data-Protection-Bill-2019.pdf. *See also What is India's Personal Data Protection Bill?*, REAL SECURITY (Apr. 7, 2022), https://www.real-sec.com/2022/04/what-is-indias-personal-data-protection-bill/.

limits.[386] Following the 93 recommendations to the PDP, the revised version of the Bill is known as the Data Protection Act, 2021.[387] The bill would implement a framework similar to that of the EU's GDPR by restricting data fiduciaries and processors conducting business in India to collect only necessary information, limiting reasons for data collection and processing, and ensuring consumer consent is provided for data usage. The key factors of the bill include: requirements that apply to personal and non-personal data, data fiduciary obligations, and the enforcement of data localization requirements.[388] The Indian government withdrew the bill briefly,[389] although it reportedly is expected to re-emerge.[390]

The back-and-forth of the bill's trajectory, the lack of transparency into the process over the past several years, and the lack of clarity over the provisions of the PDPB have created an uneasy regulatory environment for U.S. industry. The Indian government's process has drawn criticism from the Indian startup community.[391]

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."[392] 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.

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

---

[386] *Price of Protection*, INDIA BUSINESS LAW JOURNAL (June 7, 2022), https://law.asia/price-of-protection/.

[387] What You Should Know About India's Data Protection Bill 2021, https://securiti.ai/india-dpb/.

[388] *Non-Personal Data Likely to be Dropped From New Data Law*, HINDUSTAN TIMES (June 21, 2022), https://www.hindustantimes.com/india-news/nonpersonal-data-likely-to-dropped-from-new-data-law-101655752906037.html.

[389] Sameer Yasir & Karan Deep Singh, *India Withdraws a Proposed Law on Data Protection*, N.Y. TIMES (Aug. 4, 2022), https://www.nytimes.com/2022/08/04/business/india-data-privacy.html.

[390] *India Pivots to Online Regulation After Scrapping Personal Data Bill*, FT, https://www.ft.com/content/e8cb4554-4de5-4570-a0f7-c5f57cce5786).

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

[392] 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.

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.[393]

Continued Internet shutdowns have left widespread human rights impacts as well as economic losses—the U.S. International Trade Commission found that an estimated $549.4 million was lost in India due to repeated Internet shutdowns affecting Facebook, Instagram, YouTube, and Twitter between 2019-2021.[394] Facebook's services disruptor notes that its services were disrupted in India for a total of 3 months, 17 days, and 16 hours over the entirety of 2021 as the Indian government shut down the Internet frequently to hinder protests and dissent.[395] The Indian government conducted 106 Internet shutdowns in 2021, according to Access Now.[396]

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.[397] Earlier last year, amendments to the IT Act went into effect imposing additional requirements under the Intermediary Rules and imposing new obligations on intermediaries.[398] These included strict timelines for takedown requests and impose significant penalties for noncompliance. These laws also include localization requirements, and traceability requirements which pose greater security risks. The amendments replaced the 2011 Information Technology (Intermediary Guidelines) Rules and introduced new obligations on online intermediaries. Generally, The Rules (1) set out additional requirements for intermediaries. On the Intermediary Guidelines, it appears that the same issues we identified in the 2018 consultation remain in the final version including the 72 hour and 24 hour shot clocks, traceability mandate, and localization requirements. Further, there are additional requirements on larger intermediaries. Intermediaries must remove content within 24 hours upon receipt of a court order or Government notification and deploy tools to proactively identify and remove unlawful content (Amendment 9, Amendment 8, and Amendment 3(5)). There are also concerning law enforcement assistance provisions, including a requirement for intermediaries to "enable tracing out of such originators of information on its platform" at the request of government officials (Amendment 3(5)), and local incorporation and local presence requirements (Amendment 7). While there was a public consultation on the proposed changes in 2018, there was limited opportunity for industry and

[393] *Twitter Says It's Concerned with India Intimidation, Requests 3 More Months to Comply with New IT Rules*, TECHCRUNCH (May 21, 2021), https://techcrunch.com/2021/05/27/twitter-says-concerned-with-india-intimidation-requests-3-more-months-to-comply-with-new-it-rules/.

[394] USITC, Foreign Censorship Part 2, *supra* note 32.

[395] Meta, Internet Disruption, https://transparency.fb.com/data/internet-disruptions/ (last visited Oct. 28, 2022).

[396] Access Now, (2022) https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf.

[397] India: An Update On India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (May 21, 2021), http://blog.galalaw.com/post/102gzas/an-update-on-indias-information-technology-intermediary-guidelines-and-digital.

[398] The Indian Government Press Release is available at [fix link], and the full text is available at [fix link].

other stakeholders to provide input as the draft amendments and new obligations developed or sufficient notification of these rules.[399]

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.[400] 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. Additionally, industry representatives report the use of harassment and intimidation tactics through the IT Law to impose restrictions on freedom of expression in the country and coerce preferred behavior from online platforms, representing one of the battlefronts of the growing—and concerning—global trend of employee intimidation.[401]

Further, on June 6, 2022, India re-issued proposed content moderation restrictions and rules for social media service providers through its draft changes to its 2021 IT Law.[402] The proposed law would establish a government body to oversee content moderation policies due to the "need" for companies to "respect the rights accorded to the citizens under the constitution of India." This authority, to be dubbed the Grievance Appellate Committee and reportedly include a government official on the panel, would have outsized influence on what can and cannot be posted on social media in India.[403] On October 28, 2022, the Ministry of Electronics and Information Technology released the final version of the amendment, which stipulated that the panel would have the ability to hear complaints from users regarding social media providers' content moderation decisions and reverse such decisions of platforms.[404] The panel is set to be established within three months of the release of the rules, which require social media providers to acknowledge user complaints within 24 hours and address users' requests within 15 days—further, if the request seeks the removal of content, the social media provider would be obligated to address that complaint within 72 hours. The proposed measure comes amidst a brewing fight between

[399] CCIA 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

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

[401] *'Hostage-Taking Laws' Seem to Be Fuelling a Twitter Crackdown in India*, REST OF WORLD (July 1, 2022), https://restofworld.org/2022/twitters-censorship-india/.

[402] Ministry of Electronics and IT (MeiTY), Press Note (June 6, 2022), https://www.meity.gov.in/writereaddata/files/Press%20Note%20dated%206%20June%2022%20and%20Proposed%20draft%20amendment%20to%20IT%20Rules%202021.pdf.

[403] *One Government Nominee, Independent Experts Likely on Grievance Appellate Panel for Social Media*, TIMES OF INDIA (Aug. 24, 2022), https://timesofindia.indiatimes.com/india/one-government-nominee-independent-experts-likely-on-grievance-appellate-panel-for-social-media/articleshow/93759424.cms; *India's Tech Regulations Onslaught Poses Dilemma For U.S. Companies*, WALL ST. J. (Oct. 4, 2022), https://www.wsj.com/articles/indias-tech-regulation-onslaught-poses-dilemma-for-u-s-companies-11664885649.

[404] Ministry of Electronics and Information Technology, India, Notification, October 28, 2022, available at https://egazette.nic.in/WriteReadData/2022/239919.pdf.

the government, digital firms, and rights advocates regarding policing of online content due to arrests over posts and a government effort to take down or block posts.[405]

These conditions both restrict political, ethnic, and personal expression while simultaneously hindering U.S. firms' access to the Indian market. Reports from online content providers reflect the chilling effect of the 2021 IT Law on business and the ability of consumers to use these services. WhatsApp reported millions of accounts were banned each month in 2021 under the law, with the number topping 2 million in most months.[406] From just July to December 2021, Twitter reported receiving requests for information for 7,800 accounts and requests for removal related to 12,900 accounts.[407] Google data shows that requests for information and removal in India have increased over time, with a notable spike between June and December 2021.[408]

Draft Telecommunications Bill

In September 2022, the Department of Telecommunications released the Draft Indian Telecommunication Bill, which updates and aggregates the Indian Telegraph Act of 1885, the Indian Wireless Telegraphy Act of 1933, and the Telegraph Wires (Unlawful Protection) Act of 1950.[409] The bill redefines "telecommunications services" as "service of any description (including broadcasting services, electronic mail, voice mail, voice, video and data communication services, audiotex services, videotex services, fixed and mobile services, internet and broadband services, satellite based communication services, internet based communication services, in-flight and maritime connectivity services, interpersonal communications services, machine to machine communication services, over-the-top (OTT) communication services) which is made available to users by telecommunication, and includes any other service that the Central Government may notify to be telecommunication services." Telecommunications services providers would then be effectively required to gain a license from the central government for "providing telecommunication services or establishing, operating, maintaining and expanding telecommunications networks."

The provision of licenses would then entail a host of conditions for online services providers including paying into the country's Telecommunication Development Fund, one of the functions of which is to deploy broadband services. Licensed firms would then be obligated to "unequivocally identify" individuals to whom it provides services. The government would give itself the power to intercept communications, demand the disclosure of communications, mandate standards for services, and seize the services from licensed telecommunications services

---

[405] *See Indian Journalist Arrested Over Twitter Post*, FT (2021), https://www.ft.com/content/f2c729b7-c98c-4c1e-9f5e-37b8c81ad393; *Twitter, Challenging Orders to Remove Content, Sues India's Government*, N.Y. TIMES (July 5, 2022), https://www.nytimes.com/2022/07/05/business/twitter-india-lawsuit.html.

[406] WhatsApp, Monthly India Reports https://www.whatsapp.com/legal/india-monthly-reports/?lang=en (last visited Oct. 28, 2022).

[407] Twitter, Transparency Country Reports: India, https://transparency.twitter.com/en/reports/countries/in.html (last visited Oct. 28, 2022).

[408] Google, Transparency Reports, https://transparencyreport.google.com/government-removals/government-requests/IN (last visited Oct. 28, 2022).

[409] Draft Indian Telecommunication Bill, 2022. https://dot.gov.in/sites/default/files/Draft%20Indian%20Telecommunication%20Bill%2C%202022.pdf ; https://dot.gov.in/relatedlinks/indian-telecommunication-bill-2022.

to government authorities as well as require the suspension of classes of communications if the action is deemed necessary to protect the "sovereignty, integrity or security of India, friendly relations with foreign states, public order, or preventing incitement to an offence". The bill includes must-carry obligations through requirements for "press messages intended to be published in India or correspondents accredited to the Central Government or a State Government" for telecommunications services. The legislation would include a troubling move of authority away from the traditional regulator, TRAI, to a central government authority.[410] The lack of clarity in the authority the Indian government grants itself in this bill could endanger Internet freedom and the security of services. Depending on how the bill is implemented and enforced, the legislation could contravene India's WTO commitments under the GATS.

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.[411] 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.[412]

India's Ministry of Consumer Affairs released proposed e-commerce rules in June 2021, although final rules are still to be determined as the process has stagnated.[413] The rules also impose obligations on all e-commerce entities without regard to unique e-commerce models and inter se 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 is connected with protection against unfair trade practices by e-commerce entities, and creates an arbitrary and

---

[410] *Crossed Wires: Editorial on Implications of Modi Government's Draft Telecom Bill 2022*, TELEGRAPH INDIA (Sept. 26, 2022), https://www.telegraphindia.com/opinion/crossed-wires-editorial-on-implications-of-modi-governments-draft-telecom-bill-2022/cid/1888772.

[411] 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.

[412] 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).

[413] No.J-10/3/2018-CPU (Computer No:16082), https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Comments_eCommerce_Rules2020.pdf. See also India Proposes Tougher E-Commerce Rules to Address 'Widespread Cheating' Complaints, Tech Crunch (June 21, 2021), https://techcrunch.com/2021/06/21/india-proposes-tougher-e-commerce-rules-following-widespread-cheating-and-unfair-trade-by-amazon-and-flipkart/

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.[414] 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 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. The Indian government has mandated compliance to these guidelines.[415]

Regulations on Cloud 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% and a Class 2 Supplier is 20%. Up to this date, 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 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.

In April 2022, India began to tighten its restrictions on cloud services providers and virtual private network (VPN) providers through extremely invasive Indian Computer Emergency Response Team requirements for cloud service and VPN providers to collect the personal information—including customers' names and IP addresses. VPN, cloud, and several other IT services providers would be required to log their customers' activity and surrender that information to Indian authorities when demanded. Firms that decline to undergo this broad-sweeping surveillance on their users would have to leave India's prominent market.[416] After pressure, the Indian government agreed in June to delay the rules for three months,[417] but VPN

[414] Guidelines for Acquiring and Producing Geospatial Data and Geospatial Data Services Including Maps, https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data.pdf.

[415] *India's Push for Home Grown Navigation System Jolts Smartphone Giants*, REUTERS (Sept. 26, 2022), https://www.reuters.com/technology/exclusive-indias-push-home-grown-navigation-system-jolts-smartphone-giants-2022-09-26/

[416] FAQs on Cybersecurity Directions (May 2022), https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf. *See also VPN Providers Threaten to Quit India Over New Data Law*, WIRED (May 5, 2022), https://www.wired.com/story/india-vpn-data-law/.

[417] Manish Singh, *India Delays VPN Rules to Log Customer Data By 3 Months*, TechCrunch (June 28, 2022), https://techcrunch.com/2022/06/27/india-delays-strict-new-vpn-rules-by-3-months/; Access Now, Letter to Government of India, June 27, 2022, https://www.accessnow.org/cms/assets/uploads/2022/06/Cybersec-Experts-CERT-In-Directions-Statement.pdf.

operators have already left the market due to the regulatory uncertainty and impending invasive oversight, undermining digital security and services exports to the country.[418]

T. 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 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.[419] Companies determined to have a significant economic presence will be declared permanent establishments and as a result subject to domestic tax regulations.[420] 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.[421] 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.[422] Governments should be discouraged from pursuing discriminatory taxes on foreign companies to fund economic response measures.[423]

As of time of filing, implementation details are still uncertain, even as Indonesia officials have stated that they would align politics with the OECD consensus reached in October 2021. A new VAT on digital goods and services went into effect on April 1, 2022.[424] The VAT will be collected on all goods and services that are taxable and delivered to Indonesia via electronic systems at a rate of 11% (which will rise to 12% starting in 2025).[425] U.S. trade officials should continue to monitor developments.

---

[418] Center for Democracy & Technology, *India's New Cybersecurity Order Drives VPN Providers to Leave* (June 24, 2022), https://cdt.org/insights/indias-new-cybersecurity-order-drives-vpn-providers-to-leave-chilling-speech-and-subjecting-more-indians-to-government-surveillance/.

[419] *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.

[420] *Id.*

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

[422] *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.

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

[424] Text available at https://jdih.kemenkeu.go.id/download/1bfe41fc-a312-41f0-b107-70e55b69767a/60~PMK.03~2022Per.pdf. *See also Indonesia Revises Regulations for VAT on Digital Goods and Services*, ORBITAX (May 12, 2022), https://www.orbitax.com/news/archive.php/Indonesia-Revises-Regulations--49820.

[425] Yvonne Beh *et al*., *Indirect Tax Developments in Asia-Spotlight on the Digital Economy*, BLOOMBERG TAX (Sept. 6, 2022), https://news.bloombergtax.com/daily-tax-report-international/indirect-tax-developments-in-asia-spotlight-on-the-digital-economy.

Customs Duties on Electronic Transmissions

Indonesia issued Regulation No.17/PMK.010/2018 (Regulation 17) in 2018.[426] 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[427] and most recently reaffirmed in June 2022.[428] Left unchecked, Indonesia's actions will set a dangerous precedent and may encourage other countries to violate the WTO moratorium. This is especially critical as members at the WTO continue discussions on e-commerce, and as the renewal for the moratorium comes up during the 13th WTO Ministerial Conference, likely to be held in early 2023. This is particularly concerning as despite the late-struck deal at WTO MC12 to renew the moratorium, Indonesia's actions were cited several times by India and South Africa in materials seeking the end of the moratorium.[429] As such, the continuance of this policy endangers the future of the WTO agreement. 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.[430] 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. Further, different ministries interpret the landing points differently, and industry reports a lack of clarity over the process to propose new corridors. 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, creates significant business uncertainty, and serves as a hindrance to U.S. economic interests.[431]

---

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

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

[428] *WTO Members Secure Unprecedented Package of Trade Outcomes at MC12* (June 17, 2022).

[429] Work Programme on Electronic Commerce, Communication of India and South Africa, Nov. 8, 2021, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/GC/W833.pdf&Open=True

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

[431] CSIS, Securing Asia's Subsea Network: U.S. Interests and Strategic Option (Apr. 5, 2022) https://www.csis.org/analysis/securing-asias-subsea-network-us-interests-and-strategic-options ("One very rough, back-of-the-envelope method is to consider the size of the U.S. digital economy, which hinges on internet traffic, and the percentages of traffic that are routed internationally and carried by subsea cables. Doing so estimates the contribution of subsea cables to the U.S. economy at nearly $649 billion in 2019, or about 3 percent of U.S. GDP. Of that total, U.S. traffic routed through Asia is responsible for roughly $169 billion. Another telling indicator, depicted in Figure 1, examined further in this section, is the contribution of U.S. digital exports, which rely on subsea cables and totaled $520 billion in 2020.").

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 that has been operational for five years and completed 100 percent of construction commitments for the first five years, (2) the local partner to be part of the consortium, (3) a minimum of 5% 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 / Regulation on Private Electronic System Providers

The ICT Ministry issued Ministerial Regulation 5/2020 on private electronic systems providers ("ESP"s)—the definition of which includes practically every Internet website or Internet-enabled service—in December 2020.[432] 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.

The process for registering and subsequent punishment for failing to do so is excessively opaque and difficult to understand, and the procedure behind when the law would be enforced lacked transparency—The law stated that ESPs would be given 6 months of transition time to register in Indonesia's database. However, although some assumed that could mean May 2021, Kominfo never provided any guidance until June 14, when the government sent around a "Circular Letter" that stated that the six month grace period started on Jan. 21, 2022, and that therefore the ESPs had to comply by July 20, 2022.[433] Effectively, the government announced in June 2022 that the regulations had been in effect for five months at that point, unbeknownst to industry players, and that firms had a little over a month to comply with the law. The regulatory uncertainty led to several major U.S., French, and Japanese companies failing to register and being blocked in Indonesia, such as Yahoo, PayPal, Valve, Nintendo, Ubisoft, and others, although several of these companies were eventually unblocked.[434]

---

[432] *See Indonesia Regulator Set Clearer Terms for Internet Platforms (Domestic and Foreign)*, HOGAN LOVELLS (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; Afriyan Rachmad & Louise Patricia Esmeralda, *Indonesia's New Regulation on Private Electronic System Operators: Important Notes for Corporate Compliance of Domestic and Foreign Information Technology Companies*, ZICO LAW (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/.

[433] Available at https://jdih.kominfo.go.id/produk_hukum/view/id/804/t/surat+edaran+menteri+komunikasi+dan+informatika+nomor+3+tahun+2022. See also *Indonesia: Deadline for Registration of Electronic System Operators Now Set for 20 July 2022*, GLOBAL COMPLIANCE NEWS (July 5, 2022), https://www.globalcompliancenews.com/2022/07/05/indonesia-deadline-for-registration-of-electronic-system-operators-is-now-set-for-20-july-2022-01072022/.

[434] *Indonesia Block Yahoo, Paypal, Gaming Websites Over Licence Breaches*, REUTERS (Aug. 1, 2022), https://www.reuters.com/technology/indonesia-blocks-yahoo-paypal-gaming-websites-over-licence-breaches-2022-07-30/.

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.[435]

Particularly given the tumultuous beginning of the law, CCIA urges USTR to continue to monitor the implementation of these regulations to ensure they do not further restrict the ability of online services to operate in the country through unreasonable blocking or otherwise punishing services for hosting certain lawful content that adhere to platforms' terms of services.

Elsewhere, Indonesia's excessive content takedown requests and Internet shutdowns bring monetary harm for U.S. firms and implicate broader concerns of freedom of expression online. The government shut down the Internet in Indonesia twice in 2021 according to Access Now,[436] while Meta reported services disruptions for 14 days across the same period.[437] The USITC estimated $82.2 million in economic losses in Indonesia due to the shutdown of the Internet in 2019 affecting Facebook, Instagram, YouTube, and Twitter between 2019-2021.

The phenomenon of content restrictions appears to be skyrocketing—between July and December 2021 alone, Meta reported that in Indonesia, the company restricted access to "3,377 items reported by the Ministry of Communication and Information Technology (KOMINFO) for allegedly violating local laws."[438] That represented an increase from 634 between January and July of 2021 and a mere 130 in the period between July and December 2020. Industry continues to be concerned about this trend and urges the U.S. trade agencies to remain vigilant, particularly as a March 2022 report suggested that the Indonesian government was preparing strict rules for internet and social media firms to quickly remove "unlawful" content within four hours if a request were to be designated as "urgent" and other take down demands, such as those from government agencies, would require action within 24 hours.[439] The rules have yet to be introduced, but CCIA urges USTR to monitor developments—if any materialize—on this issue, given the speed with which the rules could be introduced and declared in effect.

---

[435] Joint Civil Society Letter, May 31, 2021, https://www.article19.org/resources/indonesia-repeal-ministerial-regulation-5/; https://www.eff.org/deeplinks/2021/02/indonesias-proposed-online-intermediary-regulation-may-be-most-repressive-yet ("MR5 empowers an official with the Orwellian title "Minister for Access Blocking" to coordinate the prohibited information that will be blocked. Blocking requests may originate with Indonesian law enforcement agencies, courts, the Ministry of Information, or concerned members of the public… If a Private ESO (with the exception of a cloud provider) does not comply, it may receive warnings, fines, and eventually have its services blocked in Indonesia—even if the prohibited information was legal under international human rights law.")

[436] Keep It On, The Return of Digital Authoritarianism: Internet Shutdowns in 2021, https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf.

[437] Meta, Transparency Center, Internet Disruptions, https://transparency.fb.com/data/internet-disruptions/ (last visited Oct. 28, 2022).

[438] Meta, Transparency Center, Indonesia Country Report, https://transparency.fb.com/data/content-restrictions/country/ID/ (last visited Oct. 28, 2022).

[439] *Indonesia Preparing Touch New Curbs for Online Platforms*, REUTERS (Mar. 23, 2022), https://www.reuters.com/world/asia-pacific/exclusive-indonesia-preparing-tough-new-curbs-online-platforms-sources-2022-03-23/

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,[440] storing and processing of data offshore by any "Electronic Systems Providers (ESPs)" will require prior approval from the government.[441] These requirements present market access barriers for foreign services when delivering products and services online.

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

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. [442] 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.

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

[441] *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.

[442] *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

Personal Data Protection Bill

On September 20, 2022, Indonesia's Parliament ratified its Personal Data Protection bill which differentiates the responsibilities between data controllers and data processors, drawing from the EU's GDPR.[443] Data transfer across borders is limited to countries which have equivalent standards of data protection, however there are no guidelines on assessing the level of data protection across countries, which are set to be the subject of further regulations to dictate the implementation of cross-border data transfers.[444] However, as currently established, the new law does not obligate notification to the Ministry of Communications and Informatics (MOCI) before and after any cross-border data transfer—CCIA urges USTR to monitor the implementation and future regulations on this matter to ensure the principles of data free flows are respected under Indonesian law.[445] The bill would also impose extraterritoriality as its cross-jurisdictional basis, again similar to GDPR, and applies to any entity located either in Indonesia and/or outside Indonesian but either has legal impact for Indonesia and/or Indonesian citizens located outside of the country.[446]

E-Commerce Regulation

Indonesia's Government Regulation No. 80/2019 on E-Commerce distinguishes between domestic and foreign e-commerce business actors, and also prohibits personal data from being sent offshore unless otherwise approved by the Ministry of Trade.[447] 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.

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.[448]

---

[443] *Indonesia Enacts its First Data Protection Act*, LEXOLOGY (Sept. 23, 2022), https://www.lexology.com/library/detail.aspx?g=ca80b3ee-012c-40e4-bf31-c82f3d97db67.

[444] *Indonesia's New Personal Data Protection Law*, LEXOLOGY (Sept. 30, 2022), https://www.lexology.com/library/detail.aspx?g=31320d3a-2e25-4a03-97e3-f58f641c8e3c.

[445] *Indonesia Passes Historic Personal Data Protection Bill*, LEXOLOGY (Sept. 26, 2022), https://www.lexology.com/library/detail.aspx?g=e91959fe-01aa-4285-ab9d-e37a867dbd19.

[446] *Id*.

[447] *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.

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

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

U.S. firms face additional barriers in Indonesia through the country's restrictions on foreign direct investment for e-commerce services. Foreign firms cannot directly retail many products through electronic services. Ownership for physical distribution, warehousing, and further logistics is limited to 67 percent, provided that each of these services is not ancillary to the main business line. Legislation is scheduled to take effect in November 2020 that aims to add clarity for e-commerce firms.[449]

Indonesia's Ministry of Industry issued regulation No. 22/2020 (IR22) on the Calculation of Local Content Requirements (LCR) for Electronics and Telematics. Industry reports that the regulation is motivated by the government's target to achieve 35 percent import substitution by 2025, which will force U.S. companies to use local manufacturing partners. IR22 provides specific and extensive requirements for manufacturing and development for both digital and non-digital physical products. The policy will have an additional administrative burden to physical ICT products that are needed for ICT companies to operate in Indonesia. This regulation could lead to an importation threshold for ICT equipment. Industry reports that the government has also signaled intention to build on this LCR requirement and add similar LCRs for software and applications, which will become a primary blocker for digital platform companies that provide services over the internet. The Government plans to introduce a draft by end of 2020.

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

U. Italy

Taxation of Digital Services

Italy's 2020 Budget introduced a 3 percent digital services tax closely aligned with the EU's original proposal.[450] 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".[451]

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.[452] 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, and struck a deal with the U.S.[453] However, U.S. officials should work closely with countries that have enacted a DST to remove the discriminatory tax as soon as possible.

Ex-ante Platform Regulation

On August 27, 2022, Law No. 118, the "2021 Annual Competition Law," went into effect.[454] The law presumes economic dependence—which entities can challenge—for firms that offer intermediation services on digital platforms that facilitate end users or suppliers.[455] Examples of abusive behavior in the law include: providing inadequate information about the service offered regarding scope or quality, mandating obligations that are unreasonable based on the type or content of the service, and limiting competitive providers ability to offer the same service, such

---

[450] 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.

[451] *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).

[452] *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.

[453] 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.

[454] Available at: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2022;118. *See also The Italian Parliament Approves Competition Law Reform*, CLEARY ANTITRUST WATCH (Aug. 16, 2022), https://www.clearyantitrustwatch.com/2022/08/the-italian-parliament-approves-competition-law-reform/.

[455] *Entry Into Force of Italy's Annual Law for Competition*, JD SUPRA (Aug. 26, 2022), https://www.jdsupra.com/legalnews/entry-into-force-of-italy-s-annual-law-9761724/.

as through the enforcement of unilateral conditions or added fees.[456] The Italian Competition Authority will have the power to demand information from digital platforms even when the regulator has not yet launched a formal proceeding.[457]

Implementation of the EU Audiovisual Services Directive

Italy is implementing the 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. The implementation of the AVMS-D in Italy went into effect on March 1, 2022.[458] The quotas remained, with a slight reduction in the quota to 20 percent following 2024, which still reflects an excessively high bar.[459]

V. Japan

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

The Japanese Ministry of Communications (MIC) expanded the application of the Telecommunications Business Act (TBA) to foreign services suppliers in 2021.[460] This change mandates that foreign over-the-top (OTT) services—which could encapsulate search, digital advertising, and other services that facilitate communications—that use third-party facilities to (1) provide notification and register as a local service provider with a local representative, and (2) observe obligations under its Telecommunications Business Act. MIC amended the TBA in 2022, which included privacy and data protection obligations for large platform providers and to apply third-party data transfer information—such as the usage of third-party cookies—to all products.

---

[456] *Id*.

[457] *Italian Competition Authority: New Powers to Address Concentrations and Conduct by Digital Platforms*, LEXOLOGY (Oct. 3, 2022), https://www.lexology.com/library/detail.aspx?g=0ec45801-9877-46e8-96bd-e85120fb7bef.

[458] *Italy Transposes DSM Copyright Directive and AVMS Directive*, MERLIN (2022), https://merlin.obs.coe.int/article/9359.

[459] *Focus: Transposition of the Revised AVMSD*, PORTOLANO CAVALLO (Feb. 21, 2022), https://portolano.it/en/newsletter/portolano-cavallo-inform-digital-ip/focus-transposition-of-the-revised-avmsd ("17% of the annual net revenue in Italy; from 1 January 2023: 18% of the annual net revenue in Italy; from 1 January 2024: 20% of the annual net revenue in Italy").

[460] *Japan's Efforts to Strengthen the Effectiveness of Enforcement Against Foreign Telecommunications Operators*, JD SUPRA (May 7, 2021), https://www.jdsupra.com/legalnews/japan-s-efforts-to-strengthen-the-8593184/

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.[461] The amendments include increased data breach reporting thresholds, stricter data transfer requirements, new standards on pseudonymized personal information similar to the GDPR, and increased data subject access rights with extraterritorial enforcement options. The new cross-border data transfer requirements introduced now require either an individual's opt-in consent prior to the transfer of personal information outside of Japan or an established personal information protection framework with the party receiving the information outside of Japan.[462] The APPI requires a review of the policy once every three years—therefore, the discussion of revisions are expected to commence in 2023.

Discriminatory Platform Regulation

Following various reports and consultation CCIA has cited in previous NTE submissions,[463] the Headquarters for Digital Market Competition released its final report in 2021 on "Competition in the Digital Advertising Market."

In May 2021, the Japanese Consumer Affairs Agency (CAA) enacted "Act on the Protection of the Interests of Consumers Using Transaction Digital Platforms".[464] 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.

On April 26, 2022, the Japan Digital Market Competition Headquarters (DMCH) released interim reports on *Evaluation of Competition in the Mobile Ecosystem* and *New Customer Contacts (Voice Assistants and Wearables).*[465] In these interim reports, the DMCH proposed several new avenues for *ex ante* digital platform regulation in mobile apps and voice assistants and wearables that could disproportionately harm U.S. digital firms without accounting for the broader market dynamics that implicate local and foreign firms, if the regulations fail to incorporate a robust market analysis and pursue heavy-handed *ex ante* restrictions on certain companies. Problematic proposals and explorations made in the interim reports include forcing digital platforms to share data with third parties and to provide third parties access to data (such as click-and-query search data); restrictions on platforms using data across services; undermining intellectual property by imposing obligatory sharing of trade secrets and copyright; and overly

[461] Available at: https://www.ppc.go.jp/en/legal/.

[462] *Amended Japanese Privacy Law Creates New Categories of Regulated Personal Information and Cross-Border Transfer Requirements*, JD SUPRA (Mar. 15, 2022), https://www.jdsupra.com/legalnews/amended-japanese-privacy-law-creates-7847421/.

[463] CCIA 2020 NTE Comments

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

[465] Interim Reports on Evaluation of Competition in the Mobile Ecosystem and New Customer Contacts (Voice Assistants and Wearables) (Apr. 26, 2022), Japan Digital Market Competition Headquarters, https://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai6/index.html.

relying on similar actions taken in other jurisdictions that have yet to be genuinely tried and tested.[466]

On July 5, 2022, the Ministry of Economy, Trade and Industry released a Cabinet Order which stipulated that the digital advertising sector would be regulated under the 2020 Act on Improving Transparency and Fairness of Digital Platforms.[467] Platforms that use advertisers' ads on their websites—such as search engines, portal sites, and social networking services, through primarily auctions—would be designated under this new policy if they sell at least 100 billion yen (roughly $691.4 million) each fiscal year in Japan. Platforms that are interlocutors between advertisers and website operators through primarily auctions would be designated if they sell at least 50 billion yen (roughly $345.7 million) each fiscal year in Japan. The new rules could be used to target U.S. digital platforms that engage in advertising in conducting business, as the Final Report on the Evaluation of Competition in the Digital Advertising Market by the Digital Market Competition Council—which set the foundation for these new rules—identified only Google, Facebook, and Yahoo! in its analysis of the market.[468] As the rules are implemented, it will be crucial to monitor the extent to which METI oversight becomes overly intrusive and whether it targets U.S. companies. Industry reports concern that METI will require providers of platforms to undergo unnecessary administrative procedures such as information not pertinent to the law and seeks adherence to good regulatory practices in light of Article 3 of the Transparency Act which states that the "involvement of the State and other regulations shall be kept to the minimum necessary."

Copyright Policy

In 2020, Japan made revisions to 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 that [the use] does not unduly harm the interests of the copyright holder."[469] The changes took effect on January 1, 2021.

[466] Comments of CCIA to DMCH on Interim Reports (2022), https://www.ccianet.org/wp-content/uploads/2022/06/CCIA-Comments-on-the-Japan-DMCHs-Interim-Reports.pdf.

[467] METI. Cabinet Decision on Improving Transparency and Fairness of Digital Platforms, https://www.meti.go.jp/english/press/2022/0705_001.html

[468] Evaluation of Competition in the Digital Advertising Market Final Report: Summary (Apr. 27, 2021), https://www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_210427.pdf at 2.

[469] *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/.

W. 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".[470] 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 the purpose of "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 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 US companies operating in Kenya.

Taxation of Digital Services

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. Kenya has still not endorsed the OECD Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy.[471]

[470] *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/.

[471] David Herbling, *OECD Urges Kenya to Drop Plan to Double Tax Digital Services*, Bloomberg (Apr. 14, 2022), https://www.bloomberg.com/news/articles/2022-04-14/oecd-urges-kenya-to-drop-plan-to-double-digital-services-tax; Kenya Enacts Finance Act, 2022, EY, https://www.ey.com/en_gl/tax-alerts/kenya-enacts-finance-act--2022.

X. 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.[472] 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

Seven proposals have been made by the Korean National Assembly to mandate "network use fee" payments by certain content providers over the past year and a half. This is at times justified by an argument that network fees will 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 and application providers.[473] This follows years of conflict among U.S. content providers operating in the region and local telecommunication providers.[474] These proposals have been consolidated into the seventh piece of legislation on this matter, introduced by Rep. Young-chan Yoon, called the "Netflix Free Ride Prevention Act" on September 8, 2022.[475] The legislation would effectively mandate foreign content access providers—namely U.S. firms such as Google, Facebook, and Netflix—to enter into paid contracts with Internet service providers for the content demanded by ISPs' customers. The bill would directly undermine long-standing global norms and procedures that serve as the foundation of the Internet ecosystem and would likely violate Korea's trade obligations to the U.S. by targeting U.S. content providers and

[472] 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.

[473] Kyung Sin Park & Michael Nelson, *Afterword: Korea's Challenge to the Standard Internet Interconnection*, Carnegie Endowment for Int'l Peace (Aug. 17, 2021),

[474] *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/.

[475] *See* https://blog.naver.com/yyc8361/222870020115.

requiring contracts and extractionary fees for any company meeting arbitrary data transfer thresholds.[476]

The incumbent ISPs, three of which together hold a market share of over 90% for Internet access services, have long argued these fees are necessary to keep up with the increasing demand for traffic. However, a more effective avenue—that would not involve discriminatory fees on U.S. firms to subsidize local incumbents—would be to encourage content access providers (CAPs) to voluntarily negotiate with ISPs and install temporary storage facilities in the country to bring content closer to consumers to reduce international bandwidth costs for ISPs and improve quality for users. These practices and negotiations, leading to settlement-free peering, are a norm globally. However, Korean ISPs—and in turn, legislators—have rejected this tried and tested method, instead opting to rent-seek from content providers. This trend began in 2016, when Korean ISPs succeeded in bringing about legislation instituting inter-ISP Internet traffic payments and incentivizing them to impose similar network usage fees on Korean online services suppliers such as Korean search, video, gaming and communications applications. Now, Korean ISPs believe they are experiencing "reverse discrimination" because foreign firms have the option of exchanging traffic outside of Korea (depriving them of similar revenue they have succeeded in extracting from domestic suppliers). However, the policy of network usage fees has been found to be demonstrably bad for both content providers and consumers, undermining the argument of the original legislation as well as this new effort to target U.S. companies.[477]

The legislation would put South Korea in danger of violating several provisions of their Free Trade Agreement with the United States, including KORUS Article 14.2 (Access and Use); KORUS Article 14.5 (Competitive Safeguards); and KORUS Article 15.7.[478]

CCIA has appreciated the engagement of USTR and the Department of Commerce on this issue in the past and encourages continued vigilance as this legislation advances. As the United States and Korea seek continued engagement through initiatives such as the Indo-Pacific Economic Framework, ensuring digital services are not subject to discriminatory treatment is of paramount interest to the U.S. tech industry.

---

[476] *New Korean Legislation Undermines Internet Norms and Raises Broad Trade Concerns*, DISRUPTIVE COMPETITION PROJECT (Sept. 19, 2022), https://www.project-disco.org/21st-century-trade/091922-new-korean-legislation-undermines-internet-norms-and-raises-broad-trade-concerns/; INTERNET SOCIETY, *Old Rules in New Regulations – Why 'Sender Pays' Is a Direct Thread to the Internet* (May 26, 2022), https://www.internetsociety.org/blog/2022/05/old-rules-in-new-regulations-why-sender-pays-is-a-direct-threat-to-the-internet/.

[477] INTERNET SOCIETY, *Sender Pays: What Lessons European Policy Makers Should Take from the Case of South Korea* (Sept. 30, 2022), https://www.internetsociety.org/blog/2022/09/sender-pays-what-lessons-european-policy-makers-should-take-from-south-korea/.

[478] CCIA, Proposed to Mandate Payments by Content and Application Providers (CAPs) Undermines the Future of U.S.-Korea Trade (Sept. 2022), https://www.ccianet.org/wp-content/uploads/2022/09/CCIA-Trade-Analysis-of-Korean-Network-Usage-Fee-Proposals.pdf.

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). Industry reports that the three main technical requirements that have prevented all global CSPs from being able to obtain the CSAP: (1) physical separation; (2) Common Criteria (CC) certification; and (3) use of domestic encryption algorithms.

Through these onerous requirements that depart from international standards, the CSAP effectively casts technical blockers to trade and prohibits global CSPs from accessing public sector workloads in Korea. The government also requires CSAP-like controls in other sectors, such as in healthcare, with the Ministry of Health and Welfare (MOHW)'s recent inclusion of CSAP-like controls—such as the physical location of cloud facilities, data residency, and CC certification obligations—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 satisfy the CSAP-like controls.

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 ban 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.[479] The targeting of U.S. firms could conflict with Korea's trade 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).

The rules banning app store operators from requiring "specific payment methods" were approved by the Korea Communications Commission on March 8, 2022.[480] The agency announced on August 16, 2022, that it was investigating Google, Apple, and SK Group's OneStore over potential violations regarding in-app payments, with a specific warning to Google and Apple: "In addition, the KCC determined that if Google or Apple imposes discriminatory conditions on the payment method (third-party payment) provided by the app developer in an internal payment, or makes the

[479] 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.

[480] Enforcement Decree, Mar. 8, 2022, https://www.kcc.go.kr/user.do?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=4&boardSeq=52916

usage process inconvenient, that act may constitute an act of forcing a specific payment method (own company payment)."[481]

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. Industry reports inconsistent and opaque definitions and implementation procedures of the legislation by the KCC which has resulted in uncertainty for businesses operating or seeking to operate in Korea.

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 long-standing 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.[482] While in the pursuit of

[481] KCC Begins Fact-Finding Investigation of Three App Market Operators, Aug. 16, 2022, https://www.kcc.go.kr/user.do?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=1&boardSeq=53609.

[482] 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.[483]

Y. 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.[484] 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% of the world's internet, voice and data traffic, including the backhaul of mobile network traffic and data for digital trade.[485]

The revocation was a means to protect the domestic shipping industry from foreign competition. In May 2022, Malaysia's transport minister Wee Ka Siong said the revocation would remain, and that the requirement for foreign vessels to obtain a Domestic Shipping License is "not a hindrance" to submarine cable projects.[486]

Restrictions on Cloud Services

In October 2021, the Malaysian Communications and Multimedia Commission (MCMC) expressed its intent to subject data centers and cloud service providers to licensing obligations under the Communications and Multimedia Act 1998 (CMA 1998).[487] 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 are 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

---

[483] *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/.

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

[485] *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).

[486] *Shipping License Requirement Does Not Hinder Projects, Says Dr. Wee*, THE STAR (May 20, 2022), https://www.thestar.com.my/news/nation/2022/05/20/shipping-license-requirement-does-not-hinder-undersea-cable-projects-says-dr-wee.

[487] 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.

make mandatory payments to the Universal Service Fund. These new rules went into effect on January 1, 2022.[488]

Z. Mexico

Taxation of Digital Services

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,[489] and the kill switch was removed in the previous Budget. However, the fact that a limited number of companies registered in the government's regime (35 companies in Mexico, compared to more than 100 in Chile in the same timeframe, due to Mexico's incredibly complex registration process) has led them to reintroduce the measure as a way to force compliance. The measure was approved by Congress in November 2020, and entered into force on January 1, 2021.[490] 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 made reforms to its Federal Copyright Law in 2020 in attempts to bring its law in compliance with commitments under USMCA. There are concerns that the text of the provisions implementing Article 20.87-88 of the USMCA inappropriately narrows the application of this framework for Internet services.

---

[488] *Malaysia: Cloud Services to Be Licensed From 1 January 2022*, BAKER MCKENZIE, https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/malaysia-cloud-services-to-be-licensed-from-1-january-2022.

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

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

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 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

Additional E-Commerce Barriers

Mexico published new regulations that increased import rates on shipments from the U.S. and Canada valued between USD $50-117 by 1 percent (from 16 percent to 17 percent). These changes were made without following appropriate protocols or advance notice, and they became effective immediately. Mexico should fully implement its commitments under USMCA's Customs Chapter, including eliminating the new import rates and implementing an informal clearance threshold for shipments up to USD $2,500.

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 in order to use secure U.S.-based cloud computing services. The regulations could also lead to U.S. cloud services being disadvantaged in the region compared to local data center firms.

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

Article 49 would establish an authorization model with a high degree of discretion and lack of transparency for the use of cloud computing services. These provisions would 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.[491] Industry reports concerns that the requirements could result in Federal Government cloud procurement to favor providers with data centers located in Mexico.

Industry reports concerns that 2021 rules stipulating electronic payment fund entities must retain a disaster recovery plan that depends on either relying on several cloud service providers from various jurisdictions or a data center in Mexico that is self-sufficient from the country of origin of the firm. The National Banking and Securities Commission administers approvals, a process that industry is concerned requires large amounts of resources and discriminates against non-Mexican providers, as data centers in Mexico are privy to a shorter and more streamlined notification process. These rules represent a de facto data localization requirement, complicating a situation where U.S. and foreign firms are already subjected to a time-consuming and complicated process for approval. Industry is encouraged by the United States informing Mexico's government that these obligations on cloud services providers and electronic payment fund institutions could hinder U.S. competitiveness in the Mexican market.

Local Content Requirements

In September 2020, Senator Ricardo Monreal presented a legislative proposal that seeks to reform the Federal Telecommunications Act and require a 30 percent local content quota for over-the-top (OTT) platforms operating in Mexico. A local content quota for OTT platforms would violate Mexico's commitments under Articles 14.10 and 19.4.1 of USMCA. Local content requirements also limit free expression and consumer choice, distort the growing audio-visual 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 15%-10% national content quota requirement for OTT services.

Barriers to Energy Access

Industry continues to harbor concern regarding the persistent obstacles to connections to the electricity grid for the purchase of clean and reliable energy created by the government of Mexico. Firms are required to buy energy directly from a state-owned entity, the Federal Electricity Commission, and subsequently being subjected to a disproportionate volume of infrastructure transmission requests to connect to the grid with the National Center for Energy Control. The government additionally continues to restrict any potential for firms to go off-grid or generate energy privately. Firms are therefore unable to sustain their energy needs in Mexico

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

absent participation in this scheme, jeopardizing their clean energy targets. Industry is pleased to see the United States requesting dispute settlement consultations with Mexico's government under the USMCA on this matter.

AA. New Zealand

Taxation of Digital Services

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.[492] 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 in order to find a workable solution to the issue of multinational corporations not paying their fair share of tax."[493] CCIA urges New Zealand to continue its support for a multilateral solution with other nations.

Data Policies

The NZ Government has pursued 'Cloud First' policies[494] that are promising in regards to enabling digital trade, and has led 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."[495] Industry is monitoring some calls for data flow restrictions which may have implications for the free flow of data across borders.[496] CCIA urges the U.S. government to engage New Zealand to work collaboratively to address these issues to ensure there is a solid basis for digital trade agreements.

---

[492] 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/.

[493] Our Manifesto To Keep New Zealand Moving, 2020, Labour_Manifesto_2020.pdf at 10, https://drive.google.com/file/d/13uhcVrn8HUXEoWoPQgkJYjHX_d_Za-O0/view.

[494] Digital Government New Zealand. Cloud Services, https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/ (last visited Oct. 28, 2022).

[495] 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).

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

News Publishers' Association Collective Bargaining with U.S. Online Platforms

The Commerce Commission of New Zealand reached a preliminary view on August 8, 2022,[497] that it would allow the News Publishers' Association of New Zealand to collectively bargain with Meta and Google for payment in return for the platforms "display[ing], host[ing], featur[ing], link[ing] or summaris[ing]" their content.[498] Several New Zealand publishers have already reached separate agreements with Meta and Google. The Commerce Commission's final decision is set to be delivered by November 4, 2022.[499]

BB. 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. The ban was eventually lifted in January 2022 after seven months,[500] and was condemned by the Economic Community of West African States.[501] 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.[502] Additionally, the government imposed two outright Internet shutdowns in 2021, a reflection of the concerning level of digital barriers U.S. online services providers experience in the country.[503]

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

---

[497] Commerce Commission Issues Draft Determination on News Publishers' Association's Collective Bargaining Application, https://comcom.govt.nz/case-register/case-register-entries/news-publishers-association-of-new-zealand-incorporated2/media-releases/commerce-commission-issues-draft-determination-on-news-publishers-associations-collective-bargaining-application.

[498] Application for Provisional Authorisation, https://comcom.govt.nz/__data/assets/pdf_file/0024/271671/News-Publishers27-Association-of-New-Zealand-Incorporated-Provisional-authorisation-application-25-November-2021.pdf at 4.

[499] Case Register – News Publishers Association of New Zealand, https://comcom.govt.nz/case-register/case-register-entries/news-publishers-association-of-new-zealand-incorporated2.

[500] *Nigeria Lifts 7-Month Ban on Twitter*, N.Y. TIMES (Jan. 13, 2022) https://www.nytimes.com/2022/01/13/world/africa/nigeria-lifts-twitter-ban.html.

[501] *Nigeria's Twitter Ban Unlawful in W. African Court*, FRANCE 24 (July 14, 2022), https://www.france24.com/en/live-news/20220714-nigeria-s-twitter-ban-unlawful-w-african-court.

[502] *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/.

[503] Keep It On, The Return of Digital Authoritarianism, *supra* note 436.

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.[504] Additionally, the legislation could undermine the very structure of the open Internet.[505]

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 cross-border transfer. 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. 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.

While this current draft version has moved well beyond data localisation 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."

Reports suggest the government seeks to ramp up consideration of this legislation and begin the process by the end of December 2022.[506]

---

[504] *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.

[505] INTERNET SOCIETY, *Internet Impact Brief: Nigeria's Protection from Internet Falsehood and Manipulation Bill 2019* (Feb. 2022), https://www.internetsociety.org/resources/2022/internet-impact-brief-nigerias-protection-from-internet-falsehood-and-manipulation-bill-2019/ ("The reports finds that implementing the regulatory measures described in the proposed Protection from Internet Falsehood and Manipulation Bill 2019 would negatively affect the performance, resilience, trustworthiness and security of the Internet; with significant impact on the Critical Properties of the Internet Way of Networking. It could also reduce future socio-economic opportunities that the Internet could offer for Nigeria by limiting global access to information by Nigerian citizens, and cutting them off from participating in online spaces.")

[506] *See It's a Criminal Offense to Access Data in Nigeria Without Permission*, Vanguard (Oct. 2022), https://www.vanguardngr.com/2022/10/its-criminal-offence-to-access-data-in-nigeria-without-permission-pantami/. Nigerian Data Protection Bureau, Protection Bill to Be Passed Before December, https://ndpb.gov.ng/Home/NewsDetails/11.

A complicating factor is the emergence of a new agency in Nigeria, the Nigeria Data Protection Bureau, which was created in February 2022.[507] The establishment of this new authority takes data privacy and processing oversight away from the National Information Technology Development Agency, into the new NDPB's hands.[508] As the Data Protection Bill advances simultaneously to the development of the NDPB's modus operandi, CCIA urges the U.S. government to ensure U.S. digital services exports are not adversely affected.

Taxation of Digital Services

The 2020 Finance Act introduces income tax obligations for non-resident companies providing digital goods and services in Nigeria.[509] 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 US 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.

This policy was eventually signed into law as the Finance Act of 2021 on December 31, 2021,[510] which captured U.S. tech firms under revisions to its Value Added Tax code policies and resulted in a knock-on 7.5% VAT rate for tech firms such as Google.[511] Non-resident digital services firms are also required to pay 6% of their yearly turnover as well.[512]

Another form of taxation is developing in Nigeria, whereby the government requires *all* advertising of any kind to be approved by the Advertising Regulatory Council of Nigeria at risk of monetary punishment. In October 2022, the body fined Meta $70 million for allegedly running advertisements without prior vetting, a process that poses an unreasonable burden for online platforms that rely on such advertising presented to a market as large as Nigeria—and interconnected with services offered globally—for their revenue streams.[513]

---

[507] *Nigeria Has a New Data Protection Enforcing Body*, TECH POINT (Mar. 10, 2022), https://techpoint.africa/2022/03/10/nigeria-data-protection-bureau.

[508] *The Nigeria Data Protection Bureau and the Challenges of Data Privacy and Compliance in Nigeria*, MONDAQ (Mar. 30, 2022), https://www.mondaq.com/nigeria/privacy-protection/1177500/the-nigeria-data-protection-bureau-and-the-challenges-of-data-privacy-compliance-in-nigeria.

[509] 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.

[510] Available at https://www.firs.gov.ng/wp-content/uploads/2022/04/Finance-Act-2021-Gazetted.pdf and https://pwcnigeria.typepad.com/files/finance-act-2021-gazette.pdf.

[511] *Google, Meta, and Others Raise Nigeria Prices Due to Digital Tax*, QZ (Mar. 4, 2022), https://qz.com/africa/2137660/google-meta-and-others-raise-nigeria-prices-due-to-digital-tax/.

[512] *Id.*

[513] *Nigeria Regulator Seeks $70M Penalty Against Meta*, AP NEWS (Oct. 5, 2022), https://apnews.com/article/technology-africa-business-lawsuits-nigeria-f00313679c07f2a56d844d53b7094643

Draft Code of Practice for Interactive Computer Service Platforms/ Internet Intermediaries

Nigeria's National Information Technology Development Agency posted draft regulations, dubbed the "Code of Practice for Interactive Computer Service Platforms/ Internet Intermediaries" in June 2022 which contain a wide spread of concerning government intrusiveness into online platforms' content moderation decisions, onerous takedown regimes, and localization requirements reserved only for "large" suppliers.[514]

The regulations would require platforms to take down content, once notified by a user or a government agency, unlawful content within 24 hours and to take down content of a wide range of sexual material once notified within 24 hours. The regulations would also require platforms to reveal the identity of "the creator of information" on its service when demanded by a court order if it is for the "purpose of preventing, detecting, investigating, or prosecuting an offence concerning the sovereignty and integrity of Nigeria, public order, security, diplomatic relationships, felony, incitement of an offence relating to any of the above or in relation to rape, child abuse, or sexually explicit material." Given Nigeria's prior attempts to restrict use of social media to target dissent of the government and blocking of Twitter due to political disagreements,[515] the ability to demand personal information of online platforms' users—a deeply invasive and intrusive measure for these suppliers—for offenses in the broad categories of "public order", "sovereignty and integrity of Nigeria", and "security" are concerning on its own. However, even beyond the problematic requirement for social media companies to demand identifiable information for all users of its service—there are many reasons in the interest of freedom of expression users seek anonymity that are not nefarious—the feasibility of requiring a platform to track down the original creator of a certain piece of content who themselves may not be a user of that platform would be burdensome in the easiest circumstances, while more likely often being impossible to comply with.

The regulations would also impose monitoring requirements on platforms—under the term "due diligence" to ensure no unlawful content is uploaded to their services and a subsequent requirement to not only take down content when alerted by authorized government agencies but to also "ensure it stays down." This would be an unreasonably burdensome requirement to impose on online platforms while also infringing on individual users' privacy. The regulations would also dictate to platforms what to include in their terms of service, including requirements to tell users that they cannot "create, publish, promote, modify, transmit, store or share any content or information" that accomplishes a wide variety of harmful outcomes that are poorly defined and could be broadly interpreted.

Additionally, the draft regulations impose additional obligations on "large service platforms," defined as those with more than 100,000 users (which would implicate largely U.S. companies as

---

[514] Available at https://nitda.gov.ng/wp-content/uploads/2022/06/Code-of-Practice.pdf. *See also Nigeria to require social media platforms to open local offices*, REUTERS (June 14, 2022), https://www.reuters.com/world/africa/nigeria-require-social-media-platforms-open-local-offices-2022-06-14/.

[515] Danielle Paquette, *Nigeria's 'Fake News' Bill Could Jail People for Lying on Social Media*, WASH. POST (Nov. 25, 2019), https://www.washingtonpost.com/world/africa/nigerias-fake-news-bill-could-jail-people-for-lying-on-social-media-critics-call-it-censorship/2019/11/25/ccf33c54-0f81-11ea-a533-90a7becf7713_story.html.

well as some Chinese companies).[516] Requirements on these larger suppliers include mandating local presence and a Liaison Officer; human supervision of "automated tools"; and to disclose details behind automated tools and algorithms "on demand" for both a user and a government agency.[517]

In June, the government stated they were still soliciting feedback, but the timeline for finalizing these rules is not clear.[518]

CC. 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. 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."[519] 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.[520]

These eventually became the set of new regulations, dubbed "Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021," that were published and enacted on October 13, 2021.[521] The law empowers the government to demand online services providers—defined through "any information system"—to take down online content it deems necessary to protect the "glory of Islam", the "security of Pakistan", "public order", "decency and morality", and the "integrity or defence of Pakistan". Online content providers—such as social media companies—would have 48 hours to comply, or the government would have the ability to

[516] Leading Social Media Platforms in Nigeria: https://www.statista.com/statistics/1176101/leading-social-media-platforms-nigeria/

[517] From the draft regulations: "On demand, furnish a user, or authorised government agency with information on: a) reason behind popular online content demand and the factor or figure behind the influence. b) why users get specific information on their timelines."

[518] NITDA Draft Code for Interactive Service Intermediaries, https://www.jdsupra.com/legalnews/nitda-draft-code-for-interactive-2201828/.

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

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

[521] Available at https://moitt.gov.pk/SiteImage/Misc/files/Removal%20Blocking%20of%20Unlawful%20Online%20Content%20Rules%202021.PDF. *See also* Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021, A Law in Furtherance of the Main Data Protection Law in Pakistan, The Prevention of Electronic Crimes Act 2016, https://www.legal500.com/developments/thought-leadership/removal-and-blocking-of-unlawful-online-content-procedure-oversight-and-safeguards-rules-2021-a-law-in-furtherance-of-the-main-data-protection-law-in-pakistan-the-prevention-of-electronic-crimes/.

degrade the providers' services, block the provider, or impose a fine of up to 500 million rupees (about $2.24 million). Additional requirements for online content providers include: mandatory local office presence and registration by the entity providing the service within three months; obligations 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); compliance "with the user data privacy and data localization provisions" of a forthcoming Data Protection Law; intrusive content moderation and monitoring requirements; and providing user data in a decryptable and readable format to investigative authorities in accordance with existing federal law. These rules greatly jeopardize the ability of U.S. firms to operate in Pakistan and undermine freedom of expression in a sizable market.[522]

Additionally, the Pakistani government implemented two outright Internet shutdowns in 2021, which as previously stated, imposes large economic losses and harms human rights.[523]

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. 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. The draft bill would also introduce and provide broad powers to a new National Commission for Personal Data Protection with the ability to bring forth new regulatory frameworks and to demand access to data.

Restrictions on Cloud Services

Pakistan established a Cloud First Policy in 2022 that implements data localization requirements on broad-sweeping categories of data, such as "restricted", "sensitive", and "secret". Further, the State Bank of Pakistan (SBP) disallows financial sector institutions from storing and processing fundamental data troves on offshore cloud. These data localization requirements are ineffective at enhancing data protection while simultaneously making the costs of compliance excessive for U.S. suppliers, which represent a potential barrier to participation in the market.

[522] Asia Internet Coalition, *Comments on Pakistan Removal and Blocking of Unlawful Content* (June 2021), https://aicasia.org/2021/06/28/pakistan-aic-submits-comments-on-the-amendment-removal-and-blocking-of-unlawful-online-content-procedure-oversight-and-safeguards-rules-june-2021/.

[523] KEEP IT ON, *The Return of Digital Authoritarianism*, *supra* note 436.

DD. Peru

Copyright Liability Regimes for Online Intermediaries

Peru remains out of compliance with key provisions under the U.S.-Peru Trade Promotion Agreement (PTPA). Article 16.11, para. 29 of the PTPA requires certain protections for online intermediaries against copyright infringement claims arising out of user activities. USTR cited this discrepancy in its inclusion of Peru in the 2018 Special 301 Report, and CCIA supports its inclusion in the 2021 NTE Report. CCIA urges USTR to engage with Peru and push for full implementation of the trade agreement and establish intermediary protections within the parameters of the PTPA.

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

In 2020, the Digital Government Secretariat of Peru released Emergency Decree 007 - Digital Trust Framework draft regulations for consultation.[524] 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 ability to access client's information, or organizations that use digital channels to provide their services. The Data Protection Authority would determine model contract clauses, which appear to exceed what is currently required under the Data Protection Law. The National Data Center would incentivize domestic data storage by providing infrastructure to domestic data center operations, granting the government control over the data.

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

In July 2021, Russia enacted Law N236-FZ. The Law provides that companies owning any website/app which is accessed daily by 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. The law also provides for a detailed set of requirements beyond establishing local presence, including processing enquiries from RU legal entities and state bodies, complying with RU courts' and state bodies' rulings, registering on the Rosco site, removing notified content, installing

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

government-provided software to "count users" of the website/app, and providing an electronic form for applications by Russian individuals and entities.

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 "land" – and failure to comply with other obligations – may trigger a wide range of sanctions, including service blockage, traffic throttling, platform advertising bans, and bans on money transfers and payments from Russia.

Import Barriers

The National Superintendent of Customs and Tax Administration has limited the number of express delivery shipments that an individual without a tax number can execute annually to a maximum of three. The regulations lack clarity whether individuals engaging in more than three shipments of personal imports would be deemed to be commercial and therefore introduce new income tax requirements. These obligations therefore restrict individuals' ability to import personal goods and establishes a potential barrier for firms engaging in express delivery shipments to the country. The requirement also contradicts the U.S.-Peru Trade Promotion Agreement of 2009, which established a de minimis threshold of $200.[525]

EE. Philippines

Additional Restrictions for E-Commerce

The Department of Trade and Industry, Department of Health, Department of Agriculture, Department of Environment and Natural Resources, Intellectual Property of the Philippines, and National Privacy Commission issued Joint Administrative Order No. 22-01 (JAO), Guidelines for Online Businesses Reiterating the Laws and Regulations Applicable to Online Businesses and Consumers, on March 4, 2022.[526] The JAO consolidates all existing regulations for online transactions and cautions merchants against the sale of "unlicensed, restricted or prohibited products." The ASEAN Online Business Code of Conduct is adopted by the JAO to inform merchants of standards for the fair treatment of consumers. The government agencies sought comment and will jointly monitor the JAO's enforcement.[527]

Forced Social Media Identification Database

On October 10, 2022, the SIM Card Registration Act was signed into law, requiring Public Telecommunications Entities to mandate that their SIM users register with the business. The law's original formation included an obligation for social media providers to demand users' real names and phone numbers to create an account for their services, though was not included in the

[525] Article 5.7(g)

[526] DEP'T OF TRADE & INDUSTRY, Joint Administrative Order on Online Businesses Released, https://www.dti.gov.ph/archives/news-archives/joint-administrative-order-on-online-business-released/.

[527] *See* DEP'T OF TRADE & 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].

final version of the legislation that became law. However, instead of this requirement, a proposed bill—Senate Bill 1289 or the Online & Social Media Membership Accountability Bill, has been introduced in the legislature.[528] The bill would require electronic identification that compels users to submit a valid proof of identification to use services, while also restricting consumers from owning multiple accounts in the same website and from using separate usernames that are not their actual names. Including such a requirement would dampen free expression and represent an undue burden on online platforms serving customers in the Philippines.

Taxation of Digital Services

The Philippines Bureau of Internal Revenue (BIR) has implemented obligations for income payors to gain the benefits afforded to them under the Income Tax Convention of 1976. This treaty, signed between the United States and the Philippines, ensures that a country's taxation of the profits of a business earned by a resident of the partner country is overseen by the "standard treaty concept that tax liability will arise only to the extent that the profits are attributable to a 'permanent establishment' in the taxing country."[529] The BIR, however, mandates income payors to seek a request for confirmation with the agency through a filing, the approval of which is governed by complex and burdensome documentation procedures that hinder the ability of firms to avail themselves of the benefits of this treaty. Industry has expressed concern that failure to adhere to the documentation guidelines could lead to entities being subjected to penalties and criminal liabilities. The BIR has not established standard procedures guiding the length of time requests for confirmation are processed, and businesses are subsequently required to wait indefinitely without any commitment towards a resolution of the filing. These requests are required of all U.S. non-resident service providers operating in the Philippines and, therefore, this policy is not limited to digital services but does impact members of the industry seeking to provide their services and goods to the Philippines market.

Separately, industry reports concern about the introduction of a Digital Value-Added Tax (VAT) bill, (HB No. 372), into the House of Representatives. Despite failing to pass the Senate when sent there from the House, at a House Committee on Ways and Means deliberation on August 17, 2022, lawmakers discussed introducing a provision requiring non-resident foreign corporations to designate an agent of the firm to reside in the Philippines as part of the legislation, which industry fears could serve as an avenue for a direct tax.[530] Industry is monitoring the provision as the VAT bill continues to be considered by lawmakers.

Government Procurement

Industry expresses concern that Republic Act No. 9184—the Government Procurement Reform Act—acts in conjunction with Republic Act. No. 5183 to preference Philippine nationals or firms controlled by Philippine nationals for government procurement contracts.[531] This favorable

[528] Available at https://legacy.senate.gov.ph/lis/bill_res.aspx?congress=19&q=SBN-1289.

[529] Income Tax Conventions with the Republic of the Philippines, https://www.irs.gov/pub/irs-trty/philip.pdf at 3.

[530] *See* Committee Meeting Schedule, https://www.congress.gov.ph/commsched/schedule.php?d=17%20&m=8&y=2022.

[531] The 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184 (as of 31 March 2021), https://www.gppb.gov.ph/assets/pdfs/Updated%202016%20IRR_31%20March%202021.pdf.

treatment for Philippines entities is worsened by Commonwealth Act. No. 138 and Republic Act No. 9184, which stipulates that the government body in question can elect the lowest domestic bidder as the winner of a contract even when a foreign entity offers a lower bid if the domestic bidder's offer represents fifteen percent or less of the foreign bidder's offer.[532] These rules reflect general preference for domestic contractors and therefore hinder foreign entities from gaining access to government procurement work.

Restrictions on Cloud Services

The public procurement preferences for domestic entities extend to the cloud sector, restricting foreign and U.S. suppliers' activities in the Philippines market absent domestic partnership. Industry continues to offer cloud services to the Philippines but is concerned that foreign providers are subjected to a mandated licensing process administered by the Securities and Exchange Commission in the country in exchange for providing cloud services to the public sector.[533] Due to U.S. cloud services providers lacking a license with the SEC, entities seeking public sector procurement are forced to work with domestic entities, reflecting a de facto obligation.

Internet Transactions Legislation

A proposed bill, dubbed the Internet Transactions Bill, which is currently pending consideration in the Philippines legislature would require digital platforms to submit to the Trade Ministry a list of each of its online merchants every six months at risk of criminal penalties for non-compliance.[534] The proposed legislation would empower the Trade Minister with broad power to issue takedown orders as well as other obligations for online platforms providers such as mandatory registration to the Online Business Registry. Industry reports concerns that the bill has been marked as priority legislation of the President and could move quickly in the coming months to becoming law.

FF. 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.[535] 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 have 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

[532] *Id.*

[533] See Government Procurement Policy Board Resolution No. 14-2021, https://www.gppb.gov.ph/issuances/Resolutions/GPPB%20Resolution%20No.%2014-2021_SEC%20Registration%20with%20SGD.pdf

[534] Available at https://www.pna.gov.ph/articles/1182088. *See also* https://www.lexology.com/library/detail.aspx?g=f6fc2b5c-6adb-4cc7-a00e-ee726ff9ee9c.

[535] 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-serwisowspolecznosciowych.

speech. In early 2022, Poland Deputy Minister Michał Woś indicated the law was ready for approval, but final passage has not yet occurred.[536]

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, e-books and audiobooks.[537] 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 provide access to e-books and audiobooks for a specific monthly subscription.

Taxation of Digital Services

As part of its broad tax reform initiative, the Polish Government has proposed the introduction of a minimum corporate tax levy.[538] 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.[539]

GG. Russia

After Russia began invasion of Ukraine, its actions towards U.S. digital firms became increasingly hostile as well, as a combination of aggressive regulatory and discriminatory practices and U.S. firms exiting the market due to the unprovoked war on Ukraine left the online services market—and the physical goods market—with a significantly smaller U.S. presence. Russia's long-sought pursuit of an isolated Internet infrastructure and ecosystem accelerated—along with severance from the global financial and business system, technology companies have largely either been banned, have voluntarily removed themselves from Russia's market since Russia launched its war in Ukraine, or have been forced to close after Russian authorities seized its financial assets, as was the case with Google.[540] Meanwhile, a state-run company has bought

---

[536] *Polish Justice Ministry Proposes Online Free Speech Law After Facebook Debacle*, EURACTIV (Jan. 18, 2022), https://www.euractiv.com/section/politics/short_news/polish-justice-ministry-proposes-online-free-speech-law-after-facebook-debacle/.

[537] Available at http://www.pik.org.pl/komunikaty/876/ustawa-o-ochronie-rynku-ksiazki-d-uojck-iuzasadnienia-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/.

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

[539] 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-advertisingcontributions-traditional-online-advertising.html.

[540] Jillian Deutsch & Ivan Levingston, *War Accelerates Russia's Internet Isolation*, BLOOMBERG (Mar. 10, 2022), https://www.bloomberg.com/news/articles/2022-03-10/russia-internet-isolation-accelerates-after-ukraine-invasion; Adam Satariano & Valerie Hopkins, *Russia, Blocked from the Global Internet, Plunges Into Digital*

the search engine, news feed, and blogging services of Google's local competitor Yandex, expanding the Kremlin's control of the Internet domestically.[541] This has left Russia with an almost-entirely isolated internet.[542]

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 a number of obligations on services to comply with government demands. Russia's telecommunications regulator has developed away from its primary objective towards a quasi-intelligence agency over the past several years, orchestrating the Kremlin's censorship and surveillance activities.[543]

Russia's already stringent state-sponsored censorship of content online also dramatically increased. The censorship of news has blended interference with traditional media outlets as well as news online. In March, Russia enacted a "fake news" law which prohibited the publication of what the government determined to be falsities about the war in Ukraine—including calling the war an "invasion."[544] The campaign to control news in Russia has been prominent online.

The government has threatened to block websites of outlets for critical commentary or news about its invasion of Ukraine and throttled and/or blocked access to websites and platforms hosting online news sources such as Twitter and Instagram.[545] Russia blocked use of Facebook in March.[546] YouTube, which has historically represented one of the only sources for news that is free from the Kremlin's propaganda, continues to operate but has been hit with a series of fines by the Russian telecommunications regulator—the Russian Federal Service for Communications Supervision, or Roskomnadzor—for leaving up what the Russian government called "misleading information" about the war in Ukraine. The two fines imposed on Google for YouTube's hosting policies equaled 5-10% and 8% of the company's yearly turnover earned in Russia, respectively.

Isolation, N.Y. TIMES (Mar. 7, 2022), https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html; Elahe Izadi & Sarah Ellison, *Russia's independent media, long under siege, teeters under new Putin crackdown*, WASH POST (Mar. 4, 2022), https://www.washingtonpost.com/media/2022/03/04/putin-media-law-russia-news/.

[541] *Russia Tightens Grips on Internet as Yandex Sells Assets to State-Run VK*, REUTERS (Aug. 23, 2022), https://www.reuters.com/markets/europe/russia-tightens-grip-media-yandex-sells-homepage-news-rival-vk-2022-08-23/.

[542] *Russia, Blocked from the Global Internet Plunges into Digital Isolation*, N.Y. TIMES (Mar. 7, 2022), https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html.

[543] *They Are Watching: Inside Russia's Vast Surveillance State*, N.Y. TIMES (Sept. 22, 2022), https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html.

[544] *Russia's Intendent Media, Long Under Sieges, Teeters Under New Putin Crackdown*, WASH. POST (Mar. 4, 2022), https://www.washingtonpost.com/media/2022/03/04/putin-media-law-russia-news/.

[545] *Russia: With War, Censorship Reaches New Heights*, HUMAN RIGHTS WATCH (Jan. 28, 2022), https://www.hrw.org/news/2022/02/28/russia-war-censorship-reaches-new-heights.

[546] Available at https://t.me/s/rkn_tg. *See also Russia Blocks Access to Facebook*, CNBC (Mar. 4, 2022), https://www.cnbc.com/2022/03/04/russia-blocks-access-to-facebook.html.

Despite the tension between the two, a leading lawmaker for information policy in the Duma suggested in June that YouTube is not yet under threat of being blocked in Russia.[547]

Other enforcement actions Russia has taken regarding what it has deemed "misinformation" or "fake news" include when it blocked Soundcloud in October for spreading "false information",[548] fined Google $373 million in July for repeated "fake news",[549] and fined Twitch $33,000 in August for hosting a brief video with purported "fake" information about the invasion of Ukraine.[550]

Other recent laws include Federal law N482-FZ and Federal law N511-FZ, which came into effect in 2021.[551] Under Federal law N482-FZ, certain platforms can be fined or blocked (through explicit blocking or throttling of Internet traffic) for removing or restricting access to content by the Russian media. Federal law N511-FZ imposes fines for services that do not remove banned information, which has included political protest content. 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. 66 Firms that Russian authorities determine have not sufficiently complied with demands have experienced an uptick in throttling and restriction in services.[552]

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.[553] In March 2019, Russia passed two laws aimed at eliminating "fake news". The Federal Law on

---

[547] *See, e.g., Google Faces Second Turnover Fine in Russia Over Banned Content*, REUTERS (June 22, 2022). https://www.reuters.com/technology/google-faces-second-turnover-fine-russia-over-banned-content-regulator-2022-06-22/; *Russia Court Fines Google For Breaching Data Rules*, REUTERS (June 16, 2022), https://www.reuters.com/technology/russia-fines-google-260000-breaching-data-localisation-rules-tass-2022-06-16/

[548] *Russia Blocks SoundCloud, Citing Spread of 'False Information'*, REUTERS (Oct. 2, 2022), https://www.reuters.com/technology/russia-blocks-soundcloud-citing-spread-false-information-ifx-2022-10-02/

[549] *Russia Fines Google for Repeated Content Violations*, REUTERS (July 18, 2022), https://www.reuters.com/technology/google-is-fined-390-mln-russia-not-deleting-banned-content-interfax-2022-07-18/.

[550] *Russia Fines Streaming Site Twitch Over 31-Section 'Fake' Video*, REUTERS (Aug. 16, 2022), https://www.reuters.com/technology/russia-fines-streaming-site-twitch-over-31-second-fake-video-agencies-2022-08-16/.

[551] Baurzhan Rakhmetov, 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.

[552] *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.

[553] *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/.

Amending Article 15-3 of the Federal Law on Information, Information Technologies and Protection of Information[554] and the Federal Law on Amending the Code of Administrative Violations,[555] 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.[556] The law took effect in early 2021.[557] The scope of devices is likely to include smartphones, computers, tablets, and smart TVs, and the scope of applications is likely to include search engines, navigation tools, anti-virus software, software that provides access to e-government infrastructure.

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.[558] In early June 2022, Russia began to accelerate its ongoing campaign to block virtual private networks as part of its effort to block off citizens from outside news sources and influences amidst its invasion of Ukraine. Roskomnadzor stated it was taking "measures to restrict the use" of VPNs, including Proton VPN, arguing that the "Law on Communications defines means used to bypass the blocking of illegal content as a threat."[559] That followed a revelation in mid-March from a senior Duma member focused on information policy that at least 20 VPN services were being blocked in Russia with the intent of blocking more services deemed to be in violation of Russian law.[560]

---

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

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

[556] Jon Porter, *Russia Passes Law Forcing Manufacturers to Install Russian-made Software*, THE VERGE (Dec. 3, 2019), https://www.theverge.com/2019/12/3/20977459/russian-law-pre-installed-domestic-software-tvs-smartphones-laptops.

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

[558] 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.

[559] Russia Restricting Proton VPN, https://interfax.com/newsroom/top-stories/79803/.

[560] Andy Maxwell, *New VPN Crackdown Underway In Russia*, TORRENT FREAK (June 3, 2022), https://torrentfreak.com/new-vpn-crackdown-underway-in-russia-government-confirms-220603/.

The harms to U.S. digital services exports from these actions are drastic. The U.S. ITC found that Russia's throttling of Twitter in March 2021[561] resulted in an estimated $200,000 in losses, and estimated that a hypothetical block of Facebook, Instagram, YouTube and Twitter—all of which but YouTube *are* currently banned in Russia—would constitute 23.5% of country-wide economic losses.[562]

Further, these restrictions are not limited to its own jurisdiction. Internet disruptions and the rerouting of Ukrainian Internet traffic have been a key feature of Russia's invasion of Ukraine. Russia's aggression against Ukraine and attempted seizure of the country has been replicated in the digital arena, as Ukrainian Internet service providers have been forced to redirect their services to Russian companies, leaving Ukrainian internet users vulnerable to Russia's surveillance and censorship policies.[563] In July, Russian-backed separatists blocked Google due to purported spread of "disinformation" in a breakaway region of eastern Ukraine.[564] Regional internet outages have occurred throughout Ukraine since Russia began its war campaign in the country,[565] with some areas experiencing blackouts for multiple days—in some cases due to reported Russian cyberattacks.[566] All of these actions represent deeply concerning damages to human life and the ability to communicate during wartime, while also leaving essential online communications services unusable in Ukraine.

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.[567] 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

[561] Dan Goodin, *Russia's Twitter Throttling May Given Censors Never Been Seen Capabilities*, ARS TECHNICA (Apr. 6, 2021), https://arstechnica.com/gadgets/2021/04/russias-twitter-throttling-may-give-censors-never-before-seen-capabilities/

[562] USITC, Foreign Censorship Part 2, *supra* note 32, at 74.

[563] *Russia is Taking Over Ukraine's Internet*, WIRED (June 15, 2022), https://www.wired.com/story/ukraine-russia-internet-takeover/

[564] *Russia-Baked Separatists in Ukraine Block Google Search Engine*, REUTERS (July 22, 2022), https://www.reuters.com/world/europe/russian-backed-separatists-ukraine-block-google-search-engine-2022-07-22/.

[565] *Ukraine Facing Major Regional Outages as Russian Invasion Continues*, NBC NEWS (Mar. 9, 2022), https://www.nbcnews.com/tech/tech-news/ukraine-facing-major-regional-internet-outages-russian-invasion-contin-rcna18973.

[566] *Occupied Regions of Southern Ukraine Lose Internet Services*, WALL ST. J. (May 1, 2022), https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-04-30/card/occupied-regions-of-southern-ukraine-lose-internet-service-YrGVuhNABIkQzxc099dM.

[567] 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.

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. Roskomnadzor put forward a list of firms that would be obligated to register as Russian legal entities or establish offices in the country. Firms were given a deadline of February to adhere to the law. 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.

This landing law—previously imposed on foreign technology companies to pressure firms to establish legal entities in Russia for permission to continue operations in the country—has been leveraged by the Kremlin along with throttling websites, fining companies, and jailing individuals as a method of censorship during the war in Ukraine.[568] Illustrative of this, a BBC analysis of 400 social media posts referenced in Russian court proceedings for removal demands revealed that an "overwhelming majority" reflected outreach for pro-Navalny protests.[569] In early July, 2022, Russian lawmakers passed legislation that would impose heavier fines—up to 10% of a company's prior year revenue in Russia and rising to potentially 20% if a company is found to repeatedly violate the law—on foreign internet companies with 500,000 or more users per day that decline to open a local office in the country.[570] As Article 19 highlights, establishing local presence in Russia in compliance with the landing law makes it easier for the Russian government to demand removal of content which contradicts its narrative about the war in Ukraine and other political activities and to threaten jail time to company representatives residing in the country.[571] Fines, threats of jail time for employees, and more could be leveraged going forward for companies that continue to operate in the country, leaving U.S. digital services exports with a dangerous landscape for any potential operations.

Russia's broader data localization efforts have intensified, as a Russia court levied fines in late June against Google, Airbnb, Pinterest, Twitch, and UPS for allegedly failing to store the personal data of Russians within the country.[572] The court's announcement of the fines on

---

[568] *Russia Intensifies Censorship Campaign, Pressuring Tech Giants*, N.Y. TIMES (Feb. 26, 2022), https://www.nytimes.com/2022/02/26/technology/russia-censorship-tech.html.

[569] *How Russia Tries to Censor Western Social Media*, BBC (Dec. 17, 2021), https://www.bbc.com/news/blogs-trending-59687496.

[570] *Russian Lawmakers Approve Harsher Fines for Foreign Tech Firms*, REUTERS (July 5, 2022), https://www.reuters.com/world/europe/russian-lawmakers-approve-harsher-fines-foreign-tech-firms-without-offices-2022-07-05/.

[571] Article 19, *Russia Internet Companies Must Challenges Censorship Under New Law* (Jan. 21, 2022), https://www.article19.org/resources/russia-internet-companies-must-challenge-censorship-under-new-law/.

[572] *Russia Fines Streaming Company Twitch Over Data Storage*, REUTERS (June 28, 2022), https://www.reuters.com/technology/russia-fines-streaming-company-twitch-over-data-storage-2022-06-28/; *Russia Fines Airbnb, Twitch, Pinterest on Not Storing Local Data*, GIZMODO (June 28, 2022), https://gizmodo.com/russia-fines-airbnb-twitch-pinterest-google-local-data-1849118187.

Telegram cite "repeated violations" of the country's data localization laws.[573] In mid-June, a Moscow court fined Google 15 million roubles ($260,000) for being found to have repeatedly declined to adhere to data localization laws.[574] These court cases and fines are likely to continue—Roskomnadzor had also announced that an administrative case against Apple had begun in late May.[575]

HH. 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.[576] The rules contain a provision on data localization that may restrict access to the Saudi market for foreign Internet services.[577] 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.[578] 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.[579] Neither the ECC, nor the draft CCC,

[573] Available at https://t.me/s/rkn_tg.

[574] *Russia Fines Google $260,000 for Breaching Data Rules*, REUTERS (June 16, 2022), https://www.reuters.com/technology/russia-fines-google-260000-breaching-data-localisation-rules-tass-2022-06-16/.

[575] *Roskomnadzor Drew Up Administrative Protocols for Airbnb, Pinterest, Apple, Google, Twitch,* FRONT NEWS (May 28, 2022), https://frontnews.eu/en/news/details/31852.

[576] *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.

[577] *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.").

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

[579] *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.

distinguish between data localization requirements for different levels of data classification, which conflicts with the 2018 Cloud Computing Regulatory Framework (CCRF).[580]

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.

The Personal Data Protection Law was passed in September 2021 and went into effect on March 23, 2022, with punishments for certain violations rising to 5 million riyals (approximately $1.33 million) and others leading to up to two years in prison.[581] The law requires storing data in Saudi Arabia and requires any entity that seeks to store or process abroad to first conduct "an impact assessment and [obtain] the written approval of the Regulatory Authority after the Regulatory Authority has liaised with the Competent Authority on a base-by-case basis."[582] Entities that seek to process personal data are required to register and pay an annual fee associated, and non-Saudi companies that process the personal data of Saudi residents are mandated to have a local representative.[583] Data transfers outside of the country are only permitted in limited circumstances and with several restrictions on top of those lifted from GDPR and similar laws implementing adequacy assessments and a list of approved export markets. Firms may only process personal data without a user's express consent in limited instances, and individuals have the ability to rescind that consent—this lack of clarity over exceptions to data transfer restrictions represents confusion for businesses seeking to operate in Saudi Arabia. This law presents a significant barrier to cross-border data flows.

Additional E-Commerce Barriers

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

[580] 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.

[581] Available at https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/b7cfae89-828e-4994-b167-adaa00e37188/1.

[582] Comments of Global Data Alliance, available at https://globaldataalliance.org/wp-content/uploads/2022/03/03292022gdasadatapro.pdf.

[583] *How to Prepare for Saudi Arabia's Personal Data Protection Law*, IAPP, https://iapp.org/news/a/how-to-prepare-for-saudi-arabias-personal-data-protection-law/.

reports extensive documentation requirements that depart from global practice in developed countries.[584]

II. Singapore

Government-Imposed Content Restrictions and Related Access Barriers

The Protection from Online Falsehoods and Manipulation Bill became effective starting on October 2, 2019.[585] The law requires online services to remove content or carry 'corrections' on their platforms in response to claims from the government or from individuals that content is false or misleading.[586] 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. As Singapore holds significant policy influence for the region, industry is concerned that these laws could spread to neighboring countries, particularly those with less due process, weaker rule of law, and more authoritarian regimes. There are also threats to undermine security and privacy.[587] Stakeholders have raised concerns with enforcement of these laws since it went into effect,[588] with early use cases of the law that involved demands to take down political speech and media platforms ahead of the July 2020 general elections.[589] The use of POFMA has moderated throughout the past two years.

In late June 2022, the Ministry of Communications and Information announced two proposed codes of practice for social media service providers—the Code of Practice for Online Safety and the Content Code for Social Media Services—to dictate content moderation practices and safety standards, including the ability to direct such companies to disable access to certain content.[590] The government said that the first would compel social media services to have "system-wide processes" to enhance safety for all users and that the second would empower Infocomm Media

[584] 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.

[585] 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.

[586] *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/.

[587] *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.

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

[589] *Freedom on the Net 2022: Singapore* (2022), https://freedomhouse.org/country/singapore/freedom-net/2022.

[590] *Social Media Platforms to Remove Harmful Content*, STRAITS TIMES (June 20, 2022), https://www.straitstimes.com/tech/tech-news/social-media-platforms-to-remove-harmful-content-add-safeguards-for-young-under-spores-internet-rules.

Development Authority (IMDA) to order social media providers to disable access to certain types of content for Singaporean users.[591]

In October 2022, the Ministry of Communications and Information introduced amendments to the Broadcasting Act, including a Code of Practice for Online Safety for Social Media Services, which would proscribe content moderation practices and "system-wide" safety standards. These procedures would also empower the Infocomm Media Development Authority to compel such companies to block access to harmful—even if not illegal—content for users in Singapore. Industry expects the bill to pass in early November 2022. CCIA urges the U.S. government to remain engaged with counterparts in Singapore, as the specific provisions of the legislation will be crucial to determining the extent to which U.S. industry can continue to participate in Singapore.[592]

Industry is also monitoring government suggestions that they will pursue consultations to form new Online Harms legislation that would likely include issues such as terrorism, fraudulent activity, gambling and other activity online that would implicate offline harms.

Foreign Interference (Countermeasures) Act

The Foreign Interference (Countermeasures) Act (FICA) was passed on October 4, 2021. The law went into effect in July 2022.[593] Similar to the earlier content legislation, the Protection from Online Falsehoods and Manipulation Bill (POFMA), FICA requires online services to remove content or carry 'corrections' on their platforms in response to claims from the government or from individuals that content is being covertly influenced by a foreign actor and introduce service restriction guidelines to certain platforms. 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 rather than a tool of targeting critical political speech. 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. Singapore attempted to address many of these concerns to the United Nations in February 2022, although none of the specific harms were assuaged, even as human rights advocates have expressed opposition.[594]

[591] *Government Proposes Disabling Social Media Access*, Today Online (June 21, 2022), https://www.todayonline.com/singapore/govt-proposes-disabling-social-media-access-harmful-content-part-new-codes-practices-online-safety-1928596.

[592] MCI Seeks Comments on Proposed Code of Practice for Online Safety (July 2022), https://www.allenandgledhill.com/sg/perspectives/articles/22083/sgkh-mci-seeks-comments-on-proposed-code-of-practice-for-online-safety-and-content-code-for-social-media-services.

[593] *Measures in Foreign Surveillance Law to Take Effect*, STRAITS TIMES (July 6, 2022), https://www.straitstimes.com/singapore/measures-in-spores-foreign-interference-law-to-counter-hostile-information-campaigns-take-effect-from-july-7.

[594] Available at https://www.mfa.gov.sg/Overseas-Mission/Geneva/Mission-Updates/2022/02/Sgp-reply-to-a-JC-frm-SPMHs-Foreign-Interference and https://www.hrw.org/news/2021/10/13/singapore-withdraw-foreign-interference-countermeasures-bill.

Revisions to the Cybersecurity Act

The Minister for Communications & Information signalled the government's intent to review and amend the Cybersecurity Act in March 2022. Specifically, the government will be seeking a review to the definition of critical information infrastructure to potentially adapt the definition to account for virtual assets, such as "systems hosted on the cloud… including those that may not be hosted in Singapore."[595] Industry is concerned that these comments suggest that cloud services would be designated as critical information infrastructure by the government. The Minister also stated an interest in securing "foundational digital infrastructure and services" that are not critical information infrastructure, such as those that form "the backbone of our connectivity, computing and data storage needs." Although a subsequent industry consultation, the Cyber Security Agency of Singapore (CSA) stated cloud services would not be designated as critical information infrastructure, the process is still in development and industry reports concern that the issue could resurface. Given the potential for a wide range of services being included in the government's pursued review of the Cybersecurity Act, the U.S. government should seek to remain engaged with the Singapore government to ensure no discriminatory impacts on U.S. cloud service providers materialize, particularly given the prominence of U.S. firms in the country and Singapore's influence in the region.

JJ. Spain

Taxation of Digital Services

On October 7, 2020, the Senate approved legislation to impose a digital tax of 3 percent of revenue derived from online advertising services, the sale of online advertising, and the sale of user data.[596] 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.[597]

---

[595] Available at https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2022/3/speech-by-mrs-josephine-teo-minister-of-communications-and-information-at-the-ministry-of-communications-and-information-committee-of-supply-debate-on-4-march-2022?pagesize=6&type=Speeches&category=Cyber+Security&page=3

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

[597] 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

KK. 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.[598]

LL. Taiwan

Digital Intermediary Services Act

Taiwan's National Communications Commission (NCC) has been contemplating a content regulation bill in the mould of the EU's Digital Services Act for over a year. On June 29, 2022, the NCC approved a set of proposed rules on this issue, called the Digital Intermediary Service Act—previously released as the Digital Communication Services Act in December—which would impose content moderation requirements on online platforms and internet providers and directly cites the EU's DSA on numerous occasions.[599] The bill—reportedly was set to be applicable to both Taiwanese and foreign companies[600]—would mandate "digital intermediary service providers" to implement a method through which anyone can submit complaints to request the takedown of content and respond quickly to orders to do so; to establish mechanisms to remove illegal content swiftly; to formally showcase that they can remove illegal content quickly; and set up a publicly-accessible database to document each takedown. More stringent requirements are applied to larger firms for risk assessment and management. All digital intermediary service providers would be required to provide the names and contact information of representatives present in Taiwan—foreign firms would be obligated to maintain local representation. The bill received public feedback and public hearings,[601] which eventually resulted in the legislation being pulled after over 99% of the more than 30,000 individuals who commented in the consultation opposed it,[602] and concerns regarding its constitutionality emerged.[603] While the legislation appears to be stalled currently as it has been returned to the

---

Amazon or Glovo, or applications like Facebook, Telegram or WhatsApp - accumulate billions of benefits at the cost of the use of citizenship (online).]).

[598] *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.

[599] Available at: https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&is_history=0&pages=0&sn_f=47684; https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&is_history=0&pages=0&sn_f=46983. *See also* https://www.taipeitimes.com/News/front/archives/2022/06/30/2003780844.

[600] Taiwan Digital Intermediary Service Act, https://www.theregister.com/2022/06/30/taiwan_digital_intermediary_service_act/.

[601] Shelley Shan, *Telecoms Facing Tighter Regulation*, TAIPEI TIMES (Aug. 12, 2022), https://www.taipeitimes.com/News/taiwan/archives/2022/08/12/2003783409.

[602] *Controversial Bill Regulating Internet Put on Hold*, FOCUS ON TAIWAN (Aug. 8, 2022), https://focustaiwan.tw/politics/202208200008.

[603] *Provisions of Digital Services Bill May Be Unconstitutional*, TAIWAN NEWS (Aug. 21, 2022), https://www.taiwannews.com.tw/en/news/4633159.

drafting stage through a task force group,[604] given Taiwan's long-standing interest in enacting DSA-like regulations, industry remains concerned that similar onerous content moderation obligations could be implemented in Taiwan and urge U.S. trade officials to continue monitoring developments.

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. As the Taiwanese government opened and closed a consultation on a white paper on the digital economy in March, it will be important to ensure that the process does not lead to discriminatory treatment of U.S. services.[605]

Ancillary Copyright and New Bargaining Code

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 "very big cross-border" digital platforms.[606] While the Taiwan government has not released any draft, industry is concerned with acknowledgements of Australia and Canada as models for Taiwan to follow and industry is concerned 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. On November 1, 2021, a commissioner at the Fair Trade Commission in Taiwan called for Taiwan to adopt a News Media Bargaining Code similar to that of Australia, although no proposals have yet been drafted.[607]

Restrictions to 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 burdensome approval process imposes unnecessary 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 US cloud services providers.

---

[604] *NCC Halts Drafting of Controversial Online Legislation*, TAIWAN TIMES (Sept. 8, 2022) https://www.taipeitimes.com/News/taiwan/archives/2022/09/08/2003784968.

[605] Available at: https://www.ftc.gov.tw/internet/english/doc/docDetail.aspx?uid=179&docid=16968.

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

[607] Wei Hsin-fang, *Protecting media copyright online*, TAIPEI TIMES (Nov. 1, 2021), https://www.taipeitimes.com/News/editorials/archives/2021/11/01/2003767098

In addition to the Cloud Outsourcing Regulation for financial institutions, the FSC also issued a regulation for insurance firms in December 2019. However, there are still no cloud outsourcing regulations for securities, futures, and investment trust and investment advisory enterprises. Industry reports a lack of clarity for cloud outsourcing regulations that has hindered U.S. cloud service providers' capability to contract with firms in these sectors, who themselves state regulatory uncertainty restricts them from adopting cloud services.

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. Industry reports a growing interest in Taiwan to hold discussions surrounding digital sovereignty in alignment with the policy debates emerging from the European Union.

Restrictions on Over-the-top (OTT) Services

In May 2022, the National Communications Commission approved a proposed framework for its draft of the "Internet Audio-Visual Services Law" which would require large over-the-top providers to register with the government and submit to new obligations.[608] The draft, which represents an updated version of a 2020 proposal away from the previous voluntary approach, include requiring large companies—with the specific size-level definition of "large" to be determined—to establish on-the-ground presence in Taiwan, comply with new reporting obligations, and commitments to produce and/or host local content. Wong Po-tsung, the NCC Deputy Chairman, reportedly affirmed that services hosting user-generated content would not be subject to the rules.[609] The NCC will publish the full draft of the rules after undergoing a review

[608] Available at https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=5306&cate=0&keyword=&is_history=0&pages=0&sn_f=43455; https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&cate=0&keyword=&is_history=0&pages=0&sn_f=47561.

[609] Shelley Shan, *Large OTT TV operators subject to new regulations under NCC's latest draft act*, TAIPEI TIMES (May 26, 2022), https://www.taipeitimes.com/News/taiwan/archives/2022/05/26/2003778837

process. The new rules would present barriers to foreign-based OTT services, including by requiring the disclosure of commercially sensitive data.

MM. 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, which has been leveraged to expand oversight of content and identify millions of posts.[610] The government has also issued emergency decrees in relation to the global pandemic that further restrict online and press freedom.[611]

In 2019, Thailand passed a controversial Cybersecurity Law following amendments in 2018. Industry has criticized the law due to provisions that enable government surveillance.[612] Under the new law, officials are granted authority to "search and seize data and equipment in cases that are deemed issues of national emergency."[613] This could "enable internet traffic monitoring and access to private data, including communications, without a court order."[614]

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 was approved

[610] *Freedom on the Net 2022: Thailand* (2022), https://freedomhouse.org/country/thailand/freedom-net/2022; https://www.nationthailand.com/in-focus/40010570.

[611] *Id.*

[612] *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.").

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

[614] *Id.*

by the cabinet in late October 2021.[615] The Electronic Transactions Development Agency continues to defend its Draft Royal Decree on the Supervision of Digital Platform Services to regulate digital platforms with a broad and heavy brush and has forecast an enforcement date of sometime in 2023.[616]

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

The Personal Data Protection Act went into effect on June 1, 2022, which tracks with some of GDPR, but veers from it in some data transfer regards.[617] The law mostly applies to *all* entities that collect, use, or otherwise share personal data in Thailand or of residents of the country, with no restrictions regarding their own standing under Thai law or where they themselves are incorporated, or even if they operate in Thailand. The extraterritorial nature of the law reflects an obstacle to U.S. online services providers that may even decline to establish a business presence in Thailand but have Thai individuals use their services.[618]

The Thai Office of the Personal Data Protection Committee released draft regulations to dictate rules for transferring personal data outside of Thailand under the PDPA, called the "Notification of the personal data protection committee on rules and principles of appropriate personal data protection for international transfer" in September 2022.[619] The rules governing the export of data from Thailand include a provision that could lead to companies needing to obtain consent from customers if they opt to change business partnerships surrounding the sub-processing of data. If enacted, this could prove restrictive for businesses that would be obligated to wait for

[615] Chattong Sunthorn-opas & Nopparak Yangiam, *Update on Thailand's draft decree to regulate digital platform services*, NAGASHIMA OHNO & TSUNEMATSU (Dec. 21 2021), https://www.lexology.com/library/detail.aspx?g=c944759d-3e49-40eb-8c22-28f80c238715; Threenuch Bunruangthaworn & Archaree Suppakrucha, *Thailand's Attempt at Regulating Digital Platforms*, ZICO LAW THAILAND (June 6, 2022), https://www.zicolaw.com/resources/alerts/thailands-attempt-at-regulating-digital-platforms/.

[616] Suchit Leesa-Nguansuk, *ETDA defends royal decree regulating digital platforms*, BANGKOK POST (Mar. 17, 2022), https://www.bangkokpost.com/tech/2280351/etda-defends-royal-decree-regulating-digital-platforms

[617] Janine Phakdeetham, *Explainer: What is PDPA, Thailand's new data law?*, BANGKOK POST (June 1, 2022), https://www.bangkokpost.com/business/2319054/explainer-what-is-pdpa-thailands-new-data-law-; Svasvadi Anumanrajdhon, Vunnipa Ruamrangsri, & Vilaiporn Taweelappontong, *Thailand's Personal Data Protection Act (PDPA): are companies in Thailand ready?*, PWC THAILAND, https://www.pwc.com/th/en/tax/personal-data-protection-act.html (last accessed Oct. 28, 2022); HUNTON ANDREWS KURTH, *Thailand's Personal Data Protection Act Enters into Force* (June 1, 2022), https://www.huntonprivacyblog.com/2022/06/01/thailands-personal-data-protection-act-enters-into-force/.

[618] DLA PIPER, *Data Protection Laws of the World: Thailand*, https://www.dlapiperdataprotection.com/index.html?t=law&c=TH.

[619] Available at: https://www.mdes.go.th/uploads/tinymce/source/%E0%B8%AA%E0%B8%84%E0%B8%AA/%E0%B8%A3%E0%B9%88%E0%B8%B2%E0%B8%87%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%81%E0%B8%B2%E0%B8%A8%E0%B8%AF%20%E0%B8%81%E0%B8%B3%E0%B8%AB%E0%B8%99%E0%B8%94%E0%B8%AB%E0%B8%A5%E0%B8%B1%E0%B8%81%E0%B9%80%E0%B8%81%E0%B8%93%E0%B8%91%E0%B9%8C%E0%B9%81%E0%B8%A5%E0%B8%B0%E0%B8%99%E0%B9%82%E0%B8%A2%E0%B8%9A%E0%B8%B2%E0%B8%A2%E0%B9%82%E0%B8%AD%E0%B8%99%E0%B9%84%E0%B8%9B%E0%B8%95%E0%B9%88%E0%B8%B2%E0%B8%87%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B9%80%E0%B8%97%E0%B8%A8.pdf.

consent from each of its customers in Thailand to approve what is usually seen as a standard business decision requiring swift movement.

NN. 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.[620] CCIA has previously identified laws that preemptively block websites on vague grounds, and specific instances of blocking by Turkish authorities.[621] The aggressive treatment of Turkey's government to U.S. digital services imposes economic harms—the U.S. International Trade Commission report estimated that $14.6 million was lost in Turkey after it blocked several U.S. services in early 2020.[622]

In recent years, the market conditions have worsened. 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" [623]) in July 2020 that grants the government sweeping new powers to regulate content on social media.[624] The law went into effect October 1, 2020, and authorities were quick to take action against U.S. firms, imposing fines,[625] advertising bans, and bandwidth restrictions within months.[626] 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.

---

[620] *Freedom on the Net 2022: Turkey* (2022), https://freedomhouse.org/country/turkey/freedom-net/2022.

[621] 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://rsf.org/en/turkey-enemy-internet; *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.

[622] USITC, Foreign Censorship Part 2, *supra* note 32 at 74

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

[624] *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.

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

[626] *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.

Turkey continued its trend of digital censorship policies in late May 2022 with the introduction of a draft of a "disinformation bill" dubbed the "Law Proposal on the Amendment of the Press Law and Some Laws" aimed to clamp down on disinformation proliferated online, but which fails to include robust legal definitions for the terms such as "disinformation", "fake news", "baseless information", and "distorted information" that underpin the rules.[627] The bill includes additional obligations for online services providers and platforms as well as the restrictions on free expression. The Turkish parliament passed the bill in October 2022.

The justification for the proposal takes specific aim at "bad" aspects of social media, as it states, "the use of social media increases in parallel with the internet facilitating and accelerating access to news and information" as a reason that the bill is needed. The Chair of the Digital Platforms Commission in Parliament and a high-ranking official of the ruling Justice and Development Party cited laws and regulations targeting fake news and disinformation in Germany, France, and the United States, but opponents have pointed to the March "anti-fake news" law passed in Russia as a similar framework for Turkey's disinformation bill.[628]

The law will require platforms to disclose their algorithms and the personal information of users to the government upon demand. The bill would criminalize the act of "distributing deceptive information publicly"; expand a 2020 social media law to require representatives of foreign social network providers to reside in Turkey; establish a prison sentence of one to three years for those responsible for spreading false information regarding the "internal and external security of the country, public order and public health" in a way that is "convenient to disrupt public peace" with longer sentences if the identity of the posting individual is hidden; expand reporting requirements for social network providers for information related to content deemed potentially illegal by the government, algorithms, data processing methods, and corporate organization; and empower the government with the ability to levy fines on, impose bans on advertising for, and throttle the bandwidth of media firms.[629]

Given the weaponization of purported national security and public order needs to undermine dissent in Turkey and the politicized judiciary in the country, opponents of the bill have warned that the "law would become another tool for harassing journalists and activists and may cause blanket self-censorship across the Internet" and could be the "last nail in the coffin of an independent media."[630] The legislation is pending in the Turkish legislature, which is controlled by the two parties which introduced the bill.

---

[627] Available at https://www.tbmm.gov.tr/Yasama/KanunTeklifi/316898. *See also AKP MHP Proposes Amendment to Press Law Introducing Prison Sentences for Disinformation*, BIANET (May 27, 2022), https://m.bianet.org/english/freedom-of-expression/262461-akp-mhp-propose-amendment-to-press-law-introducing-prison-sentences-for-disinformation.

[628] *New Disinformation Law Will Be Soon Announced, Turkish Official Says*, DAILY SABAH (Apr. 17, 2022), https://www.dailysabah.com/politics/legislation/new-disinformation-law-will-be-soon-announced-turkish-official-says.

[629] *Law Proposal Amending the Press Law and Further Laws Has Been Published*, MONDAQ (June 7, 2022), https://www.mondaq.com/turkey/compliance/1199264/law-proposal-amending-the-press-law-and-further-laws-has-been-published.

[630] *Turkey's 'Disinformation' Law Will Devastate Media Freedom, Experts Predict*, BALKAN INSIGHT (July 1, 2022), https://balkaninsight.com/2022/07/01/turkeys-disinformation-law-will-devastate-media-freedom-experts-predict/.

Additional restrictions apply to larger providers—for social media providers with over 1 million daily users in Turkey, their local representative will be obligated to be a resident of Turkey as well as a Turkish citizen, which is already required. Further, for social media providers with over 10 million daily users in Turkey, the legal entity representatives will be mandated to be a branch of a capital company.[631] If authorities demand certain information and the firm fails to disclose it, the bill proposes a punishment of throttling service to that platform by 90% of usual bandwidth.

The bill would also give authority to the Information Technologies and Communications Authority (ICTA) to regulate over-the-top communications providers, which were previously not the subject of a specific law. This could render OTT communications providers responsible for informing ICTA the number of active individual and business users in the country, the volume and length of voice calls, the volume and active time of video calls, the volume of instant messages, and other data which ICTA would have broad authority to determine along with the speed with which these disclosures would need to occur. OTT communications providers would further have to adhere to forthcoming regulations established by ICTA. Failure to comply could result in fines rising to 30 million Turkish Liras ($1.6 million) and if that fine is not paid in the time ICTA dictates while regulatory requirements are not met by the provider, ICTA has the power to throttle service to that provider to a level rising up to 95% restriction on the usual bandwidth capacity or outright block the service.[632]

Taxation of Digital Services

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.[633] 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".[634] 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.[635] In November 2021, Turkey struck a

[631] *Proposal for Amendment of Press Law*, LEXOLOGY (July 15, 2022), https://www.lexology.com/commentary/tech-data-telecoms-media/turkey/zdastanli-ekici-attorney-partnership/proposal-for-amendment-of-press-law.

[632] *New Regulations Expected for OTT Service Providers* (July 2022), https://gun.av.tr/insights/articles/new-regulations-expected-for-ott-service-providers.

[633] 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.

[634] Turkey Revenue Administration, Digital Service Tax Office, https://digitalservice.gib.gov.tr/kdv3_side/maindst.jsp?token=d1078f5e3dc646b78d5d4e5842f21e97feb48d366bc76 17458b6679dec12675154a01fccc42292bb04d926bc259dbc75e39dd8e202535fd70a7098396c74a6f7&lang=en.

[635] *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.

deal with the United States on DSTs prior to the implementation of the OECD Framework, but given the rise of this policy globally, industry remains concerned about its potential re-emergence.[636]

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.[637] 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.[638] The Regulation establishes a framework for use of cloud services as an outsourced service, but only applies for services located in Turkey.[639]

The Law on the Protection of Personal Data (numbered 6698) governs international transfer of data, which is permitted under the following conditions: (1) when transferring personal data to a country with adequate level of protection, (2) obtaining explicit consent of data subjects, or (3) ad-hoc approval of the Data Protection Board to the undertaking agreement to be executed among data transferring parties.[640] 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.

Additional E-Commerce Regulations

A new set of e-commerce regulations in a law dubbed the Law on Amending the Law on Regulation of Electronic Commerce was adopted in July 2022 and will go into effect on January 1, 2023.[641] Firms that facilitate sales equalling or topping ten billion Turkish lira net ($538.3

[636] OFFICE OF THE U.S. TRADE REP., USTR Welcomes Agreement with Turkey on Digital Services Taxes (Nov. 22, 2021), https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/november/ustr-welcomes-agreement-turkey-digital-services-taxes.

[637] *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.

[638] *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.

[639] *Id*.

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

[641] *New Law Amending the Law on the Regulation of Electronic Commerce in Turkey (*Aug. 5, 2022), https://www.mondaq.com/turkey/contracts-and-commercial-law/1218860/new-law-amending-the-law-on-the-regulation-of-electronic-commerce-in-turkey-a-brief-introduction; https://www.srp-legal.com/2022/07/22/the-law-amending-the-law-on-the-regulation-of-electronic-commerce-has-been-published-in-the-official-gazette/.

million) annually and over one hundred thousand executed transactions will be required to obtain a license to operate in the country and renew that license when the Ministry of Commerce dictates. Further, the law requires a restriction on e-commerce providers selling goods of their own brand or brands with which they have economic associations.[642] E-commerce providers will also be subject to obligations to take down illegal content and ads, ensuring information is correct, obtaining consent before using brands for promotions, and refraining from anticompetitive practices. For firms with a net transaction of over 60 billion liras ($3.3 billion), there are a host of other restrictions regarding banking, transportation, and delivery.

OO. 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. The law imposes licensing requirements 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". Such onerous licensing requirements covering a broad scope of social influencing activities add unnecessary friction to digital trade and inhibit new social 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, it could be enforced on a highly selective basis to target certain influencers at will.

Blocking of OTT Communications Providers

The UAE's Telecommunications Regulatory Authority has historically blocked the over-the-top communications services of Apple's FaceTime and Meta's WhatsApp. Although the services briefly began to work again with no explanation from the government in October 2021,[643] these restrictions have reappeared for video and voice calls.[644]

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

A new GDPR-style Personal Data Protection Law went into effect in January 2022 and will be enforced beginning November 2022.[645] The is extraterritorial in scope and envelopes data

---

[642] *New Era In Turkey's E-Commerce Market*, LEXOLOGY (July 8, 2022), https://www.lexology.com/library/detail.aspx?g=4e0f3279-d48c-4f2e-a0e1-752e9a7abfb8 ("As such, if these goods are offered for sale in different electronic mediums, providing access between such is not permitted. However, this regulation will not apply if the brand owner's revenue from e-commerce is less than half of its total sales revenue, or if the platform in question solely offers items carrying the Intermediary's brand in the form of agency contracts or franchising. Moreover, periodic publications, books and e-readers are also exempt from this regulation.").

[643] *Long-Banned FaceTime Call Apparently Working in UAE*, AP NEWS (Oct. 10, 2021), https://apnews.com/article/dubai-middle-east-united-arab-emirates-eb2461eda153f3bc6ec281e7d1039db9.

[644] *How to Get Around WhatsApp Ban in Dubai* (Feb. 13, 2022), https://www.cloudwards.net/whatsapp-ban-in-dubai/.

[645] *Personal Data Protection Law Coming Into Force in January 2022*, CONNECT ON TECH (Dec. 13, 2021), https://www.connectontech.com/uae-personal-data-protection-law-coming-into-force-on-2-january-2022/;

controllers and data processors outside the UAE that happen to process UAE individuals' data. Personal data transfers abroad are permitted if the Data Office has approved that country for having an adequate level of protection. Transfers to countries not on this list are possible through user consent and contracts, among other options.

PP. United Kingdom

As the U.S. looks to negotiate with the UK following its exit from the EU, it should consider a number of regulations and policies that deter U.S. digital exports.[646]

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.[647] The proposal not only had trade implications, but also free expression concerns, to the extent these rules would conflict with U.S. law. The UK Office of Communications also released a report on regulating online platforms to address online harms, all of which served as a basis for the work that has since come in this effort.[648]

In December 2020, the UK government released its response to the Online Harms consultation.[649] 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 the upcoming legislation will establish different categories of content and activity on platform services, then attribute different duties to each.

In March 2022, the UK government released a new version of the "Online Safety Bill" aimed at imposing new obligations for online platforms to police and remove illegal content with a focus on content "relating to terrorism and child sexual exploitation and abuse."[650] The bill would compel the "biggest and most popular social media platforms," search engine providers,

---

New UAE Federal Data Protection Law, NATIONAL LAW REVIEW (Feb. 10, 2022), https://www.natlawreview.com/article/new-uae-federal-data-protection-law.

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

[647] 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.

[648] 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.

[649] Online Harms White Paper: Full government response to the consultation (Dec. 15, 2020), https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response.

[650] Policy Paper: Online Safety Bill Factsheet (Apr. 2022), https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet.

messaging services, cloud storage providers, and other content platforms to implement "proactive technologies" to scan for the presence of illegal content and to ensure children are not exposed to it; adopt "highly accurate technology" to scan private messaging services; provide assurances that children do not see "harmful disinformation" and remove "illegal disinformation" for all users; tackle anonymous accounts in the context of spreading hate speech; as well as a litany of other provisions with the potential to undermine freedom of speech and encryption through vague definitions for pertinent harms covered by the bill and broad-sweeping calls for real-time monitoring of harmful content.[651]

In early July 2022, the UK government announced an amendment to the Online Safety Bill to add obligations for social media providers to "proactively look for and remove disinformation from foreign state actors which harms the UK," with the threat of hefty monetary or blocking punishments if not adequately implemented.[652] Companies that fail to adhere to the rules would be punished through fines—the higher figure between £18m or 10% of their yearly turnover worldwide or the potential blocking of their services in the UK.

The Public Bill Committee finished receiving and incorporating feedback on June 8, 2022, and was set to begin the stage for its report and third reading starting on July 12, 2022.

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.[653] The U.S. should push back against the tax as part of the negotiations for a U.S.-UK free trade agreement.

---

[651] *The UK's Online Safety Bill Undermines Encryption and Anonymity*, CENTER FOR DATA INNOVATION (May 26, 2022), https://datainnovation.org/2022/05/the-uks-online-safety-bill-undermines-encryption-and-anonymity/; *Online Safety Bill Is a Serious Threat to Human Rights*, ARTICLE 19 (Apr. 25, 2022), https://www.article19.org/resources/uk-online-safety-bill-serious-threat-to-human-rights-online/

[652] Press Release, Internet Safety Laws Strengthened to Fight Disinformation, July 5, 2022, https://www.gov.uk/government/news/internet-safety-laws-strengthened-to-fight-russian-and-hostile-state-disinformation.

[653] 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*

Backdoor Access to Secure Technologies

The UK has pursued policies that undermine secured communications by mandating law enforcement access to encrypted communications. Passed in 2016, the Investigatory Powers Act allows for authorities to require removal of "electronic protections" applied to communications data.[654] The UK also recently joined the United States and Australia in a concerning request to Facebook regarding undermining the security of user communications.[655]

The UK government executed an orchestrated campaign against the introduction of end-to-end encryption on one service, called "No Place to Hide", starting in January 2022.[656] The government's £534,000 ($724,000) effort sought to condemn the decision to provide end-to-end encryption and link it to personal and national security. Government efforts to target digital security in this manner are damaging to U.S. digital exports and the future of online communications.[657]

Restrictions on Cross-Border Data Flows

The EU's General Data Protection Regulation (GDPR) went into effect in 2020, 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.[658] The UK initially signaled intent to maintain GDPR compliance following Brexit, as expected pursuant to the EU Withdrawal Act (2018),[659] but the future of data transfers remains up in the air.

In June 2022, the UK government announced the contours of what will eventually become the Data Reform Bill that would move certain privacy rules away from those of the EU's General Data Protection Regulation in an effort to "harness the power of data to help British businesses trade abroad, boost the UK's position as a science and technology superpower, and improve

---

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.").

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

[655] 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/.

[656] *UK Gov't Plans Publicity Blitz to Undermine Privacy of Your Chats*, ROLLING STONE (Jan. 16, 2022), https://www.rollingstone.com/culture/culture-news/revealed-uk-government-publicity-blitz-to-undermine-privacy-encryption-1285453/.

[657] *UK Paid $724,000 for A Creepy Campaign to Convince People Encryption is Bad*, EFF (Jan. 21, 2022), https://www.eff.org/deeplinks/2022/01/uk-paid-724000-creepy-campaign-convince-people-encryption-bad-it-wont-work.

[658] *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.

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

people's everyday lives."[660] The bill would eliminate the UK GDPR's obligations such as small businesses needing to hire a Data Protection Officer and implement impact assessments; shift the existing requirements for cookies to be opt-out instead of opt-in; empower the UK government's International Data Transfer Expert Council to eliminate barriers to cross-border data flows in an effort to improve digital trade; and implement a series of reorientations of the UK's Information Commissioner's Office. The outline of the bill came in the form of a final response to a consultation conducted in the fall aimed at reforming data protection after the EU provided the UK with the "adequacy" determinations needed for data flows between the two entities.[661]

In July 2022, the effort advanced with the introduction of the "Data Protection and Digital Information Bill."[662] The direction of this bill is under public debate in the UK.

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 of its customers equally. Furthermore, the regulator is legally required to carry out detailed market reviews regularly and to impose regulatory remedies where the biggest national operator is found to have significant market power.

Regulation of Digital Markets

In June 2022, the UK's Competition and Markets Authority (CMA) published a final report recommending a market investigation and possible regulatory interventions to address findings of market power of Apple and Google for mobile browsers and cloud gaming.[663] The report suggests that interventions would be necessary, as in the absence of action "both companies are likely to maintain, and even strengthen, their grip over the sector, further restricting competition and limiting incentives for innovators." The CMA previously investigated digital advertising platforms,[664] is currently investigating the music and streaming[665], and is expected to soon open an investigation into the e-commerce sector. The UK's telecoms regulator OFCOM has also

[660] Press Release, New Data Laws to Boost British Business, Protect Consumers, (June 17, 2022), https://www.gov.uk/government/news/new-data-laws-to-boost-british-business-protect-consumers-and-seize-the-benefits-of-brexit.

[661] DEP'T FOR DIGITAL, CULTURE, MEDIA & SPORT, Consultation Outcome Data: A New Direction, https://www.gov.uk/government/consultations/data-a-new-direction.

[662] Data Protection and Digital Information Bill, https://publications.parliament.uk/pa/bills/cbill/58-03/0143/220143.pdf; https://bills.parliament.uk/bills/3322.

[663] Press Release, CMA Plans Market Investigation Into Mobile Browsers and Cloud Computing (June 10, 2022), https://www.gov.uk/government/news/cma-plans-market-investigation-into-mobile-browsers-and-cloud-gaming.

[664] Online Platforms and Digital Advertising Market Study (2020), https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

[665] Music and Streaming Market Study (2022) https://www.gov.uk/cma-cases/music-and-streaming-market-study

recently announced the launch of a market study examining the position of Amazon, Microsoft and Google in the UK's £15bn cloud services market.[666]

Previous UK market studies and competition reports have led to a consultation on the creation of a Digital Markets Unit and sector-specific ex-ante regulation of digital platforms deemed to have strategic market status. Prior to former Prime Minister Boris Johnson's resignation, the UK Government had planned to introduce a draft of this legislation in the coming legislative year,[667] and it had responded to a consultation setting out detailed plans for what the legislation would look like.[668] While the previous UK Government had indicated it would be somewhat lighter touch than the EU's Digital Markets Act, it would broadly follow the same objectives, and function similarly to the new EU and German market-based regulations, designating a handful of leading U.S. technology companies as falling within its scope, and making it more difficult for them to engage in pro-competitive conduct otherwise available to their competitors.

QQ. Vietnam

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

Vietnam remains a country of concern for industry as it continues to pursue localization measures. The Law on Cybersecurity took effect January 1, 2019. The law is expansive and includes both data localization mandates and content regulations. Under the law, covered service providers are required to store personal data of Vietnamese end users, data created by users, and data regarding the relationships of a user within the country for a certain period of time.

On Aug. 15, 2022, the Vietnamese government issued Decree No. 53/2022/ND-CP which added detail to several of the articles under the original Law on Cybersecurity regarding local data storage and went into effect on October 1, 2022, with no adjustment period.[669] The Decree was issued without prior notice or consultation by Vietnam. The Decree includes potential conflations with the Law including on localization requirements for domestic and foreign companies; a failure to delineate between domestic companies and Vietnamese companies, rendering foreign companies forced to incorporate locally are included; a lack of clarity regarding whether data needs to be kept in Vietnam or whether a copy suffices; and other issues implicating provisions of the Law and other laws regarding data localization, local representation, and data processing.[670] The Law on Cybersecurity could be in conflict with the Comprehensive and Progressive Agreement for Trans-Pacific Partnership—implicating

[666] Ofcom, Ofcom To Probe Cloud, Messenger, and Smart-Device Markets (Sept. 22, 2022), https://www.ofcom.org.uk/news-centre/2022/ofcom-to-probe-cloud,-messenger-and-smart-device-markets.

[667] Queen's Speech 2022, https://www.gov.uk/government/topical-events/queens-speech-2022.

[668] Consultation Outcome, A New Pro-Competitive Regime for Digital Markets (May 6, 2022), https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets/outcome/a-new-pro-competition-regime-for-digital-markets-government-response-to-consultation.

[669] Available at: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Decree-53-2022-ND-CP-elaborating-the-Law-on-cybersecurity-of-Vietnam-527750.aspx. *See also* Foreign Firms Required to Store Use Data in Vietnam, https://english.mic.gov.vn/Pages/TinTuc/154653/Foreign-firms-required-to-store-users--data-in-Viet-Nam.html; https://rouse.com/insights/news/2022/vietnam-cybersecurity-law-decree-issued.

[670] Joint Industry Letter on Law on Cybersecurity (Sept. 9, 2022), https://aicasia.org/wp-content/uploads/2022/09/Industry-Letter-Regarding-Decree-53-LOCS.pdf.

companies that are incorporated in CPTPP member countries that do business in Vietnam—although Vietnam secured Side Letter agreements for countries in the agreement would not pursue charges of violations for five years following the entry of force of the CPTPP for Vietnam.[671]Notwithstanding this moratorium on enforcement, Vietnam remains legally bound by these obligations.

The Vietnamese government is working on a Personal Data Protection Decree (PDP), but there are concerns of localization requirements based on the current draft.[672] The current draft prescribes conditions that a personal data processor must fully satisfy with regard to 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% of total revenue. 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.

In February 2022, the Vietnamese Government held a policy discussion with business representatives on the subject of supply chains in which industry voiced concerns about Vietnam's data localization requirements. In response, the Ministry of Public Security has issued Official Letter No. 470/BCA-ANKT which stated that firms could import and export data without data localization requirements if they implement data security measures aligned with international standards and Vietnam's rules.[673] The details of the Draft PDP Decree will prove essential to the details of this policy.

In March 2022, the Vietnamese Government issued a resolution to approve the Personal Data Protection Decree.[674] A final version of the Draft PDP Decree for Government submission was due in May 2022 for enactment; however, the approved version of the draft remains undisclosed. The initial Draft PDP Decree was released for public comments in February 2021, which received feedback on its requirements for sensitive data procession, cross-border data transfers, and data localization. The feedback on these regulations is expected to have been implemented in the approved version.

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

[671] Id.

[672] DLA PIPER, *Data Protection Laws of the World: Vietnam*, https://www.dlapiperdataprotection.com/index.html?t=law&c=VN.

[673] *Vietnam Updates on Data Localization Requirement*, CONNECT ON TECH (Mar. 15, 2022) https://www.connectontech.com/vietnam-update-on-data-localization-requirement-cross-border-data-flow/.

[674] *Vietnam's Personal Data Protection Decree*, ROUSE (Mar. 10, 2022), https://rouse.com/insights/news/2022/vietnam-s-personal-data-protection-decree-recent-developments-and-what-to-expect.

regarding the user. "Prohibited" content includes content that is critical or disparaging of the Vietnamese government. Companies have already been fined under this provision.[675]

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 the country if the U.S. firm did not censor certain political content on its platform at the request of the government.[676]

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

On August 19, 2020, the Ministry of Information and Communications released a draft Decree to amend the Decree 181/2013 Decree on Elaboration of some Articles on the Law on Advertising.[677] The draft rules would regulate advertising content, and expanded the scope of these rules to applications and social media. As drafted, the Decree (1) lacks clarity on definitions, procedures and restrictions, (2) imposes onerous reporting requirements, and (3) obligates providers to actively manage ad content and placement. Revisions are needed to remove clauses to avoid confusion and prevent overlapping liability and duplication.[678]

In July 2021, the Vietnamese government proposed amendments to the Ministry of Information and Communication Decree 72/2013. Numerous new restrictions were proposed, including requiring all foreign enterprises providing cross-border services with over 100,000 Vietnamese unique visitor access per month to 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. Further, these data localization measures were extended to include data centers and cloud services providers. Requirements for content removal and the development of methods to report content-related violations of domestic laws

[675] *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/vietnam-quick-to-enforce-new-cybersecurity-law/.

[676] *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.

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

[678] For example, takedown requests and tax obligations should only be regulated pursuant to Decree 72 and relevant tax laws.

and policies are also onerous and sweeping, especially in light of 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). 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 law also includes social media services providers for promotional and other sales-adjacent operations. The Decree will come into effect from 1 January 2022.[679]

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.[680] 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.[681] 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.[682] While these standards are technically voluntary, in practice, these standards are expected to be adopted by the Vietnamese public sector.

Decree 53 on the Law on Cybersecurity, issued by the Ministry of Public Security, went into effect on October 1, 2022. Industry reports that the Law's provisions hinder the ability of cloud service providers to operate and prevent full market access to the technology and security choices that are typically afforded to firms through a competitive cloud marketplace.

---

[679] *Vietnam Taxation of E-Commerce and Digital-Based Transaction*, KPMG (Oct. 15, 2021), https://home.kpmg/us/en/home/insights/2021/10/tnf-vietnam-taxation-ecommerce-digital-based-transactions.html; *Vietnam Passes Regulation on E-Commerce: Decree 85*, VIETNAM BRIEFING (Oct. 12, 2021), https://www.vietnam-briefing.com/news/vietnams-passes-regulation-e-commerce-decree-85.html/.

[680] Available at https://vanbanphapluat.co/decision-749-qd-ttg-2020-introducing-program-for-national-digital-transformation.

[681] *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.

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

Taxation of Digital Services

The Tax Administration Law, effective July 1, 2020, taxes cross-border e-commerce and other digital services.[683] The Ministry of Finance issued Circular 80[684] 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.

Import License Requirement Restrictions

Industry reports concern over mandates from Vietnam's Government Cipher Committee that any product imported or exported from the country with cryptographic functionality must first receive permits and licenses to do so. Entities importing or exporting IT products with capabilities of data encryption are obligated to seek a Cryptography Trading License as well as a Cryptography Import License. Industry reports onerously long waiting times—six months—for such licenses to be granted. The government mandates companies seeking these licenses provide detailed product information, specific technical plans, details of the cryptographic function of the product, local employees' information, and other details as part of the application. Firms frequently face delays due to these requirements and industry reports inconsistent application of the government's approval processes and these license requirements and the application of arbitrary rules restrict foreign firms operating in Vietnam from importing necessary hardware for their goods and services.

IV. CONCLUSION

As the global Internet continues to grow and becomes even more tightly intertwined with international commerce, CCIA is concerned that digital trade barriers like those discussed above will continue to proliferate. Identifying and addressing these barriers is crucial to ensure that the Internet continues to be a positive driver of the U.S. economy and a force for 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.

[683] *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/.

[684] *See* 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.