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

In re Request for Comments on Significant Foreign Trade Barriers for the 2024 National Trade Estimate Report	Docket No. USTR–2023–0010

COMMENTS OF THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION REGARDING FOREIGN TRADE BARRIERS TO U.S. EXPORTS FOR 2024 REPORTING

October 23, 2023

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 88 Fed. Reg. 62,421 (Sept. 11, 2023), 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 over 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 encourages USTR's to renew focus and enforce 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. 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 COVID-19 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 delivering a hefty digital trade surplus of $256 billion for the United States in 2022.

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 ill-defined public policy concerns, many countries are adopting discriminatory policies that disadvantage, and often target, U.S. technology companies.

Unfortunately, some foreign governments are also increasingly overt in their efforts to discriminate against U.S. enterprises with a stated goal of supporting domestic rivals. 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.

---

[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.

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 continued work on 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, and the U.S.-Kenya Strategic Trade and Investment Partnership over the past year. CCIA urges USTR and the U.S. government writ large to use these initiatives to promote the digital economy and establish strong, enforceable protections for U.S. exporters and prevent emerging trade barriers. This can be achieved through 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 not only for digital goods and services providers but the U.S. economy overall that also relies on internet-enabled resources and tools to reach foreign markets.

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; (2) data and infrastructure localization mandates and restrictions on cloud services; (3) government-imposed restrictions on internet content and related access barriers; (4) taxation of digital products and services; (5) experimental platform regulation; (6) copyright liability regimes for online intermediaries; (7) forced revenue transfers in digital news; (8) imposing legacy telecommunications rules on internet-enabled services; and (9) threats to encryption and the security of devices. 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.

The real gross output of the digital economy in the U.S. grew at an annual rate of 5.6% between 2016 and 2021, much faster than the overall economy's growth rate of 1.9 % over the same period.[3] According to U.S. Department of Commerce estimates, the digital economy generated $2.41 trillion of value added to U.S. GDP, or 10.3% of total U.S. GDP. The digital economy accounts for 8 million jobs, which generated $1.24 trillion in total compensation, with the average annual wage consistently increasing from 2006 ($85,595) to 2021 ($154,427). 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 and the global competitiveness of the U.S. economy generally.[4] The United States generated almost $626 billion globally Potentially ICT-Enabled Services in 2022, with a trade surplus of $256 billion.[5] Digitally-deliverable services are an essential part of U.S. export strength, as they represented 67% of *all* U.S. services exports in 2022.[6] For at least the last 15 years, digitally-enabled services exports have made up more than half of all U.S. services exports, a majority that skyrocketed to 75% in 2021. U.S. services trade overall reflects an area of historic strength for the economy—the United States has held a strong surplus in recent years. As such, the fact that digital services represent a majority of overall services trade reflects its importance to U.S. economic strength, competitiveness, and national security.[7]

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.[8] One firm estimated that the larger technology

---

[3] BUREAU OF ECONOMIC ANALYSIS, *New and Revised Statistics of the U.S. Digital Economy, 2005–2021* (Nov. 2022), https://www.bea.gov/system/files/2022-11/new-and-revised-statistics-of-the-us-digital-economy-2005-2021.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 Potentially-ICT Services, https://apps.bea.gov/iTable/?reqid=62&step=9&isuri=1&product=4#eyJhcHBpZCI6NjIsInN0ZXBzIjpbMSw5LDZdLCJkYXRhIjpbWyJwcm9kdWN0IiwiNCJdLFsiVGFibGVMaXN0IiwiMzU5Il1dfQ==.

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

[7] https://www.project-disco.org/uncategorized/strength-of-digital-services-exports-to-u-s-economy/.

[8] 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.

companies earn 58% of their revenue abroad.[9] Broadly speaking, foreign markets represent a key area for growth for small businesses—the U.S. Census Bureau has estimated that 97.4% of the more than 277,000 U.S. companies that exported goods in 2021 were small and medium-sized enterprises (SMEs), which in turn contributed 34.6% of the country's $1.5 trillion reported revenue from goods exports.[10] In the digital space, the benefits to small businesses of being able to export, and the impact of restrictions, are clear—for example, restrictive data transfer requirements or a requirement to use local data centers (two sets of restrictions that trade rules seek to reasonably constrain absent genuine security concerns) might represent costs that a large company would be able to absorb as the cost of doing business. However, the expensive nature of either complying with difficult data transfer requirements or being forced to construct costly data centers in every jurisdiction of doing business could be economically infeasible for a smaller company. Further, the fact that the United States does not impose such restrictions means that when foreign countries implement such restrictions (against whom U.S. companies of all sizes compete), it puts all U.S. firms and their workers at a distinct competitive disadvantage.

This was made more apparent during the global pandemic, the lingering effect of which continues to impact 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.[11] The Department of Commerce recently detailed in its 2023 National Export Strategy how the rise in prominence of digital trade has coincided with benefits for a broad swath of U.S. exporters, particularly when the world ground to a halt during the COVID-19 pandemic.[12]

International markets continue to present the most significant growth opportunities for U.S. companies that are both large and small, 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.

---

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

[10] https://www.trade.gov/press-release/international-trade-administration-and-amazon-launch-new-initiative-boost-export.

[11] *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.

[12] https://www.trade.gov/sites/default/files/2023-06/National-Export-Strategy-2023.pdf ("With the emergence of digital trade and e-commerce, artisans, entrepreneurs, app developers, freelancers, and small businesses participated directly in the global marketplace in ways that were previously impossible, and at a time when the rest of the world is also increasingly digitalizing. As global travel was disrupted, digital approaches to finding customers became the norm, and deals could be struck via video conference, leveling the playing field for U.S. small business exporters who lacked the time and resources for international travel.").

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.

It is no longer just 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.[13] In its 2023 *Freedom on the Net* report, Freedom House highlighted how attacks on free expression online "grew more common" globally, with 66 % living in countries where "websites hosting political, social, or religious content were blocked," and 46 % living in countries where "authorities disconnected internet or mobile networks, often for political reasons."[14] In its most recent report, Freedom House opined further on democratic governments' use of social media and internet blockages and censorship, noting that "states that have long been defenders of internet freedom imposed censorship or flirted with proposals to do so, an unhelpful response to genuine threats of foreign interference, disinformation, and harassment."[15] 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. The European Union continues to advance restrictive policies including its European Cybersecurity Certification Scheme for Cloud Services and the Data Act.

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.

---

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

[14] FREEDOM HOUSE, *Freedom on the Net 2023*, https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf [hereinafter "Freedom on the Net 2023"].

[15] *Freedom on the Net 2023, supra* note 14.

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 2023 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

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 $3.94 trillion in 2022.[16] 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.[17] These restrictions take the form of unclear privacy rules and burdensome requirements for the export of data or processing of data abroad divorced from data security protocols.

Given the reliance of other industries on the cross-border flow of data in the modern economy, all services suppliers operating in a foreign market rely to some extent on the ability to transfer data to and from that jurisdiction, benefitting from the free and open flow of information powered by digital trade agreements. Cross-border data flows lead to an increase in overall exports and an estimated 82% decrease in export costs for small and medium enterprises.[18] As a consequence, restricting the flow of data internationally is associated with damage to the national GDP and its ability to attract investment. The World Bank has noted that obstacles to data flows have "large negative consequences on the productivity of local companies using digital technologies and especially on trade in services."[19]

An OECD study released in May 2023 illustrates the impact digital connectivity and trade has for other sectors of both high-income and emerging economies by reviewing regional trade

---

[16] 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).

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

[18] https://globaldataalliance.org/wp-content/uploads/2023/07/07192023gdaindex.pdf.

[19] https://www.worldbank.org/en/publication/wdr2020.

agreements that contain e-commerce chapters and those without such provisions.[20] The OECD report found that agreements with e-commerce provisions were correlated with increases exports of high-income countries by 10.3%, which represents double that of agreements without e-commerce commitments, while exports of emerging economies was correlated with a 16.9% increase (although the detail and strength of the chapter was found to play a significant role in the effect on overall trade). The OECD report notes, digital connectivity has an effect "across all sectors of the economy, but it is most important for digitally-deliverable sectors."[21] The report notes that digitalization is "key for agriculture and food sectors."[22]

Insofar as privacy rules disadvantage foreign digital firms' ability to operate in the market, such rules can impose a barrier to entry for U.S. companies, particularly smaller and medium-sized businesses seeking to expand to foreign markets. Industry reports concerns about these obstacles to cross-border data flows that hinder the global nature of the internet and, in turn, digital services providers' operations.

B. Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

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.[23] Governments often cite domestic privacy protections, defense against foreign espionage, law enforcement access needs, and local development as motivations for 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.[24] 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.[25]

---

[20] https://www.oecd-ilibrary.org/docserver/11889f2a-en.pdf?expires=1689867389&id=id&accname=guest&checksum=5F2AA0C17DA28F354ECB65582A8A8CBA.

[21] *Id.*

[22] *Id*.

[23] 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.

[24] 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.

[25] 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.

Rather than promote domestic industry, data localization policies are likely to hinder economic development and restrict domestic economic activity,[26] and impede global competitiveness.[27] Reports have shown that data localization laws distinctly harm the economic output of the countries that adopt such policies, while also increasing the costs exponentially for both complying companies and their consumers.[28]

Further, foreign jurisdictions adopting data localization rules actively harms U.S. workers and economic interests. The United States leads the world in data processing and storage capacity, so any requirement to move such capacity to a foreign location undermines a clear competitive

---

[26] *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).

[27] For example, foreign investment will likely decline. Given the high cost of constructing data centers, many companies will simply opt out of serving markets with onerous data localization requirements, especially small and medium-sized businesses. In 2013, the average cost of data centers in Brazil and Chile were $60.3 million and $43 million, respectively. Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill Push for Data Localization*, WALL ST. J. (Nov. 13, 2013), http://online.wsj.com/articles/SB10001424052702304868404579194290325348688. *See also* U.N. CONFERENCE ON TRADE AND DEVELOPMENT, DATA PROTECTION REGULATIONS AND INTERNATIONAL DATA FLOWS at 3 (2016), http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ("[I]f data protection regulations go 'too far' they may have a negative impact on trade, innovation and competition."); Nigel Cory, *Cross-Border Data Flows: What Are the Barriers, and What Do They Cost?*, INFORMATION TECHNOLOGY & INFORMATION FOUNDATION (May 2017), https://itif.org/publications/2017/05/01/crossborder-data-flows-where-are-barriers-and-what-do-they-cost at 6-7 ("At the firm level, barriers to data flows make firms less competitive, as a company will be forced to spend more than necessary on IT services. Companies will likely have to pay more for data-storage services, especially those in 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.").

[28] https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf; https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/; https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=2009&context=aulr.

advantage the U.S. enjoys.[29] According to a recent report, one state alone (Virginia) boasts 245 large-scale data centers that power one-third of the globe's online activity.[30] The United States has the largest number of data centers globally as it boasted 2,701 in 2022, with the next largest number being Germany's 487.[31] As digital services proliferate and traditional forms of national and international commerce become ever more data-intensive, the importance of this strategic advantage will grow as will the centrality of these data centers for information flowing worldwide.

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.[32] 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.[33]

Continued opposition from the United States and likeminded allies is needed at the multilateral stage in light of these growing trends.[34]

Data localization policies are often leveraged in ways that harm U.S. cloud services providers or otherwise 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.[35] More recently, the EU has advanced plans to adopt an EU-wide cloud that would localize data within EU borders and preclude U.S. suppliers from participation, in parallel with initiatives like its proposed cloud certification scheme, designed to put U.S. firms at a disadvantage.[36]

---

[29] https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf.

[30] https://www.washingtonpost.com/dc-md-va/2023/02/10/data-centers-northern-virginia-internet/.

[31] https://www.statista.com/statistics/1228433/data-centers-worldwide-by-country/.

[32] 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).

[33] *See* Chander & Lê, Data Nationalism, *supra* note 24; 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*"].

[34] 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.

[35] 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.

[36] Under Annex I NIS2 Directive, "essential entities" include among others airlines, banks, railway companies, energy companies, Securities Exchanges, pharmaceutical companies, healthcare providers, digital infrastructure

The provision of cloud services drives billions of dollars in economic value, as cloud computing supports millions of companies, applications, and services reliant on cloud infrastructure and related services.[37] 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. workers. 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 now 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 and under consideration in the Philippines, 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.

C. 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.[38] In a survey of the past year, Freedom House reported that between June 2022 and May 2023, 54% of the world's population that has access to the internet had social media platforms temporarily or permanently restricted

providers including those providing online communications tools, ICT managed services, and public administration entities.

[37] 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.

[38] *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).

by the government.[39] As of April, 36 countries were restricting access to Twitter, with political protests and social unrest often being the impetus for such restrictions.[40]

Russia has continued to isolate 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;[41] Turkey restricted access to Twitter in the country in the days following severe earthquakes and has pursued expanded limitations on the use and operation of social media services;[42] and India has intensified its campaign to interfere with political content posted on social media websites through government-mandated-and-orchestrated fact-checking while also pursuing a consultation pursuing the legal and technical power to selectively block over-the-top services—a development of high concern,[43] since it is already, after China, one of the world's most prolific practitioners of internet shutdowns.[44] 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.[45]

---

[39] *Freedom on the Net 2023*, *supra* note 14.

[40] https://techpolicy.press/digital-disruption-measuring-the-social-and-economic-costs-of-internet-shutdowns-throttling-of-access-to-twitter/; https://surfshark.com/research/internet-censorship.

[41] *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; *Freedom on the Net 2023*, *supra* note 14 ("Roskomnadzor, Russia's media and telecommunications regulator, requires internet service providers to install a unique, government-produced deep packet inspection (DPI) system that enables the blocking of websites across the country. The Kremlin has used this system to block global social media platforms, Ukrainian news sites, and domestic sites that carry any hint of dissent regarding its invasion of Ukraine. The coverage period also featured increased Russian blocking of websites that host LGBT+ content, part of a broader assault on that community in the country. The Belarusian government, which has aided Moscow's military aggression, has blocked more than 9,000 websites, including a slew of independent news sites and associated mirror sites that are maintained by Belarusian journalists working in exile.").

[42] https://www.reuters.com/business/media-telecom/twitter-restricted-turkey-netblocks-2023-02-08/; *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; https://techpolicy.press/digital-disruption-measuring-the-social-and-economic-costs-of-internet-shutdowns-throttling-of-access-to-twitter/ ("According to NetBlocks reports, the temporary block was due to government concerns about misinformation being spread on the platform. Regardless of the motivation for the block, it hampered the benefits of the tool in crisis response.").

[43] https://techcrunch.com/2023/04/06/india-cracks-down-on-betting-games/; *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).

[44] https://www.theguardian.com/world/2023/sep/25/a-tool-of-political-control-how-india-became-the-world-leader-in-internet-blackouts

[45] *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.

Small businesses in Nigeria rely on Twitter for publicity and fulfilling customer requests, with many individuals in Nigeria using the service as a tool to make their earning.[46]

Access Now reported there were 187 internet shutdowns in 35 countries in 2022, an uptick in the 182 internet shutdowns in 34 countries in 2021.[47] 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.[48]

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

---

[46] https://techpolicy.press/digital-disruption-measuring-the-social-and-economic-costs-of-internet-shutdowns-throttling-of-access-to-twitter/ (Showing that one study found that, when looking at 10 small businesses in Nigeria, that the ban on Twitter severely restricted these businesses' activity through this crucial resource. "During the first month of the ban, the 10 small businesses tweeted a total of 3,865 times total (125 tweets per day), a 42% decrease from one month prior to the ban. Twitter usage by some small businesses continued throughout the ban at a limited scope, likely through the use of circumvention tools such as VPNs.").

[47] *Internet Shutdowns in 2022: Weapons of control, shields of impunity*, ACCESS NOW (Feb. 28, 2023), https://www.accessnow.org/internet-shutdowns-2022/ [hereinafter "Internet Shutdowns 2022"].

[48] 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"].

abroad. Some of these regulations are in pursuit of legitimate and valid goals to address illegal content online; however, other 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.[49]

Separately, there are continuing 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;[50]
- 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 of legal norms such as due process may help reduce impact for U.S. firms operating abroad; conversely the absence of such norms may have the opposite effect. 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

---

[49] 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 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.").

[50] *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.

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.

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.[51] Access Now documented 187 internet shutdowns in 35 countries in 2022, an increase from 182 shutdowns in 34 countries in 2021.[52] Freedom House reported that in the past year, a record 41 of the 70 countries it surveys blocked websites that hosted "political, social, and religious speech," with 22 countries blocking social media websites.[53] 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.[54] 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.[55] 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.[56] In September and October 2022, the government blocked access to Instagram and WhatsApp, and has periodically

---

[51] *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.

[52] ACCESS NOW, *Internet Shutdowns 2022*, *supra* note 47.

[53] *Freedom on the Net 2023*, *supra* note 14.

[54] 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.

[55] Foreign Censorship Part 2, *supra* note 48.

[56] *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.

shut down the internet across the country,[57] all while activists within and outside of the country leveraged online services such as Instagram to mobilize and publicize events in real-time.[58] A September 2023 report found that the restrictions to internet access and online services in Iran in the past four years have resulted in a "direct economic cost" of $1.2 billion, and noted that the implications for the workforce have likely been dire as well: "for every one job that is lost in the digital economy, a further 1.54 jobs are lost in the broader economy."[59] 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. Other countries are beginning to seek similar filtering methods for their own domestic internet access based on government-imposed censorship needs, with the National Internet Gateway adopted by Cambodia and currently being pursued in Nepal showcasing this concerning trend towards a "Splinternet."[60]

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.[61]

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

---

[57] 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.

[58] *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.

[59] https://techpolicy.press/digital-disruption-measuring-the-social-and-economic-costs-of-internet-shutdowns-throttling-of-access-to-twitter/.

[60] https://kathmandupost.com/science-technology/2023/08/26/government-s-cybersecurity-policy-criticised-for-national-internet-gateway-plan.

[61] 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.

of goods remain goods subject to the GATT."[62] 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.[63] 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."[64] 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 obligations exist, such as for "public morals/order,"[65] GATS derogations are only permissible when necessary to achieve the stated objective; where no reasonable, less restrictive alternative exists; and when applied without prejudice.[66] 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.[67] 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.[68] 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

---

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

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

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

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

[66] GATS Art. XIV. *See also The World Trade Law of Censorship and Filtering*, *supra* note 62, at 13.

[67] 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/.

[68] GATS Art. XVII:1.

either hobble user privacy and security, or that force product manufacturers to include intrusive monitoring technology.[69] 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.[70]

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.

D. Taxation of Digital Products and 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.[71]

Further, CCIA welcomes the progress made pursuant to the OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting Project since 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.[72] The document states:

---

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

[70] 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/.

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

[72] 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/.

> 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.[73]

Pursuant to this commitment, the 143 countries that have agreed to this framework cannot introduce any new unilateral measures and CCIA encourages countries to abandon any national plans to implement such measures.[74] Further, while the most appropriate action would be an immediate withdrawal of existing DSTs in exchange for terminating the Section 301 actions, 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.[75]

Despite Canada's repeatedly commitments to the OECD agreement, in 2023 Canada declined to join the 138 countries that agreed to extend the pause on imposing or maintaining such taxes through 2024 while the framework is solidified. Canada intends to implement a DST in beginning in 2024. If Canada enacts and begins collecting DSTs even as the moratorium is in effect, it will undermine the entire OECD process and likely lead to other defections, particularly given that Canada is one of the closest trading partners of the United States, and one that is bound to some of the strongest trade commitments to the United States of any country through the USMCA.

Often based on inaccurate estimates, some countries assert that digital services fail to pay adequate taxes and should be subject to additional taxation.[76] Since U.S. firms (unlike those in most countries) are taxed in the United States on their global revenues, this is particularly

---

[73] 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.

[74] Member of the OECD/G20 Inclusive Framework on BEPS (updated June 9, 2023), https://www.oecd.org/tax/beps/inclusive-framework-on-beps-composition.pdf.

[75] 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 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.

[76] 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/.

specious, and in the absence of a global agreement will inevitably lead to double-taxation. 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 initiating or continuing 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.[77] 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.[78]

While distinct from a DST, many jurisdictions have also either sought or instituted the power to impose customs duties on electronic transmissions to extract discriminatory fees from digital services providers. Such steps upend over two-decades of trade-liberalizing treatment: the 2nd Ministerial Conference of the World Trade Organization in 1998 produced the Declaration of Global Electronic Commerce which since then resulted in a 25-year moratorium on customs duties on electronic transmission.

---

[77] *See, e.g.*, Letter, Sens. Ron Wyden and Mike Crapo to USTR Katherine Tai (Oct. 10, 2023), https://subscriber.politicopro.com/f/?id=0000018b-1647-d756-adfb-96dfd0550000; 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.

[78] 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"].

The moratorium has subsequently been renewed at every Ministerial since 2000. 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),[79] Article 19.3 of USMCA,[80] and Article 8.72 of the EU-Japan Economic Partnership Agreement.[81]

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. This is already occurring in Indonesia, where despite refraining from imposing a duty, the government is implementing reporting requirements, presenting a significant obstacle to operating in the market through a confusing and burdensome regime for companies both small and large.

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.[82] Analysis on duties on electronic transmissions for economic development shows that this is not supported.[83] The United States should continue to advocate for the permanent extension of the moratorium at the WTO at the upcoming Ministerial Conference expected in

---

[79] 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.

[80] 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"].

[81] 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.

[82] *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.

[83] 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.

February 2024, and discourage countries and the World Customs Organization from furthering the inclusion of electronic transmission in their domestic tariff codes.

E. Experimental 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, reflecting a pressing concern that the policy is spreading before the likely effects of such regulations, both intended and unintended, have been adequately evaluated. In some cases, platform regulation serves as a backdoor for industrial policy explicitly designed to advantage local competitors, dressed up as competition policy, and often employs thresholds designed specifically to ensure that only the leading U.S. internet services are subject to the regulations. In many cases, such rules are tailored to specifically impede the business models of U.S. companies, including the administering of app stores. In all instances policymakers struggle to separate procompetitive conduct from hypothetical harms they seek to regulate. The effectiveness of such proposals in promoting innovation in the tech sector is highly questionable.[84] 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.

F. 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 in a manner U.S. law would preclude 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.[85] This is illustrated by Australia, Colombia, and Mexico's continued lack of compliance.

Balanced copyright rules that include reasonable 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.

---

[84] 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.")

[85] *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.

trade agreement since those struck with Chile and Singapore in 2003 including some assurances of copyright balance.[86] That commitment has been reiterated by USTR.[87]

G. Forced Revenue Transfers for Digital News

A concerning trend of governmental intervention is the growing momentum in favor of 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. Such policies impose significant negative externalities on 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.[88] A USITC report also observed that these laws tend to have "generated unintended consequences" to small online publishers.[89] 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.[90]

---

[86] *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.

[87] 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.").

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

[89] 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.").

[90] 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.

CCIA would encourage U.S. policymakers to carefully evaluate the trade implications of imposing ancillary rights in the United States.[91] 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 passed the News Media Bargaining Code law in 2021 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 Meta—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 has spread to other jurisdictions, a recent development that warrants attention and reaction from the U.S. government before it accelerates. Canada passed similar legislation to force U.S. online services suppliers to pay Canadian news publishers for content shared through their platforms. The law, the Online News Act, will require "digital news intermediaries to pay Canadian news publishers for *any* content of theirs reproduced in *any* way. This would include brief quotes and snippets, headlines, and links. As has been the case in other markets, the proposed regulations for designation of digital news intermediaries make clear that the law targets U.S. companies—the thresholds are designed so as to only capture two U.S. providers, with the next closest provider closest to meeting the threshold also being from the United States.

The developments in Australia and Canada are particularly concerning given the precedent they could set globally—if every jurisdiction were to enact similar rules, the resulting payments would amount to billions of dollars annually for the mere right to index and link to and/or host legally acceptable quotation of news content, which itself is the underpinning of the internet's information-sharing ecosystem (particularly if other local constituencies begin to demand payment for linking to their content online). Such an outcome is genuine threat, as New Zealand has introduced a piece of legislation similar to Canada's and Australia's. Larger markets such as Brazil and Indonesia have introduced draft regulations that include the concerning remuneration rights for publishers as well as troubling content moderation restrictions that could impinge on suppliers' ability to promote quality content and downgrade low-quality news and/or misinformation. Regulators in the United Kingdom, Japan, South Africa, and Malaysia are also

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

looking at adopting similar frameworks to force payment by digital platforms to news corporations,[92] and momentum is growing in India to adopt similar rules as well.[93]

Rooting out this problematic and discriminatory policy is critical, as its spread could result in billions lost for U.S. firms operating in these countries and a fragmented internet, if left unchallenged. For example, Canada's government estimates that Google and Meta would pay at least C$234 million annually under the law, with that figure likely rising if more news businesses step in to demand more than the 4% floor set for granting an extension.[94] If such approaches spread, they 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 a discriminatory approach narrowly targeted to apply solely to U.S. firms.[95]

H. Imposing Legacy Telecommunications Rules on Internet-Enabled Services

U.S. digital services exports are often hindered by foreign jurisdictions adopting telecommunications-related rules and obligations. These policies include subjecting over-the-top (OTT) communications and content services to legacy telecommunications regulations, despite the fundamental differences in their makeup and use, and regulation of telecommunications services upon which digital services are reliant to reach their customers.

Another concerning global trend took root in 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 that ISPs customers request. Borrowed from the telephony era, such "sender-party-pays" 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 certain CAPs into paid contracts with ISPs for their services' traffic—demanded by users, not the CAPs themselves—have focused on U.S. services

---

[92] https://www.mcmc.gov.my/skmmgovmy/media/General/PressRelease/MS_MCMC-CONSIDERS-REGULATORY-FRAMEWORK-TO-ADDRESS-ONLINE-HARM-AND-IMBALANCE-MEDIA-ADEX.pdf; https://assets.publishing.service.gov.uk/media/6273af6be90e0746c882c361/Platforms_publishers_advice._A.pdf; https://www.jftc.go.jp/en/pressreleases/yearly-2023/September/230921EN2.pdf; https://www.compcom.co.za/wp-content/uploads/2023/03/Media-Statement-Terms-of-Reference-to-establish-a-Media-and-Digital-Platforms-Market-Inquiry-17-March-2023.pdf.

[93] *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.

[94] https://www.ctvnews.ca/canada/online-news-act-could-see-google-meta-pay-combined-234-million-to-canadian-media-1.6544576.

[95] *Id.*

through arbitrary thresholds of subscribership and average traffic volume, two metrics which experts suggest have negligible bearing on the strain on the network.[96] These proposals to mandate discriminatory payments by CAPs to ISPs—effectively taxing 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.[97]

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 forth the success of the global internet. These efforts, such as those being pursued in India, Vietnam, 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.

---

[96] 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.

[97] 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/.

I. Threats to Encryption and Security of Devices

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. One of the most notable developments in the past year has been the passing of the Online Safety Bill in the United Kingdom, which empowers Ofcom to direct digital firms to develop and use technology to scan for illegal materials on their services, thus undermining the security of end-to-end encrypted services. Often the relevant provisions are not explicit, but they mandate facilitated access, technical assistance, or compliance with otherwise infeasible judicial orders. There is growing international hostility to encryption.[98]

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.[99] 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.[100] The new system established three different low-value import regimes: "postal," "express," and "general." Due to continued challenges in clearing goods in the

[98] 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/.

[99] 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.

[100] *Argentina — Import Requirements and Documentation,* Privacy Shield Framework (Last Accessed Oct. 23, 2023) https://www.privacyshield.gov/ps/article?id=Argentina-import-requirements-and-documentation.

"general" regime, only the "express courier" is functional for e-commerce transactions.[101] However, industry reports that there are still limits within the "express" regime that make it difficult to export to Argentina and some U.S. companies have had to stop exporting to the Argentinian market completely.

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

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.[102] On December 23, 2019, the executive branch issued Decree 99/2019, implementing a temporary 30 % tax ("PAIS tax") on the purchase of foreign currency and purchases made online invoiced in foreign currency, among other things.[103] Further on September 16, 2020 the Central Bank introduced a new 35 % tax on foreign currency purchases, including on cross-border transactions made with credit cards, to "discourage the demand for foreign currency."[104] Combined, these controls and taxes are making it increasingly difficult, and at times impossible, for foreign companies to sell to Argentine customers.

The Argentine Central Bank has tightened foreign exchange controls as a response to the inflation crisis in the country, which has included obstructing access to U.S. dollars to fund imported goods and services.

---

[101] 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.

[102] *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.

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

[104] *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.

In November 2022, Argentina issued two new laws—Communications 5271/2022 and 7622/2022—that broadened licensing requirements to apply to all types of imports.[105] The laws established a new framework ("SIRA") that introduced new obligations for multiple government agencies to approve each import by reviewing several indicators including the importer's proposed payment method, tax status, and financial capability. Industry reports that his onerous process has increased approval wait times for transactions in U.S. dollars from 3-15 days to approximately 60 days, which has impeded U.S. firms from conducting business swiftly. The rules add further complication by requiring possible reapplication for approval in the instance that shipment information changes between approval and arrival in Argentina.

The Central Bank has introduced an online process to manage requests for services providers seeking to access the foreign exchange market for cross-border payments for imported services. The process, called "SIRASE" (Sistema de Importaciones de la República Argentina y Pagos de Servicios al Exterior), applies to services providers offering services including legal services, cloud services, software licenses, and others. In April 2023, the Central Bank further restricted access to the foreign exchange market and introduced a mandate for approval from the Central Bank, the Secretary of Commerce (Secretary), and the Argentine Tax for all requests to access the foreign exchange market to fund imported services through cross-border payments (known as a SIRASE request). The Secretary is given as long as 60 days to provide an answer to SIRASE requests, which could be lengthened by an extra 60 days if the Secretary seeks additional information. Such wait times impede the ability of U.S. and other foreign services providers from market access to Argentina.

Further, in July 2023, Argentina issued a Decree No. 377/2023, which introduced new value-added taxes on imports and related services funded with U.S. dollars.[106] The decree imposes a 7.5% tax on imports under most tariff classifications where payment has been made in U.S. dollars, and a separate 7.5% tax on import/export freight services where payment has been made in U.S. dollars, with limited exceptions. This requirement means that a single import could result in an additional tax of up to 15% simply due to the fact that its purchase and transport was funded through U.S. dollars, putting U.S. suppliers at a distinct disadvantage. The discriminatory nature of this tax raises issues with respect to Argentina's compliance with is WTO national treatment obligations under both the GATT and the GATS.

Customs Release Delays

In Argentina, industry reports obstructions due to requests by customs authorities on shipment or import documentation or a physical inspection that detains shipments through "channels"—under a yellow channel for the former category and a red channel for the latter. These shipments are frequently detained by authorities for as long as one year, even in cases where all necessary inspections have been conducted and the importer responds to all inquiries, resolves potential discrepancies or disputes, and adheres to any monetary fines sought. The detainment process imposes significant delays to delivery timelines, which obstructs the supply chain and leads to

[105] https://insightplus.bakermckenzie.com/bm/international-commercial-trade/argentina-implementation-of-sira-and-sirase.

[106] https://insightplus.bakermckenzie.com/bm/tax/argentina-tax-on-the-acquisition-of-foreign-currency-extended-to-new-transactions_1.

broad uncertainty for importers and services and goods providers that rely on imports. The process also impedes importers by introducing costs for those who could be obligated to reorder goods and face additional fees for storage.

B. Australia

Forced Revenue Transfers for Digital News

In February 2021, the Australian Government passed the News Media and Digital Platforms Mandatory Bargaining Code.[107] 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.[108]

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 "final offer" 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 has broad 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.

---

[107] 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.

[108] *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/.

To date, only two companies – both American – are in scope of the law. There are significant concerns from a procedural,[109] competition,[110] trade,[111] and intellectual property[112] perspective that U.S. authorities should pay close attention to, if companies are designated as subject to its obligations. In particular, U.S. officials should monitor the implementation of the Code and its adherence to the principles of transparency, fairness and non-discrimination as consistent with the U.S.-Australia FTA.

At time of filing, no platform has been officially designated, but it is clear from the Treasury's consultation paper reviewing the code, published in April 2022, that the main targets of the law continue to be Google and Meta—who escaped designation only after concluding a range of commercial deals.[113] The law continues to be of concern to industry due to its targeting of these two companies.

In November 2022, the Australian Treasury released a report documenting the first year following the implementation of the News Media Bargaining Code. The report found that the two targeted digital platforms reached at least 30 commercial agreements with Australian news businesses that the Treasury claims would have otherwise been "highly unlikely" to materialize but the agreements contained confidentiality clauses, and the Treasury did not provide more details on the contents of these agreements.[114] The Treasury issued recommendations including that the ACCC conducting reports on the amount of Australian news made available by digital platforms and whether news businesses and digital platforms have a significant bargaining imbalance between them; determining whether government powers can be used to demand information on the deals struck between news businesses and digital platforms; and reviewing the Code after it has been in effect for four years. As initial deals expire, it will be important to closely monitor the political pressure news businesses exert on the Treasury to extract more revenue from U.S. firms as a condition of market access, further distorting Australia's internet services market.

---

[109] *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/.

[110] *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/.

[111] *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/.

[112] *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/.

[113] 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).

[114] Australian Treasury, *News Media and Digital Platforms Mandatory Bargaining Code (*Nov. 2022) https://treasury.gov.au/sites/default/files/2022-11/p2022-343549.pdf.

Experimental Platform Regulation

The Australian Competition and Consumer Commission released a consultation seeking comments on a set of reforms in December 2022 that seek to adopt a "new regulatory framework for consumer protection and to improve competition."[115] The ACCC puts forward a series of recommendations, including "targeted obligations" regarding "anti-competitive self-preferencing;" "anti-competitive tying;" "exclusive pre-installation and default agreements that hinder competition;" "impediments to consumer switching;" "impediments to interoperability;" "data-related barriers to entry and expansion, where privacy impacts can be managed;" "a lack of transparency;" "unfair dealings with business users;" and "exclusivity and price parity clauses in contracts with business users." Mandatory processes for scanning for "scams, harmful apps and fake reviews" are among the recommendations as well. The ACCC accepted comments through Feb. 15, 2023,[116] and on April 28, the ACCC released the sixth interim report for the Digital Platform Services Inquiry.[117] Industry remains concerned that the final recommendations from the ACCC focus on ill-defined and poorly documented harms, implementation of which will hinder the competitive delivery of services by U.S. digital suppliers in Australia. This initiative represents another instance of a country following the EUs lead in furthering unproven, experimental regulation without careful consideration of their unintended consequences.

Further, on March 7, 2023, the ACCC announced its annual compliance and enforcement priorities for 2023-24, which include competition and consumer issues relating to digital platforms and "big tech." There are ongoing enforcement actions against a number of digital platforms, and on April 28, 2023 the ACCC released the sixth interim report for the Digital Platform Services Inquiry.[118]

Threats to Encryption and Security of Devices

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.[119] 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

---

[115] Australian Treasury, *Digital Platforms: Government consultation on ACCC's regulatory reform recommendations* (Dec. 2022), https://treasury.gov.au/sites/default/files/2022-12/c2022-341745-cp.pdf.

[116] https://ccianet.org/wp-content/uploads/2023/02/CCIA-Comments-to-the-Australian-Treasury.pdf.

[117] https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25/march-2023-interim-report.

[118] Australian Competition & Consumer Commission, *Digital platform services inquiry 2020-2025 March 2023 interim report (March 31, 2023)* https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25/march-2023-interim-report.

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

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.[120] The Australian Government Department of Home Affairs disclosed in a February 2022 report that 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."[121]

Copyright Liability Regimes for Online Intermediaries

Failure to implement obligations under existing trade agreements serves as a barrier to trade.[122] The U.S.-Australia Free Trade Agreement contains an obligation to provide liability limitations for service providers, analogous to 17 U.S.C. § 512. However, Australia has failed to fully implement such obligations and current implementations are far narrower than what is required. Australia's statute limits protection to what it refers to as "carriage" service providers, not service providers generally. The consequence of this limitation is that intermediary protection is largely limited to Australia's domestic broadband providers. Online service providers engaged in the export of information services into the Australian market remain in a precarious legal situation. This unduly narrow construction violates Australia's trade obligations under Article 17.11.29 of the FTA. This article makes clear that the protections envisioned should be available to all online service providers, not merely carriage service providers. Although Australian authorities documented this implementation flaw years ago, no legislation has been enacted to remedy it.[123] 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.[124] 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

---

[120] 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.

[121] 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.

[122] *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.

[123] Australian Attorney General's Department, Consultation Paper: Revising the Scope of the Copyright Safe Harbour Scheme (2011), https://s11217.pcdn.co/wp-content/uploads/2011/10/revisingthescope-redacted.pdf.

[124] 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/.

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.[125] Criticism for the legislation was widespread, with particular concern about the rushed nature of the drafting and legislative process.[126] 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.[127] Australian officials have also indicated that the country will soon block access to Internet domains hosting terrorist material and will pursue additional legislation that will impose new content requirements on digital services.[128]

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."[129] 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.[130] 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

---

[125] 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.

[126] *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.

[127] *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.").

[128] 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.

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

[130] *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/.

providers; device manufacturers; hosting services; and miscellaneous electronic services such as email, messaging, gaming, and dating services.[131]

On December 15, 2022, the eSafety Commissioner released a report detailing responses it received from digital services providers pursuant to the Basic Online Safety Expectations, passed through the Online Safety Act.[132] The report detailed platforms' responses regarding efforts to address online child safety and abuse, and included condemnation of services that failed to monitor person-to-person video calls for possible child sexual exploitation and abuse (CSEA). The Commissioner announced plans to send additional notices regarding CSEA in early 2023, and to: issue the first periodic notices to begin using one or several metrics to track compliance; publish any extra guidance required; and begin issuing statements detailing compliance and/or non-compliance throughout the rest of the year.

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

Critical infrastructure reforms

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.[134] 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.

---

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

[132] eSafety Commissioner, *Basic Online Safety Expectations: Summary of industry responses to the first mandatory transparency notices* (Dec. 2022) https://www.esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf.

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

[134] 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.

Hosting Strategy Certification Framework

In 2019, the Australian Government released the Hosting Strategy,[135] providing policy direction on how government data and digital infrastructure would enable the Digital Transformation Strategy, focused on data center facilities, infrastructure, data storage and data transmission. In March 2021, the certification framework for the policy was released to operationalize the Hosting Strategy. [136] 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. The policy functions of this framework were transferred to the Department of Home Affairs in May 2023.[137]

Audiovisual Services and Mandatory Local Content Quotas

The Australian government is pursuing a framework for imposing local content quotas or mandatory spending or "prominence" obligations on local content for streaming services. The new policy, outlined in the January 2023 report, specifically calls for the introduction of "requirements for Australian screen content on streaming platforms to ensure continued access to local stories and content," to be unveiled in the "third quarter of 2023 and to commence no later than July 1, 2024."[138]

The Australian government argues that foreign investment in Australian content is not guaranteed—despite the fact it has been increasing at rapid rates—and that the current levels of such programming on online streaming platforms are insufficient.[139] AUSFTA precludes such content requirements unless the government is able to make a finding that Australian content is not readily available in Australia, a standard no credible observer would assert has been met. In fact, the data show the opposite: that Australian content is both bountiful and growing on the online streaming platforms. Production spending for Australian content is skyrocketing—fuelled largely by the foreign streaming providers—and the amount of Australian content on these platforms is in actuality plentiful.[140]

---

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

[136] 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].

[137] Machinery-of-Government Transfer of Cyber Security-Related Policy Functions from DTA to Home Affairs, https://www.hostingcertification.gov.au/.

[138] https://www.arts.gov.au/sites/default/files/documents/national-culturalpolicy-8february2023.pdf.

[139] https://apo.org.au/sites/default/files/resource-files/2022-02/apo-nid316658.pdf at 12.

[140] https://www.screenaustralia.gov.au/sa/media-centre/news/2022/11-10-drama-report-2021-22; https://www.streamingforaustralia.com.au/wp-content/uploads/2022/11/Streaming-for-Australia_Nov2022.pdf at 11; https://www.acma.gov.au/spending-subscription-video-demand-providers-2021-22-financial-year (Showing that there is an ample supply of Australian content on the streaming platforms—the Australian Communications and Media Authority reported that the five major online streaming services (Amazon Prime Video, Disney, Netflix,

Recent government papers on the subject have reflected an interest from the regulator on both investment and distribution of Australian content as well as making such content prominent and discoverable on their platforms,[141] implicating the algorithms which providers use to present content to consumers. One paper, published by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts in December 2022, sought comment on four approaches to improving prominence of Australian content on connected TV devices such as streaming boxes that included a reporting framework, a fair bargaining framework, must-carry obligations, and must-promote obligations.[142] Mandatory prominence or promotion requirements could interfere with the services that streaming providers offer in Australia and circuitously create local content requirements similar to quotas, and equally inconsistent with AUSFTA obligations.

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. CCIA urges USTR to actively monitor these developments and engage with Australia to avoid likely breaches of AUSFTA if current proposals are adopted.

Taxation of Digital Products and 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.[143] 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."[144] 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

Stan—which is Australian, and Paramount+) hosted 2,345 titles or events representing Australian programming reaching up to 7,714 hours.).

[141] https://apo.org.au/node/316658 ("The Scheme will require large Subscription Video on Demand (SVOD) services to report annually 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.").

[142] https://www.infrastructure.gov.au/sites/default/files/documents/prominence-framework-connected-tv-devices-proposals-paper.pdf.

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

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

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.

Industry is concerned that the ATO is seeking to release a second draft of these proposed rules ahead of finalizing the policy imminently. 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 Products and Services

Austria implemented a 5 % digital tax on revenues from digital advertising services provided domestically.[145] 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.[146] 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."[147] 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."[148]

---

[145] 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.

[146] 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).

[147] *Id*.

[148] 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.

Austria was among the countries that imposed a DST with whom the United States reached an interim agreement, and any payments made under the Austria DST can be accredited upon implementation of the OECD Pillar 1 solution.[149]

D. Bangladesh

Digital Security Act

The Bangladesh Parliament passed the Cyber Security Act of 2023, replacing—but largely reinforcing—the previously-enacted Digital Security Act of 2018, in September 2023.[150] The law criminalizes a wide range of online activity, creating challenges for internet-based platforms and digital media firms, retaining almost every single offense detailed in the original law.[151] The Act criminalizes publication of information online that hampers the nation, tarnishes the image of the state or hurts religious sentiment. The law also empowers the government to remove and block content online.[152] The law has come under scrutiny for harming civil liberties and human rights.[153] Upon passage of the bill, the U.S. Embassy in Bangladesh issued a statement noting that the legislation "continues to criminalize freedom of expression, retains non-bailable offenses, and too easily could be misused to arrest, detain, and silence critics."[154]

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

---

Konkret sind jene Unternehmen betroffen, die einen weltweiten Umsatz von 750 Mio. € bzw. einen jährlichen Umsatz aus Onlinewerbeleistungen von mindestens 25 Mio. € erzielen, soweit diese in Österreich gegen Entgelt erbracht werden. Aus den aus der Digitalsteuer resultierenden Einnahmen sollen jährlich 15 Mio. € an österreichische Medienunternehmen gehen." [Internet giants like Facebook or Google will have to pay for online advertising sales in the future. In order to achieve more tax justice, the digital tax that has long been discussed in public should now be implemented; the Tax Amendment Act 2020 presented by the ÖVP and FPÖ had the necessary majority of votes. Internet giants like Facebook, Google or Amazon must now pay a five percent tax on online advertising sales from 2020. Specifically, those companies are affected that achieve a worldwide turnover of € 750 million or an annual turnover from online advertising services of at least € 25 million, as far as these are rendered in Austria for a fee. From the income resulting from the digital tax, € 15 million should go to Austrian media companies every year.]).

[149] *See* https://home.treasury.gov/news/press-releases/jy0419.

[150] https://restofworld.org/2023/south-asia-newsletter-bangladesh-cyber-security-act/.

[151] https://www.amnesty.org/en/documents/asa13/7125/2023/en/; Digital Security Act, 2018, *available at* https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf [Bangladesh].

[152] https://www.dhakatribune.com/bangladesh/325228/parliament-passes-cyber-security-bill-2023.

[153] https://www.amnesty.org/en/latest/news/2023/08/bangladesh-government-must-remove-draconian-provisions-from-the-draft-cyber-security-act/; *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.

[154] https://bd.usembassy.gov/30390/.

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

In July 2022, the government of Bangladesh released a draft personal data protection bill dubbed the Data Protection Act.[155] The legislation initially implemented strict data localization requirements for sensitive data, user-generated data, and classified data. Industry expressed concern that the obligations contained within the draft legislation are confusingly defined and break from global norms and procedures.[156] The Bangladesh government released an updated draft in March 2023 that improved upon the prior draft in many ways, but still contains potential barriers to cross-border data flows.[157] While efforts have been made to restrict data localization measures to sensitive data only, a new provision allowing various regulators to regulate international data transfers as they see fit—possibly leading to different rules governing data depending on the specific sector—could hinder the delivery of online services by U.S. and other foreign providers.[158] This is particularly concerning given the remit of the Bangladesh Bank and the National Board of Revenue apply to the entire Bangladeshi economy.[159] Further, sensitive data is not well-defined and user-generated data—also poorly-defined—continues to be subject to data localization requirements in the framework for providing data subject consent to transfer sensitive data abroad has not been provided, leaving the contours of the data-sharing regime vague and uncertain.

---

[155] 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.

[156] 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.

[157] Draft Data Protection Act 2023, *Information and Communications Technology (ICT) Division, Ministry of Posts, Telecommunication and Information Technology*, Government of the People's Republic of Bangladesh, March 14, 2023, https://ictd.gov.bd/site/page/d05a8088-8272-49b4-883c-1698796dce3e/খসড়া-আইন,-বিধি-এবং-নীতিমালা.

[158] *Bangladesh Draft Data Protection Act 2023: Potential and Pitfalls,* The Atlantic Council South Asia Center (May 8, 2023) https://www.atlanticcouncil.org/wp-content/uploads/2023/05/Bangladesh-Draft-Data-Protection-Act-2023-Potential-and-Pitfalls.pdf.

[159] *Bangladesh Draft Data Protection Act 2023: Potential and Pitfalls,* The Atlantic Council South Asia Center (May 8, 2023) https://www.atlanticcouncil.org/wp-content/uploads/2023/05/Bangladesh-Draft-Data-Protection-Act-2023-Potential-and-Pitfalls.pdf ("The Bangladesh Bank and the National Board of Revenue cover the entire gamut of the economy. This "carve out" in the law coupled with the expanded definition of sensitive data indicate that the government could try to utilize the DPA 2023 to achieve other policy objectives like control on outward remittances, capital flight, and tax evasion/avoidance.").

Government-Imposed Restrictions on Internet Content and Related Access Barriers

The Bangladesh Telecommunication Regulatory Commission has 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.[160] The draft of the rules, which have been called the Regulation for Digital, Social Media and OTT Platforms and proposed several times over the past year, were presented to a subdivision of the Supreme Court of Bangladesh on January 9, 2023. Despite providing fora for public feedback to the draft legislation, the draft of the bill appears to reflect none of the vast concerns raised by industry and free expression advocates to the Bangladesh government.[161]

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.[162]

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.[163]

Internet Shutdowns

According to data from Access Now, the internet was shut off six times in Bangladesh throughout 2022, making it the fifth most frequent practitioner of internet shutdowns globally

---

[160] Bangladesh Telecommunication Regulatory Commission, Regulation for Digital, Social Media and OTT Platforms, 2021, *available at* http://www.btrc.gov.bd/sites/default/files/files/btrc.portal.gov.bd/notices/0031100b_c62f_46eb_9ce8_317e53ac881b/2022-02-06-04-33-68c9c154e5319e6e9179af538b3e47cb.pdf.

[161] *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.

[162] 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

[163] *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

that year.[164] 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.[165]

E. Brazil

Restrictions on Cross-Border Data Flows and Data

In 2018, Brazil passed a privacy law, *Lei Geral de Proteção de Dados* (LGPD). It officially came into force in August 2020, and in August 2021 sanctions were effective.[166]

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.[167] 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.[168] In addition, the national authority is tasked with determining whether a foreign government or international organization has a sufficient data protection scheme in place and overseeing standard contractual clauses before any data is authorized to be transferred to the government or organization.[169]

On Aug. 15, 2023, the Brazil Data Protection Agency (ANPD) published a draft of the International Transfer of Personal Data Regulation and solicited comments until September 14.[170] The draft regulation implements a framework to establish the jurisdictions with adequate privacy protections for the transfer of data. The regulation will dictate the terms that standard contractual clauses must meet, with the ANPD able to accept SCCs from other countries as substitutable.[171] As the ANPD finalizes these rules, USTR should monitor to make sure the rules

---

[164] ACCESS NOW, *Internet Shutdowns 2022*, *supra* note 47.

[165] 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 *supra* note 48.

[166] *See* Brazil's government landing page for LGPD: https://lgpd-brazil.info/.

[167] 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.

[168] 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).

[169] *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.

[170] https://www.gov.br/participamaisbrasil/regulation-on-international-transfer-of-personal-data.

[171] *Brazil Data Protection Agency (ANPD) Publishes Proposed International Transfer of Personal Data Regulation for Public Consultation*, Lexology (Aug. 16, 2023) https://www.lexology.com/library/detail.aspx?g=a9ec3344-2975-402d-bb7d-3b61efbd6dfb.

align with international norms that facilitate the free and fair flow of data that underpins U.S. digital services exports.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In August 2023, the Brazilian Senate introduced Bill of Law N° 4097, DE 2023, which would amend a 2014 law to implement new "digital sovereignty" measures into the General Data Protection Law.[172] Under the legislation, IT companies offering services in Brazil would have local ownership and control obligations. These companies would be required to have 25% of the voting share capital owned by Brazilian nationals and/or Brazilian companies (those that are headquartered in Brazil or incorporated under Brazilian law).

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

The Brazilian Telecommunications regulator (ANATEL) in 2023 launched a public consultation regarding the regulation of "Value Added Services" (VAS) (*e.g.*, internet services), with many questions focusing on the viability and appropriateness of network usage fees in Brazil.[173] The consultation sought input on whether there is a need for specific regulations targeted for large network users of broadband networks (such as popular U.S. online services suppliers), whether digital services providers should be regulated differently than telecommunications service providers, whether the government should impose additional responsibilities on larger services providers such as potential new remuneration obligations, and other questions related to possible regulations for the digital economy.[174] A proposal to impose network usage fees on "large" companies would be de facto discriminatory against popular U.S. internet services by nature.

There is a potential second ANATEL consultation focused on network usage fees forthcoming in late 2023. The Minister of Communications has publicly supported network usage fees and argued that ANATEL has the authority to impose them,[175] an ANATEL Commissioner has publicly expressed that he supports network usage fees,[176] and the ANATEL Chair has suggested that the agency will put forward network sustainability regulations in the coming years.[177]

---

[172] *See* text of the legislation: https://legis.senado.leg.br/sdleg-getter/documento?dm=9438842&ts=1693422692282&disposition=inline&_gl=1*qztlj8*_ga*NDA3MzMyNjQ0LjE2NTU5MDAzMDg.*_ga_CW3ZH25XMK*MTY5MzQzMjU3MC4zNTguMS4xNjkzNDM1NDMyLjAuMC4w; https://www25.senado.leg.br/web/atividade/materias/-/materia/159387.

[173] https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-abre-tomada-de-subsidios-sobre-regulamentacao-de-deveres-dos-usuarios. CCIA submitted comments, available at https://ccianet.org/wp-content/uploads/2023/07/2023-CCIA-Submission-to-ANATEL-English.pdf.

[174] *See* ANATEL consultation No. 13: https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=2&ConsultaId=10120.

[175] https://www.telesintese.com.br/fair-share-deve-criar-ambiente-justo-e-simetrico-defende-ministro/.

[176] https://teletime.com.br/14/09/2023/fair-share-e-neutralidade-de-rede-qual-a-relacao/; https://teletime.com.br/04/10/2023/a-neutralidade-de-rede-e-as-novas-dinamicas-concorrenciais-dos-mercados-digitais.

[177] https://valor.globo.com/empresas/noticia/2023/09/12/anatel-nao-vai-se-omitir-sobre-compartilhamento-de-custo-com-big-techs-diz-presidente.ghtml; https://www.telesintese.com.br/big-techs-podem-ser-bloqueadas-por-uso-abusivo-das-redes/.

ANATEL is expected to continue to consider these discriminatory mandatory payments despite significant opposition to network usage fees arising in the consultation.[178] Brazil's Congress introduced Bill 2768 in November 2022,[179] that empowers the National Telecommunications Agency (ANATEL) to oversee digital platforms as the main Brazilian regulator. The legislation introduces a regulatory framework imposing obligations on digital platforms offering services in Brazil governing how the companies are organized and operate in Brazil. The legislation includes vague definitions and fails to detail the obligations imposed on platforms to ensure adherence. Although the legislation avoids specific prescriptive mandates, the it grants ANATEL broad discretionary authority to set the definitions and draft rules. The legislation's opaque language makes it difficult for industry to predict the obligations that would specifically apply to U.S. companies, but it would, at a minimum, introduce burdens through heightened compliance costs and the possibility of obligatory business operation restructuring.

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.[180] The differential treatment and low *de minimis* threshold for consumer-to-consumer transactions create barriers to international trade by increasing transaction costs for Brazilian businesses while limiting consumer choice and competition amongst Brazilian businesses. Extending the *de minimis* threshold to business-to-consumer and business-to-business transactions and raising the *de minimis* threshold would help Brazil conform with international consumer standards and shopping behaviors. Current legislation allows for an increase of the threshold to USD $100 without the need for Congressional approval. To compare, the average *de minimis* threshold among OECD members is USD $70 for taxes and USD $194 for duties.[181]

Ex-Tariff Special Regime Requirement

Brazil's customs regime enables "ex-tariff" ("ex tarifário") imports of foreign manufactured goods to enter the country under some scenarios. This refers to the act of when importers are able to seek duty waivers for imports to decrease costs. The "ex tariff" regime comes into effect when there is no similar equipment being manufactured locally, including capital goods and information technology and telecommunications products.

In August 2023, the Brazilian Government published a new resolution for "ex-Tariff" concessions, which introduced new requirements for importers seeking a renewal. For a renewal

[178] https://www.pedagionainternet.com.br/en/post/telecom-giants-vs-everyone-else-replicating-the-polarization-of-the-european-fair-share-consult.

[179] https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2337417.

[180] 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.

[181] For an overview of *de minimis* values worldwide, *see* Global Express Association, *Overview of de minimis value regimes open to express shipments worldwide* (Nov. 4, 2021), https://global-express.org/assets/files/GEA%20De%20Minimis%20Country%20information_4%20November%202021.pdf

or future "ex-tariff" request, importers must showcase an investment project along with the previously-required evidence of no equivalent local production—thus justifying the adoption of the "ex-tariff" approval. The project would have to disclose the equipment's function; the schedule and location of the equipment's use; the necessity of the equipment or productivity gains derived from its use; the innovative technologies introduced through the product; and any other justification for a duty exemption.

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 but was never finalized into law. The Brazilian Government introduced a new version of that bill, Bill 2630 or otherwise known as the Law of Freedom, Responsibility and Transparency,[182] that would create penalties for tech and internet companies that fail to crack down on fake news and other illegal materials on their platforms. The legislation would be among the strictest legislation governing social media and other content-hosting websites if passed.[183] Among the provisions, the bill would establish a supervisory entity that would hold sweeping powers and a mandate to monitor and regulate the internet, including by establishing security protocols for companies; impose data transparency requirements; and establish a remuneration scheme for news publishers whereby online platforms are forced to carry and pay for news content in a manner that contravenes the very nature of information-sharing on the open internet and incentivizes clickbait and misinformation. The proposed law remains pending.

F. Cambodia

Government-Imposed Content Restrictions and Related Access Barriers

Reports of censorship and mandated internet filtering and blocking continue persist in Cambodia.[184] Legislation passed in April 2020 grants extensive authorities to the government to restrict information online if a state of emergency is imposed.[185] This has prompted concern at the UN over possible human rights abuses.[186]

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.[187] While the specifics of the implementation remain unclear, there is potential that this could be

[182] https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2265334&filename=Tramitacao-PRLP%201%20=%3E%20PL%202630/2020.

[183] https://www.aljazeera.com/news/2023/5/2/brazil-fake-news-bill-sparks-outcry-from-tech-giants.

[184] *Freedom on the Net 2023: Cambodia* (2023), https://freedomhouse.org/country/cambodia/freedom-net/2023.

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

[186] 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.

[187] *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.

abused and misused to block online content and keep out certain foreign digital services, akin to China's "Great Firewall," raising human rights concerns.[188] 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 resource for good."[189] The law was set to go into effect in February 2022, but has been postponed to an undetermined date due to the pandemic.[190] In the build-up to national elections in July 2023, the Cambodian government accelerated implementation of the National Internet Gateway and in February 2023, when it swiftly mandated internet service providers to block several domains associated with the Voice of Democracy news outlets.[191]

A draft Cybercrime bill has also been discussed by the Interior Ministry that could hold intermediaries liable for third party content.[192] The bill also contemplates new data localization mandates. In May 2022, government officials reiterated the desire to adopt the legislation,[193] 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.[194] The draft from September 2022 reportedly includes granting the government the power to take control of operating systems and duplicate data from private companies if they are deemed to be unable to address the harms of a cybersecurity threat or data breach.[195]

G. Canada

Forced Revenue Transfers for Digital News

In April 2022, Canadian Heritage introduced Bill C-18, the Online News Act,[196] which would empower the Canadian Radio-television and Telecommunications Commission ("CRTC") to compel large "digital news intermediaries"—namely Meta and Google—to pay groups of news

---

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

[189] 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/.

[190] 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.

[191] https://asia.nikkei.com/Politics/Cambodia-internet-providers-told-to-block-independent-broadcaster.

[192] 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.

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

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

[195] https://restofworld.org/2023/cybersecurity-law-draft-cambodia-elections/.

[196] 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].

publishers for *any* reproduction of *any* piece of news content on their services, including headlines, quotes, and links. The legislation received Royal Assent and became law on June 22, 2023, with substantive obligations set to take effect no later than December 19.

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.[197] Further, Canada's Parliamentary Budget Office ("PBO"), in responding to a request from a Member of Parliament, estimated that $329.2 million 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.[198] The estimates perpetuate concerns that the law would forcibly transfer revenue from U.S. digital services firms to shore up local behemoths.

The CRTC's regulatory plan suggests that mandatory bargaining (if affected companies do not obtain exception orders) may begin in late 2024 or early 2025, following public consultations on the implementing regulations and the development of the arbitration panel and other necessary resources.[199] Canadian Heritage published draft regulations dictating the implementation of the law on September 2, 2023,[200] which confirmed that the thresholds for designation based on this law would only capture two U.S. providers, with the next provider closest to being included also being from the United States.[201] Further, the draft regulations would require digital platforms to pay at least 4% of their total global revenue from all sources divided by the ratio of Canada's GDP to global GDP, (i.e., to create a rough attribution of Canada-relevant revenues) to news businesses to be considered for exemption from the law. This requirement reflects how the purported goal of the legislation—to fairly compensate news businesses for the value they bring digital platforms—has veered off its course to instead be a tax on all revenue. The government estimates that the two companies would have to pay at least a combined C$234 million annually to news businesses to be able to continue operating in the market with news links and sharing on their platforms. For digital platforms seeking to qualify for an exemption through commercial deals, they are also subject to an obligation to ensure that a "significant portion of independent local news businesses benefit from them," the definitions of which are fraught with uncertainty—if 10 or more news outlets (defined as any outlet with two part-time journalists in the law) state they have been excluded from deals, the regulator is empowered to deny the

---

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

[198] Office of the Parliamentary Budget Officer, Cost Estimate for Bill C-18: Online News Act, *supra* note 94.

[199] https://crtc.gc.ca/eng/industr/info.htm.

[200] https://www.gazette.gc.ca/rp-pr/p1/2023/2023-09-02/html/reg1-eng.html.

[201] https://www.ctvnews.ca/canada/online-news-act-could-see-google-meta-pay-combined-234-million-to-canadian-media-1.6544576.

application for exemption, granting hundreds of outlets with effective veto power over digital platforms' exemptions. Any agreement struck between the digital platforms and news businesses must fall within 20% of the "average relative compensation of all of the agreements submitted with that request" made by the platform, which reflects a blunt, uniform, per-journalist subsidy rather than a policy seeking to promote quality journalism.

The law 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.[202]

Taxation of Digital Products and Services

Canada announced its plans to proceed with a DST as part of its annual Budget, even as 138 countries agreed to extend the current pause on digital services taxes through 2024 while global tax reform continues to move forward.[203] Through this tax, Canada is seeking to collect up to CAD $1 billion annually, almost all of which is expected to come from U.S. companies.[204] The Parliamentary Budget Officer in October 2023 estimated that the tax would bring the Canadian government C$7.2 billion in five years.[205] The tax would be a 3% levy 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, online advertising services, and user data sales and licensing services.[206] The thresholds would be set to cover firms that 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.[207]

It is expected that a majority of the revenue collected would be from U.S. companies.[208] The targeted nature of the DST, based both on revenue thresholds and the definitions of the covered services, places Canada in conflict with its commitments under the USMCA including Articles

---

[202] 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

[203] https://www.oecd.org/tax/beps/oecd-g20-inclusive-framework-members-outcome-statement-on-two-pillar-solution-to-address-tax-challenges-arising-from-digitalisation-july-2023.pdf.

[204] https://ccianet.org/wp-content/uploads/2023/09/CCIA-Comments-Canada-2023-Budget-DST.pdf.

[205] https://www.pbo-dpb.ca/en/publications/LEG-2324-013-S--digital-services-tax--taxe-services-numeriques.

[206] https://fin.canada.ca/drleg-apl/2023/ita-lir-0823-n-2-eng.pdf.

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

[208] https://ccianet.org/wp-content/uploads/2023/09/CCIA-Comments-Canada-2023-Budget-DST.pdf.

15.3 and 15.4 of the cross-border trade in services chapter, WTO most-favored-nation commitments in the GATS, and is subject to Section 301 actions under U.S. law.[209]

CCIA is concerned that despite the OECD agreement on a global solution, and the clear commitment not to proceed with any new measures, Canada still intends to finalize this proposed legislation. Indeed, Canadian policymakers have repeatedly stated that they intend to move forward with the DST if the OECD framework is not in place by January 1, 2024.[210] Given the practical difficulty of meeting that deadline, and Canada's apparent intent in moving ahead notwithstanding, CCIA appreciates USTR's strong engagement to push back on the implementation of this discriminatory taxation measure and to instead steer Canada toward the OECD agreement.[211]

---

[209] Article 15.3 of USMCA requires Parties to "accord to services and service suppliers of another Party treatment no less favorable that that it accords, in like circumstances, to its own services and service suppliers." Once thresholds are instituted that largely shield competing Canadian companies from the effects of the tax (including competitors whose offering are largely non-digital), the discriminatory effects of the tax are unavoidable, and thus actionable under trade obligations. A DST would also conflict with USMCA MFN Article 15.4 which provides that Parties "shall accord to services or service suppliers of another Party treatment no less favorable than it accords, in like circumstances, to services and service suppliers of another Party or a non-Party." This provision obligates Canada to provide equal treatment to service suppliers regardless of county of origin. As the proposed DST would apply disproportionately to U.S. service suppliers vis-à-vis service suppliers from other countries (including Parties and non-Parties), it would violate Article 15.4, by creating a burden U.S. firms would bear, to the exclusion of numerous other foreign firms providing like services in the Canadian market. The discriminatory nature of the DST conflicts with commitments under the General Agreement on Trade in Services (GATS) for a range of specific services (e.g., for distribution, which would cover marketplaces), notably the national treatment and MFN provisions of Article II and Article XVII. Article II mandates that members offer "treatment no less favorable than it accords to like services and suppliers of any other country." While USMCA Article 32.3 exempts certain taxation measures, Article 32.3(6)(a) explicitly states that, notwithstanding this exemption, Article 15.3 applies to taxation measures on income related to the purchase or consumption of particular services. As a result, Canada would not be able to invoke this exception to justify its breach of the national treatment obligation. Additionally, the WTO includes no such exemptions for similar national treatment and MFN breaches. Additionally, Section 301 of the Trade Act sets out three types of acts, policies, or practices of a foreign country that are actionable: (i) trade agreement violations; (ii) acts, policies or practices that are unjustifiable (defined as those that are inconsistent with U.S. international legal rights) and burden or restrict U.S. commerce; and (iii) acts, policies or practices that are unreasonable or discriminatory and burden or restrict U.S. commerce. To emphasize, the United States would not need to determine that a DST violates a trade agreement in order to conclude that the measure is actionable under Section 301.

[210] 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.

[211] https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/september/readout-ambassador-jayme-whites-meeting-canadas-deputy-minister-international-trade-rob-stewart; 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; https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/september/readout-ambassador-jayme-whites-meeting-canadas-deputy-minister-international-trade-rob-stewart ("Ambassador White expressed continued U.S. concern with Canada's proposed unilateral digital service tax, and encouraged Canada to redouble its commitment to the Organization for Economic Cooperation and Development Two-Pillar process."). To emphasize,

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.[212] The broad definition of "harmful" content could lead to requirements to take down otherwise lawful content. 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.[213]

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.[214] 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.[215]

Audiovisual and Audio Services and Mandatory Local Content Quotas

The Online Streaming Act received Royal Assent and entered into law on April 27, 2023. Under the law, the CRTC is empowered to apply new "discoverability" and contribution obligations to any site of service hosting audio or audio-visual content (including "social media services") which would compel the service to both fund and give preferential treatment to Canadian content and creators.[216] The stated goal of the law 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." Canadian Heritage published a draft of its policy directive to the CRTC for implementation of the law on June 10, 2023,[217] but the draft regulations failed to address the key problems with the legislation: the failure to allow for foreign IP ownership for production in Canada and other characteristics of what could be deemed

---

the United States would not need to determine that a DST violates a trade agreement in order to conclude that the measure is actionable under Section 301.

[212] 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.

[213] *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/.

[214] 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

[215] *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

[216] Bill C-11 (Royal Assent), June 21, 2021, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-11/royal-assent.

[217] https://canadagazette.gc.ca/rp-pr/p1/2023/2023-06-10/html/reg1-eng.html.

"Canadian content;" commitment to not interfere with algorithms for "discoverability" requirements; and a commitment to exclude user-generated content altogether from the law. Although this draft policy directive has yet to be finalized, the CRTC has nonetheless already begun the process of developing implementing regulations.

The CRTC has released certain decisions—before the government has even finalized its guidance for the implementing regulations—that apply to a broad set of streaming services, including those with revenue over C$10M. Based on the draft regulations, podcast networks, most of which are U.S.-based, will be subject to the law. Despite the fact that U.S. streaming services invest billions of dollars every year into Canada's creative sector currently—which represents a significant portion of the total investment—neither the law nor the draft regulations require the CRTC to account for these investments when establishing mandatory minimum contribution requirements. The implementing regulations are a significant concern as they could disincentivize investments that are currently being made, while simultaneously harming customer choice, affordability, and companies' room to innovate in the Canadian sector.

The bill would, absent specific exemptions to be later developed, require all foreign online content providers to fund and institute preferences for arbitrarily-defined "Canadian content" and to "clearly promote" Canadian programming." The CRTC would be empowered to apply new "discoverability" obligations to any site of service hosting audio or audio-visual content (including "social media services" and podcasts) which—if pursued—would compel the service to give preferential treatment to Canadian content and creators.

The definitions for Canadian Content currently applicable to traditional broadcasters—whose obligations, if extended to online services as suggested by the government's projections of new revenue generated through the law[218]—generally disincentivize any foreign involvement in production, particularly by mandating that IP rights be owned by Canadian entities and individuals. Since much foreign production in Canada has not targeted the traditional broadcasting sector, but, rather, online distribution, this definition has not impeded foreign investment in production. But, if applied to online services, as envisaged in C-11, the effects could be highly detrimental.[219] Internet-enabled services, whose attractiveness depends on expansive libraries would suffer under rigid production requirements that would exclude many foreign producers. If the Online Streaming Act institutes obligations to spend on Canadian content or separately contribute to a fund dedicated to developing Canadian content through this law, ensuring U.S. companies have the ability to have self-produced (and owned) content qualify and the opportunity to access funding for such production could mitigate the discriminatory aspects of this law.

Additionally, the law directs the CRTC to "ensure the discoverability of Canadian programming services and original Canadian programs… in an equitable proportion," which could lead to interference in companies' curation of content and systems of recommendations. Sophisticated recommendation engines are one of the key benefits of an interactive video and audio experience

[218] https://www.scribd.com/document/638251923/Bill-C-11-Economic-Impact-PPT.

[219] https://www.scribd.com/document/638251923/Bill-C-11-Economic-Impact-PPT.

for both consumers and content producers, and help expose new artists and creators who may have otherwise not been discovered.

Although drafters of the Online Streaming Act sought to generally exclude user-generated content for the scope of the law, it is not clear that they succeeded, given definitional ambiguities and broad discretion granted to the CRTC. The potential for user-generated content to be caught up in this regulation also presents severe challenges for online streaming services operating in Canada; and, it likewise affects consumers seeking to express themselves, if their content must qualify under an arbitrary definition of being "Canadian" to reach public audiences. Although the law specifies that its obligations do not generally extend to social media services, it also provides broad discretion for CRTC to act otherwise and to create rules for monetized content on social media platforms—including user-generated content—if it determines it "necessary." The uncertainty and potential intrusiveness of regulating the provision of user-generated content looms large for foreign companies (and for content creators, both Canadian and foreign). The CRTC's September 29, 2023, decision that it is "neither necessary nor appropriate" to exempt social media suppliers from the obligation to register under the Online Streaming Act adds to the concern of the impact of the law on user-generated content.[220]

Representatives from the content creation, academic, and public interest communities have opposed the bill in addition to the streaming industry.[221] Such preferences are inconsistent with core provisions of the U.S.-Mexico-Canada Agreement ("USMCA") and CCIA urges USTR to actively engage to oppose such discriminatory measures.[222] Under USMCA's implementing legislation, USTR is required to evaluate any discriminatory measures pursued pursuant to the Cultural Industries exception, and consider appropriate actions to compensate for any adverse effects. CCIA urges USTR not to avoid its statutory obligation with respect to this measure as it is being implemented.

Restrictions on Cross-Border Data Flows

The Government of Quebec passed privacy legislation in September 2021 that, amongst other things, would make data transfers extraordinarily difficult.[223] The law entered into effect on September 22, 2022, with various provisions entering into effect in phases over three years and

---

[220] https://crtc.gc.ca/eng/archive/2023/2023-329.htm.

[221] 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/.

[222] https://ccianet.org/wp-content/uploads/2023/01/CCIA_Canada-Online-Streaming-Act_Bill-C-11_Whitepaper.pdf.

[223] *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.

the majority of the law entering into force September 22, 2023.[224] 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.[225]

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.[226] The legislation is currently being studied by the House of Commons Industry Committee. A key part of the legislation aims to update the country's current privacy law to be more aligned with European data protection and privacy standards, while also imposing new privacy protections for minors. Industry is concerned by a lack of a consistent definition of a minor (which currently differs between provinces in Canada) and lack of clarity on the exceptions for consent. Once approved by the House of Commons Committee, the bill will be studied in the Senate.

Regulations on the Trade of Artificial Intelligence Systems

Bill C-27 referenced above includes the Artificial Intelligence and Data Act, which seeks to establish "common requirements, applicable across Canada, for the design, development and use" of AI systems.[227] 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 opaque or undefined, leaving interpretations that could lead to disclosure of trade secrets, excessive punishments for innovators, and restrictions on services trade for online 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. Industry reports concerns that this legislation will introduce an overly burdensome regulatory framework, which would in turn endanger interoperability across the continent for services subject to these obligations.

An October 2023 letter from the Minister of Innovation, Science and Industry, François-Philippe Champagne, stating that the government seeks to include AI used in the "moderation of content

---

[224] https://iapp.org/news/a/2023-canada-private-sector-privacy-law-reform-keeping-track-of-moving-parts/; *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.

[225] 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.

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

[227] Id.

that is found on an online communications platform, including a search engine and a social media service" or the "prioritization of the presentation of such content" under "high-impact" could undermine online services providers' activity in the Canadian market given the potential broad-sweeping applicability of such a category.[228]

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.

Experimental Platform Regulation

On November 24, 2022, the Canadian Government opened a consultation seeking feedback on its initiative to update the Canadian Competition Act.[229] The consultation specifically requests public comment on data and digital markets, asking whether "sector-specific mechanisms" should be adopted and for suggested approaches for intersecting with privacy and data protection. The Government released a report, dubbed "The Future of Competition Policy in Canada," on November 22, 2022, as part of this effort. The report concluded that reforms could be necessary to address several modern-day competition issues, including "ensuring the necessary elements are in place to remedy unilateral forms of anti-competitive conduct, such as abuse of a dominant position, notably with regard to large online platforms" and "taking into account the implications of new technology and business practices for deceptive marketing provisions."

H. Chile

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Chapter 20-7 of the *Comisión para el Mercado Financiero*'s ("CMF") compilation of updated rules, *Recopilación Actualizada de Normas Bancos*, requires that "significant" or "strategic" outsourcing data be held in Chile. Under Chapter 20-7, cloud adoption is allowed based both on in-country cross-border supply, but financial institutions are obligated to have local data centers for contingency purposes when processing critical data and workloads overseas. This is a change from the 2017 version of the regulation which included no such obligation, and the 2019 version that only applied contingency obligations to banks lacking adequate risk management controls. By now expanding obligations to all financial institutions, many more entities will be subjecting to local data center obligations, since they do not meet CMF standards with respect to

[228] Letter from Honourable François-Philippe Champagne to Mr. Joël Lightbound, MP (Sep. 2023) https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12600809/12600809/MinisterOfInnovationScienceAndIndustry-2023-10-03-e.pdf.

[229] https://ised-isde.canada.ca/site/strategic-policy-sector/en/marketplace-framework-policy/competition-policy/making-competition-work-canadians-consultation-future-competition-policy-canada; https://laws-lois.justice.gc.ca/eng/acts/c-34/.

risk management. This has become an obstacle for data hosting services in Chile, as it pushes financial institutions to use local infrastructure offerings. Industry reports that in June 2023, the CMF cited the review of Chapter 20-7 as an aspect of 2023 priorities, but it has not yet achieved this goal.

Similar requirements are 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."[230] The bill would implement convoluted requirements for online platforms to conduct proactive monitoring of user activity to take down illegal content to avoid punishment,[231] while also limiting their ability to remove harmful legal content.[232] 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.[233]

Express Delivery Shipments

Under the U.S.-Chile Free Trade Agreement, Chile committed to expedited customs procedures for express shipments and to allow shipment operators "to submit a single manifest covering all

---

[230] 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.

[231] 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".")

[232] 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."").

[233] *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.

goods contained in a shipment transported by the express shipment service, through, if possible, electronic means." However, there are significant delays in imports coming through the border due to the current customs systems' inability to process the data from a variety of carriers.

I. China

The Chinese market continues to be hostile to foreign companies, and 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.[234] 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.[235] The United States International Trade Commission has estimated billions of dollars are being lost in the market as a result.[236] 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 3,000 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.[237]

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

---

[234] Richard Bowman, *Rise of China's Tech Giants – What to Know When Investing in Chinese Tech Companies*, CATANA CAPITAL (Aug. 3, 2020), https://www.lehnerinvestments.com/en/investing-chinese-tech-companies/; Dan Wang, *China's Hidden Tech Revolution How Beijing Threatens U.S. Dominance*, Foreign Affairs (March/April 2023) https://www.foreignaffairs.com/china/chinas-hidden-tech-revolution-how-beijing-threatens-us-dominance-dan-wang.

[235] 2023 CCIA NTE Comments, https://ccianet.org/wp-content/uploads/2022/10/CCIA-Comments-2023-National-Trade-Estimate-Reporting.pdf at 47-54.

[236] . 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 to be if it could operate in the 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.

[237] 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.

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.[238] There is confusion regarding how this draft affects prior draft legislation on cross-border data and localization mandates issued pursuant to the Cybersecurity Act.[239]

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.[240] "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."[241]

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.[242] The draft amendments released on February 1, 2019 set out the following: enhanced notice and consent requirements, new requirements on personalized recommendations and target advertising, requirements on access by third parties and data integration, revised notification requirements for incident response, and requirements to maintain data processing records.[243]

The two draft Measures above are reportedly being submitted for deliberation during the National People's Congress term ending in 2023.[244]

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

---

[238] 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/.

[239] 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").

[240] 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/.

[241] *Id.*

[242] 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/.

[243] 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/.

[244] 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/.

that would harm the "national security, public interest, or lawful interests of citizens or organizations" in China.[245] 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.[246] 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.[247]

In August 2021, the Personal Information Protection Law was passed. The law went into effect on November 1, 2021.[248] 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 transfer of personal information data will add burden to multinational companies and limit the ability of U.S. companies to operate in China. The framework establishes three avenues for cross-border data flows—primarily security assessments, protection certifications, and standard contracts.

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.

---

[245] 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/.

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

[247] *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.

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

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.[249] The draft rules seek to strengthen a data security law established in September 2021 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 2022 which sought to reinforce data security checks for firms engaging in cross-border data flows.[250] 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.[251] 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 Cyberspace Administration of China (CAC) released the final version of their Measures on the Standard Contract for the Cross-border Transfer of Personal Information Guidance on February 22, 2023.[252] There are three legal mechanisms through which organizations can transfer personal information out of China. The first is by undergoing a CAC security assessment, and certain organizations that transfer CAC defined "important data" as well as above a certain threshold of personal information must file for the assessment. The second is through entering into a Standard Contract with the recipient outside of China, and third is through obtaining a certificate from a CAC-recognized professional organization. While in the past China's data security measures mostly targeted companies with larger user bases, these new measures will sweep in smaller companies who partake in data transfers as well. The measure took effect on June 1, 2023, and there is a 6-month grace period for companies to take the necessary steps to comply that will end in November 2023.

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 introduced specific obligations dictating the assessments for data exit security, including a requirement for data processors to conduct a data exit risk self-evaluation before seeking an application.

---

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

[250] *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/.

[251] *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/.

[252] https://www.lexology.com/library/detail.aspx?g=f9bfb93a-2e6b-4fab-8c34-0f5b195dc851.

In addition to the Measures, the government promulgated regulations and standards governing protection certification and standard contracts for the cross-border transfer of personal information, under a cross-border personal data flow management mechanism. This mechanism introduces significant obstacles by imposing compliance burdens and costs for data processors. Foreign companies are required to disclose corporate data-mapping and cross-border data flow transfer routes—disclosures that risk publicizing trade secrets and key IPR. Industry reports that roughly 1,000 applications were filed in China in 2022, with less than a tenth of the applications receiving official approval as many of the 90% yet to see approval needing supplementary information.

The export from China of the ill-defined category of "important" data also requires a security assessment, but the definition of important data and implicated catalogues have not been finalized. Data handlers in certain crucial sectors are therefore experiencing significant uncertainty. Industry reports a trend of industry regulators taking advantage of the concept of important data and broadening it by introducing *de facto* data localization and cross-border data flow restrictions in the financial services, automotive, ride-sharing, online publication, mapping, and pharmaceutical industries.

Critical Information Infrastructure ("CII") 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 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. Industry reports that in the past two years, authorities in various sectors have introduced regulations and standards relating to CII. In May 2023, China's first national standard for CII security protection, dubbed "Information Security Technology—Cybersecurity Requirements for CII Protection GB/T 39204-2022," became effective.[253] Elsewhere, the Ministry of Transport put forward the "Administrative Measures for the Security Protection of CII for Highways and Waterways," which went into effect on June 1, 2023.[254]

The Cybersecurity Review Measures (CSRM) were adopted on January 4, 2022, which instituted mandatory cybersecurity reviews for CII operators that procure network products and services as well as online platforms that implicate influence national security. Industry reports a review process lacking transparency but that is expected to address security, openness, transparency, and diversity of sources of products and services; the reliability of supply channels; and the levels of risk of disruptions to the supply chain. Micron failing a CAC cybersecurity review in early 2023 demonstrates the restrictive effect of these policies, as it led to CII operators curtailing purchases from Micron. Given their opaque criteria and wide-reaching scope, there is a concern that

[253] https://practiceguides.chambers.com/practice-guides/cybersecurity-2023/china/trends-and-developments.

[254] https://practiceguides.chambers.com/practice-guides/cybersecurity-2023/china/trends-and-developments.

China's cybersecurity review regime could be manipulated to discriminate against U.S. and other foreign technology providers.

On November 18, 2022, the State Administration for Market Regulation and the Cyberspace Administration of China together announced the Rules on Implementation of Personal Information Protection Certification,[255] which implemented a framework for the certification for protecting personal information.[256] The rules govern entities which process personal information, including actions such as collecting, storing, handling, transmitting, disclosing and deleting data, as well as processing it across borders. Personal information processors will be required to comply with two standards along with other data protection laws: "Security Certification Specification for Cross-border Processing of Personal Information" and "Information Security Technology — Personal Information Security Specification." To uphold certification standards, it will require conducting a technical verification, examining the data on-site, and supervising the information following certification.

On September 28, 2023, the CAC introduced new draft provisions on regulating and promoting cross-border data flows that would decrease the scenarios where data exit security assessment would be necessary.[257] In particular, the consultation draft proposes exempting personal data transfers for the purpose of human resource management and contractual transactions, including cross-border e-commerce, payments, plane ticket purchases and hotel bookings, and visa applications. Industry remains concerned due to the uncertainty of the timeline for when these draft provisions will be enacted, or if the proposals will be enacted at all.

Regulations Governing Services that use Generative Artificial Intelligence

On July 13, 2023, the Cyberspace Administration of China (CAC) finalized its rules—the Interim Measures for the Management of Generative Artificial Intelligence Services—imposing oversight of generative artificial intelligence services.[258] The rules, which apply to generative AI systems being supplied for the general public, will require providers to receive a license and register with regulators to provide their services in China. Suppliers are further required to use technical means to avoid the generation of illegal content or false information, change the algorithm when such content is found, and report it to officials. Additionally, suppliers are subjected to a variety of requirements for treating the training data of generative AI systems relating to IP rights, personal data, authenticity, and accuracy. Suppliers must conform to "socialist values" in providing their services and are required to implement anti-addiction tools for their users. The rules also institute privacy provisions that set limits on information retention for these providers and require them to establish mechanisms for handling user complaints and mechanisms to stop generation when infringement is discovered. Further, providers are barred from using algorithms, data, platforms, and other advantages to restrict competition, but details regarding what practices would trigger a violation have yet to be provided. Lack of an effective

[255] Text at: http://www.cac.gov.cn/2022-11/18/c_1670399936983876.htm.

[256] https://www.lexology.com/library/detail.aspx?g=d219cacd-5966-472b-8314-205ce5528906.

[257] *China Proposes to Ease Oversight of Cross-Border Transfer of Personal Information*, ROPES & GRAY (Oct. 10, 2023), https://www.ropesgray.com/en/insights/alerts/2023/10/china-proposes-to-ease-oversight-of-cross-border-transfer-of-personal-information.

[258] http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm.

consultation process was striking: the CAC issued its draft policy on April 11, 2023, and provided less than 30 days for comment.[259] The subsequent measures went into effect on August 15, 2023.

National Treatment in Standardization

Industry has expressed concern regarding China's Standardization Law, which often form the basis for regulations imposing security and technological requirements necessary for participation in the Chinese market. For example, the cryptographic standards adopted by China and referenced in regulation mandate that firms use China-developed cryptographic algorithms 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.

Threats to Encryption and Security of Devices

China's Cryptography Law went into effect on January 1, 2020,[260] and introduced three categories governing encryption technologies: "core," "common," and "commercial." The definitions of the "core" and "common" encryption categories reflect encryption employed to shield information that are deemed as state secrets. Commercial encryption refers to technology used to protect information that is deemed to not be state secrets. In April 2023, the government amended the Commercial Cryptography Administrative Regulations,[261] however, these amendments undermine the interoperability of international standards and internationally standardized encryption algorithms. Industry is concerned by this move, as it reflects a vast import license/export control scheme, involves opaque clauses that could impose a *de facto* mandatary certification requirement, and introduces obligations applicable only to CII and party and government institutions to networks above China's Multi-level Protection Scheme (MLPS) level three. These regulations will result in foreign companies that depend on encryption algorithms to protect data and services facing high compliance costs and thus represent yet another market access barrier.

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

[259] https://digichina.stanford.edu/work/translation-measures-for-the-management-of-generative-artificial-intelligence-services-draft-for-comment-april-2023.

[260] *New Chinese Cryptography Law in Force*, PwC (Jan. 13, 2020), https://legal.pwc.de/de/news/fachbeitraege/new-chinese-cryptography-law-in-force-as-of-1-january-2020.

[261] *China to Regulate Commercial Cryptography*, CHINA JUSTICE OBSERVER (July 17, 2023), https://www.chinajusticeobserver.com/a/china-to-regulate-commercial-cryptography.

positive balance of trade.[262] 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.

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.[263]

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 should 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.

All telecommunications business in China are subject to cumbersome licensing requirements. Foreign companies' participation in value added telecommunication (VAT) sector is therefore significantly impeded. Several policies—"Telecommunications Regulations of the People's Republic of China," "Classification Catalogue of Telecommunications Services," and "Special Administrative Measures for Foreign Investment Access (Negative List) (2021 Version),"—in tandem prohibit foreign companies from having access to the business sectors that are essential for cloud services, particularly Internet data center (IDC) business, and content distribution network (CDN) service. Industry is concerned that the progress on this issue has stalled, despite efforts in other sectors noted in the August 2023 "Opinions on Further Optimizing the Foreign Investment Environment and Increasing Efforts to Attract Foreign Investment."[264]

---

[262] Synergy Research Group, Cloud Market Growth Rate Nudges Up as Amazon and Microsoft Solidify Leadership (Oct. 29, 2020), https://www.srgresearch.com/articles/cloud-market-growth-rate-nudges-amazon-and-microsoft-solidify-leadership.

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

[264] https://www.wilmerhale.com/insights/client-alerts/20230815-china-issues-policy-to-further-boost-foreign-investment.

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.[265] 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.[266]

On November 16, 2022, the Cyberspace Administration of China announced new rules governing the monitoring and policing of posts, comments, and likes on social media services.[267] "Post comment service providers" will be required to review comments before posting them, monitor activity on the platform in real time, collect information regarding users' identities, and police whether individual users react with "likes" to harmful or illegal content. As other authoritarian and repressive regimes look to China for guidance on internet regulation, the expansion of prior digital surveillance and requirements for providers warrants concern. The new rules will replace the 2017 regulation, "Regulations on the Administration of Internet Posting and Commenting Services," and went into effect on December 15, 2022.

China's Ministry of Public Security, the Supreme People's Procuratorate and the Supreme People's Court drafted guidelines that were open for public opinion about cyber bullying and doxxing. The guidelines would make certain actions criminal offenses, as well as allow for convictions of defamation for people who spread rumors that demean others or damage their reputation. Online service providers would be required to enhance their monitoring and removal of cyberbullying content, as well as take measures to facilitate evidence collection, and if providers fail to comply, authorities could require them to suspend content updates, as well as penalize them financially. The Cyberspace Administration published a draft of the regulation on July 7, 2023, and solicited public feedback.[268]

---

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

[266] 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.

[267] http://www.cac.gov.cn/2022-11/16/c_1670253725725039.htm; https://www.cnn.com/2022/11/30/media/china-new-internet-rule-punish-liking-posts-intl-hnk/index.html.

[268] https://www.bloomberg.com/news/articles/2023-07-07/china-warns-its-tech-giants-to-rein-in-cyberbullying.

J. Colombia

Copyright Liability Regimes for Online Intermediaries

Colombia has failed to comply with its obligations under the 2006 U.S.-Colombia Free Trade Agreement to provide protections for Internet service providers.[269] Revision to the legislation in 2018 that sought to implement the U.S.-Colombia FTA copyright chapter includes no language on online intermediaries.[270] 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.

Taxation of Digital Products and Services

In November 2022, the Colombian government approved a significant economic presence (SEP) framework that would impose a new tax on gross income earned by overseas providers of goods and digital services in-country. The SEP rule (Law 2277/22, Article 57) distinguishes between goods and digital services, though exporters of both are subjected to certain combined obligations as well.[271] For both goods and services, an entity is deemed in-scope if it has a deliberate and systematic interaction with the Colombian market, defined as interacting with 300,000 or more users or customers located in Colombia. Further, an entity is treated as in-scope if it earns a gross income of roughly $300,000 or more from consumers within Colombia. The tax applies to both the sale of tangible goods and certain digital services, such as cloud services. Because of this distinction, the SEP provisions affect companies in the digital services sector more than those in other industries.

The rule institutes a 10% withholding tax on a non-resident with an entity determined to be an SEP in Colombia. The tax is applied at the source, on the total payment earned by the non-resident for the sale of goods and/or provision of services. A withholding rate of 10% is high compared to other enacted DSTs and similar measures. An alternative regime exists whereby a non-resident is able to pay a 3% tax on the gross income earned through selling goods and/or providing digital services if they are registered. The SEP rule is expected to enter into force on January 1, 2024, and would mark the first DST imposed in the Latin American region.

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 Organisation for Economic Co-operation and Development to address global tax fairness. This tax violates the spirit of both the 2021 OECD/G20 Inclusive Framework and the conditional, one-year extension of the pause on DSTs reached in July 2023. Industry is concerned by signals that despite approving both extensions, the Colombia

---

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

[270] 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/.

[271] https://assets.kpmg.com/content/dam/kpmg/us/pdf/2022/12/tnf-colombia-dec19-2022.pdf.

government continues its plans to move forward. A new gross-basis tax imposed on non-residents of Colombia on income derived from sales to the Colombian market and would create barriers to trade to U.S. companies engaging with the Colombian market. 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.[272]

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Colombia government contracted a technical analysis in May 2023 through the Inter-American Development Bank regarding the governance and deployment of the data infrastructure that would be needed to improve how the government administers, stores, and analyses data as well as the availability and sovereignty of that data. The project envisages the creation of a Private Cloud for the government. As part of this pursuit, the project is working to identify the current and projected 10-year needs for the storage, analysis, and management of data for all national government entities, with the goal of protecting data, shielding critical infrastructure, and securing key efficiency gains in the investment of public resources.

Industry is also tracking calls from the government to localize data in Colombia following a series of cyberattacks that took down the websites of several government agencies and led to officials calling to minimize cloud-based data storage to instead rely on on-premises infrastructure for essential services provided by the government.

Trade Facilitation

Colombia committed to modernize its customs procedures in the USCTPA by implementing automation and electronic systems.[273] Colombia also committed to implement expedited customs procedures for express shipments, including fully integrating express shipments into Colombia's Single Window.[274] The submission and processing of information required for the release of an express shipment before its arrival should be a target for any expedited procedures,

---

[272] The new tax is effectively the same as a tariff, as it increases the price of imported goods and does not apply to domestic equivalents. As the SEP applies to providers of digital services, the tax would *de facto* discriminate against U.S. service suppliers. These features of the new tax contravene several commitments agreed to through the USCTPA including Articles 2.3 (no new customs duties on originating goods), 2.8 (no restrictions on the importation of any goods of another party) and 15.3 (no new customs, duties, fees, or other charges on digital products) under the USCTPA. In addition, Article 11.5 of the USCTPA prohibits Colombia from requiring that U.S. service suppliers be required to maintain a local presence as a condition for the cross-border supply of a service. The decreased 3% tax rate for non-residents that choose to register incentivizes the establishment of local presence, as Colombian legislation does not include methods for foreign entities without a permanent presence in Colombia to file an income tax return. Therefore, in order for any foreign entity to benefit from the lower rate, it is *de facto* required to establish a local presence.

[273] See Article 5.3 that stipulates that each party shall "provide for electronic submission and processing of information and data before arrival of the shipment to allow for the release of goods on arrival" and "employ electronic or automated systems for risk analysis and targeting."

[274] See Articles 5.2, 5.3, and 5.7.

as should allowing for a single manifest through electronic means, when feasible. However, industry is concerned as the Colombian government has not adopted these commitments, as physical documents are still obligatory.

K. Croatia

Taxation of Digital Products and Services

The government of Croatia announced plans to pursue a digital services tax, based on the Austrian DST model opposed by USTR in 2022.[275] CCIA urges USTR to encourage Croatia to adhere to the OECD/G20 Inclusive Framework as a method to address tax challenges of the digitalizing global economy rather than pursue discriminatory taxes on U.S. suppliers.

L. Cuba

Government-Imposed Restrictions on Internet Content and Related Access Barriers

There have been many cases of the Cuban government disrupting access or blocking certain Internet services to stifle political dissent and organization.[276] 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. [277] 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 country or that provoke acts "that alter public order."[278] The definitions behind false information and public safety are extremely vague and left in the hands of the government authorities.[279]

---

[275] *Croatia Parliament Considers Bill on Digital Services Taxation*, BLOOMBERG TAX (July 7, 2022), https://news.bloombergtax.com/daily-tax-report/croatia-parliament-considers-bill-on-digital-services-taxation?context=article-related.

[276] *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.").

[277] *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-protests-internet-watchdog-2021-07-13/.

[278] 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.

[279] *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/.

M. Czech Republic

Forced Revenue Transfers for Digital News

The implementation of the EU Copyright Directive in the Czech Republic was published in December 2022 and went into effect in January 2023,[280] which represented a marked shift away from other EU member states' implementation of the directive, and threatens 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 offer their services effectively and to fight disinformation.[281] 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 1% of a company's turnover worldwide.

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.[282] 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.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Czech government's National Cyber and Information Security Agency (NÚKIB) is in the process of implementing the EU NIS 2 Directive through a new draft Cybersecurity Act.[283] Industry reports that the current version of the legislation has proposed to place data from public administration information systems at the critical risk scale (level 4), which would restrict data processors to storing data of this category in servers located in the Czech Republic. Such a restriction would pose a burden to U.S. and foreign cloud services suppliers seeking to offer such services in the country.

---

[280] https://www.twobirds.com/en/trending-topics/copyright-directive/copyright-directive-countries/czech-republic.

[281] https://developers.google.com/search/blog/2022/12/google-services-in-czechia.

[282] *See* text of the law: https://www.sagit.cz/info/sb22429; https://www.psp.cz/sqw/sbirka.sqw?O=9&T=31; Updates to Google's Services in Czechia in Light of the Czech Transposition of the European Copyright Directive, Google Search Central Blog (Dec. 12, 2022) https://developers.google.com/search/blog/2022/12/google-services-in-czechia.

[283] *New Czech Cybersecurity Regulation What You Need to Know*, DLA PIPER (Aug. 16, 2023), https://www.dlapiper.com/en/insights/publications/2023/08/new-czech-cybersecurity-regulation-what-you-need-to-know; Directive available at: https://osveta.nukib.cz/course/view.php?id=168.

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" and "strategic autonomy." European politicians have stated that the purpose of technological autonomy is to create a "new empire" of European industrial powerhouses to resist American rivals and to turn Europe into a "tech and digital global leader."[284] 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 disadvantage U.S. exporters to the benefit of domestic EU competitors and will likely also undermine Europe's long-term prospects for digital innovation.

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.[285]

Restrictions on Cloud Services Providers

As part of the EU-wide push for "technological sovereignty," the EU has advanced industrial policy proposals that will force U.S. cloud providers out of key segments of the EU market. 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 Scheme for Cloud Services (EUCS).[286] A second, May 2023, draft of the certification would prohibit companies headquartered outside the EU or owned or controlled by non-EU entities from receiving the highest level of cybersecurity certification; impose stringent data localization requirements; and oblige customer support employees to be located in the EU. One of the scheme's stated objectives is to ensure that the highest level of cloud services is "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."

---

[284] *Tech and Geopolitics: Building European Resilience in the Digital Age*, Thierry Breton on LinkedIN (Sep. 5, 2023) https://www.linkedin.com/pulse/tech-geopolitics-building-european-resilience-digital-thierry-breton/; 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/.

[285] *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/.

[286] 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.

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.[287] 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.[288]

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,[289] any number of "important entities" regulated under said Directive,[290] 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 implemented in conformity with WTO rules.

Building on the EUCS, the European Commission recently announced the launch of new measures to "de-risk" Europe's dependence on a wide range of ICT products to strengthen the bloc's "economic security."[291] Many of those ICT products are currently supplied by U.S. companies,[292] and include: microelectronics, including processors, high performance computing, cloud and edge computing, data analytics technologies, computer vision, language processing, object recognition, and quantum technologies. Other potentially critical technologies which the EU may seek to advance its "de-risking" strategy includes: cyber security technologies such as security and intrusion systems and digital forensics, Internet of Things and virtual reality, secure communications including Low Earth Orbit (LEO) connectivity, and AI-enabled systems. For all those technologies, the European Commission seeks to prevent technology security and leakage and the weaponization of economic dependencies and economic coercion, and ensure the resilience of supply chains and the physical and cyber-security of critical infrastructure. The

---

[287] 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.

[288] 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.

[289] 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.

[290] 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;

[291] Press Release: Commission recommends carrying out risk assessments on four critical technology areas: advanced semiconductors, artificial intelligence, quantum, biotechnologies (Oct. 3, 2023), https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4735.

[292] Only a limited number of critical technologies identified by the European Commission are dominated by Chinese firms. The full list of critical technology areas for the EU's economic security available on https://defence-industry-space.ec.europa.eu/system/files/2023-10/C_2023_6689_1_EN_annexe_acte_autonome_part1_v9.pdf

European Commission will work with national governments to complete the first round of risk assessments by the end of 2023. Based on those assessments, the European Commission will reportedly announce new measures to mitigate economic dependencies by spring 2024.

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 U.S. industry from public procurements.[293] 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 now-enacted EU's e-Evidence Regulation,[294] 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.

Restrictions on Cross-Border Data Flows

The Data Act builds 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.[295] The Data Act features 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;" creating a separate regime for non-personal data transferred internationally for cloud services providers subject to third party countries' data access requests;[296] 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 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.

---

[293] *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.

[294] *Council adopts EU laws on better access to electronic evidence*, European Council (June 27, 2023) https://www.consilium.europa.eu/en/press/press-releases/2023/06/27/council-adopts-eu-laws-on-better-access-to-electronic-evidence/; 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/.

[295] Final compromise text, Data Act, Doc. 11284/23 (Jul. 7, 2023), https://data.consilium.europa.eu/doc/document/ST-11284-2023-INIT/en/pdf.

[296] Speech, A European Cyber Shield to step up our collective resilience | Opening of the International Cybersecurity Forum, by Commissioner Thierry Breton (Apr. 5, 2023): "We have also adapted our regulatory framework through the Data Governance Act and the Data Act by inserting anti-Cloud Act clauses, because it is not acceptable that the data of Europeans can be accessed in an unjustified manner" https://ec.europa.eu/commission/presscorner/detail/en/speech_23_2145

The EU's Data Governance Act 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.[297] These restrictions are similar to the General Data Protection Regulation ("GDPR") ranging from "adequacy decisions," consent, standard contractual clauses, as well as an outright ban for sensitive non-personal data.[298] 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.[299]

The updated cybersecurity legislation ("NIS2") 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).[300] The European Parliament and EU Member States reached a political agreement on the legislation in May 2022.[301] It entered into force on January 16, 2023, and must be transposed into national law by each member state by October 17, 2024. The legislation includes the obligation for such providers to be certified against an EU certification scheme to be developed under the EU Cybersecurity Act ("CSA").[302] The NIS2 Directive will 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 above.

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, particularly small businesses. The General Data Protection Regulation (GDPR) went into effect on May 25, 2018.[303] 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

---

[297] 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.

[298] *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.

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

[300] 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.

[301] 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.

[302] *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.

[303] 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"].

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.[304]

Since the adoption of the GDPR, the European Union has continuously amended its data protection rules through several legislative proposals and recently enacted regulations, leading to regulatory instability coupled with asymmetric regulation aimed at U.S. companies. For instance, the Digital Markets Act (DMA) prohibits five U.S. companies from performing innocuous data processing unless they obtain user consent.[305] No European firms are subjected to this new restriction. The Data Act also prohibits the same five U.S. firms from receiving data to any service they operate even if users choose to do so. This prohibition conflicts with data portability provisions in GDPR and DMA.[306] The Digital Services Act (DSA) forecloses the users' right to consent to online advertising based on "special categories of data."[307] Innocuous data processing for online messaging and email functionalities could also be only possible based on user consent according to the e-Privacy Regulation Proposal.[308]

Between the 2020 ruling and the adoption of the new EU-U.S. adequacy decision in 2023, thousands of companies have been impacted by the resulting legal uncertainty for transatlantic data transfers, restrictive interpretations of the ruling risk triggering additional compliance and operational challenges. CCIA applauded the signing of the Executive Order to enhance the privacy safeguards for signals intelligence activities,[309] and the EU's formal adoption of the new EU-US Data Privacy Framework.[310]

However, a decision from the European Data Protection Board (EDPB) suggests that companies can be held liable retroactively for any personal data transfers to the United States which have taken place between the 2020 CJEU decision and the entry into force of the EU-U.S. adequacy decision in 2023. The EDPB finds that such transfers constitute an infringement of the EU personal data transfer rules "with at least the highest degree of negligence," which, in the present

---

[304] 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.")

[305] See Article 5(2) DMA and Article 6 GDPR

[306] Press Release: Data Act's Undue Data Portability Restrictions: CCIA Requests EU Privacy and Competition Enforcers To Step In (Jun. 15 2023), https://ccianet.org/news/2023/06/data-acts-undue-data-portability-restrictions-ccia-requests-eu-privacy-and-competition-enforcers-to-step-in/

[307] See Article 26(3) DSA and Article 9(2)(a) GDPR

[308] 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"].

[309] 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/.

[310] Press Release, EU Countries Seal Data Transfer Deal With United States After Years of Uncertainty (Jul. 10, 2023), https://ccianet.org/news/2023/07/eu-countries-seal-data-transfer-deal-with-united-states-after-years-of-uncertainty/

case, resulted in the highest GDPR fine ever imposed on an organization.[311] Separately, French lawmaker Philippe Latombe is seeking to annul the European Commission adequacy decision. Incidentally, MP Latombe has repeatedly tabled amendments to various bills seeking to exclude U.S. cloud providers from public and private contracts through mandatory SecNumCloud certification for cloud services to provide services to "critical infrastructures" and to handle French citizens' health data.[312]

Foreign Subsidies Regulation

On July 12, 2023, the Foreign Subsidies Regulation ("FSR") came into effect.[313] Under the new rules the Commission has broad powers to receive sensitive business information involving non-EU government contracts. The Commission also has broad discretion to decide whether a non-EU subsidy distorts the EU single market and to impose strict sanctions.

From October 2023, the Regulation will broadly define non-EU subsidies as any financial contribution provided directly or indirectly by a non-EU Government that confers a benefit and is limited to an individual business or industry or several businesses or industries. This includes, but is not limited to, tax credits, tax exemptions, film credits, preferential tax treatment, cash grants, and the broad category of "the provision of goods or services or the purchase of goods or services" for up to three years before their participation in a series of actions.[314] These actions include public procurement procedures with a tender upwards of €250M and mergers and acquisitions where the parties' aggregate EU revenues are greater than €500M. Additionally, the Regulation confers an *ex officio* tool upon the Commission to investigate financial contributions on an *ad hoc* basis, that went into effect in July 2023. If the Commission determines that an entity has benefitted from "distortive" subsidies, it could subsequently disqualify them from future public tenders and EU mergers and acquisitions and impose regressive measures such as subsidy repayments.

The Regulation 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

---

[311] Press Release, 1.2 billion euro fine for Facebook as a result of EDPB binding decision, European Data Protection Board (May 2023), https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

[312] See amendment to require all critical infrastructures to use SecNumCloud certified products: https://www.assemblee-nationale.fr/dyn/16/amendements/1033/CION_LOIS/CL38; and amendment to require public and private health organization to use SecNumCloud certified products to handle French personal health data: https://www.assemblee-nationale.fr/dyn/16/amendements/1514/ESPNUM/765 and

[313] Regulation (EU) 2022/2560 of the European Parliament and of the Council of 14 December 2022 on foreign subsidies distorting the internal market https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2560&qid=1673254237527

[314] *Id.* Article 3.

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 July 2023, the Commission published an Implementing Regulation (IR) establishing procedural mechanisms for applying the Foreign Subsidies Regulation that narrowed the focus of the FSR. This winnowing of the scope of the regulation includes restricting the most burdensome and in-depth reporting requirements to a narrow range of subsidies deemed to be the "most likely to distort;" absolving contracts for the supply and purchase of goods and services on market terms from reporting requirements; and allowing general tax measures and incentives that are valued at less than €1M to not be subjected to notification. While these changes reflect strong progress for industry by limiting regulatory burdens, obstacles remain. Particular incentives fall within the scope of the regulation, but would not have to be notified if conferred by an EU Member State, such as some audiovisual incentives and R&D tax credits. In addition, the Commission has not provided any assurances or guidelines relating to *ex officio* measures, which has caused uncertainty for foreign firms and brought the possibility of discriminatory enforcement.

In this context, the Regulation 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 Regulation 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 captures any company receiving any form of benefits or compensation from a non-EU state authority.[315]

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

In response to a campaign from incumbent European telecommunications providers, the European Commission launched an exploratory consultation in February 2023 asking for input on the suggestion that "large traffic generators" should make financial contributions, termed "network usage fees," to European telecommunications network operators to support network deployment."[316] The incumbent telco association ETNO suggests that large U.S. content access

[315] 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.

[316] European Commission, The future of the electronic communications sector and its infrastructure (Feb. 2023); available at https://digital-strategy.ec.europa.eu/en/consultations/future-electronic-communications-sector-and-its-infrastructure.

providers (CAPs) should be required to pay fees to European ISPs for the content demanded by the ISPs' customers.

The initial ETNO report spurred European lawmakers' encouragement for a proposal to force "Big Tech" companies to pay ISPs for receiving their traffic. The ETNO report cites solely American companies as responsible for the traffic that requires subsidizing.[317] Network usage fees would likely be imposed predominantly on U.S. online services suppliers that offer content and applications in Europe that have garnered significant consumer demand. Industry is concerned as the exploratory consultation appeared to accept the false "fair share" premise pushed by European telecom incumbents, with questions seemingly designed to justify the idea that popular streaming and cloud services should be mandated by the EU to subsidise telecom operators. Further, given their technical nature, most consultation questions could only be answered by tech and telecom firms, thus excluding most stakeholders.[318]

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.[319] 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."[320] 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 proposal of the incumbent telecommunications providers has been challenged by some member states, seven of whom suggested slowing down the process to avoid unintended

---

[317] 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.

[318] Press Release, Network Fees: EU Commission Launches Consultation on Telco Demands (Feb. 2023),

https://ccianet.org/news/2023/07/eu-countries-seal-data-transfer-deal-with-united-states-after-years-of-uncertainty/

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

[320] *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/.

consequences of implementing a SPNP requirement,[321] and several others echoed those concerns mid-2023.[322] 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 later explained that: "[...] a mandatory payment [...] limited only to certain players (such as "LTGs") [...] would go against the principle of net neutrality as set out in recital 1 of the OIR. This is because it involves treating traffic unequally, contradicting the principles of equal treatment and nondiscrimination enshrined in Article 3(3) of the OIR." BEREC also states that "a mandatory payment from CAPs to ISPs is likely to increase the bargaining power of ISPs due to their market position regarding termination monopoly of traffic, [and] ISPs are likely to be able to discriminate and self-preference their own services (e.g., related to streaming or cloud)."[323]

The Commission released a summary of the responses received in the public consultation in October 2023, where it was documented that a majority of respondents opposed any mandatory funding mechanism.[324] Arguments against the proposal focused on the inconsistency with net neutrality principles, the harms it would impose on innovation, and the damage it could bring for competition and consumers (such as a decrease in the range of content available and/or higher prices for internet services). However, industry is concerned that the Commission has signaled an intent on imposing network usage fees regardless of this finding. The Commission deemed the consultation results "not conclusive" on the question of implementing network usage fees (despite the overwhelming opposition) and EU Commissioner Thierry Breton said that "Europe will do 'whatever it takes' to keep its competitive edge" including by "finding a financing model" for the EU telecommunications industry, potentially through new legislation (such as a "Digital Networks Act").[325] Breton has foreshadowed a white paper providing a strategy framework expected from the Commission in the first quarter of 2024, and the Commission's published work plan for 2024 also includes the topic of network usage fees: "Following the recent exploratory consultation, we will prepare the ground for possible policy and regulatory actions regarding Digital Networks and infrastructure, notably to facilitate cross-border

---

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

[322] *Majority of EU countries against network fee levy on Big Tech, sources say*, Reuters (June 3, 2023) https://www.reuters.com/business/media-telecom/majority-eu-countries-against-network-fee-levy-big-tech-sources-say-2023-06-02/.

[323] BEREC response to the European Commission's Exploratory Consultation on the future of the electronic communications sector and its infrastructure Annex to complement section 4 of the BEREC response, BoR (23) 131d (May 19, 2023) https://www.berec.europa.eu/system/files/2023-05/BoR%20%2823%29%20131d%20Annex%20to%20Section%204.pdf.

[324] *EU consultation on future telecoms cools on having big tech pay for network builds,* The Register (Oct. 12, 2023) https://www.theregister.com/2023/10/12/europe_comms_sector_future_consultation/; *Network Usage Fees: The European Commission Plays Politics with the Global Internet*, Internet Society (Oct. 19, 2023) https://www.internetsociety.org/blog/2023/10/network-usage-fees-the-european-commission-plays-politics-with-the-global-internet/.

[325] Thierry Breton, A 'Digital Networks Act' to redefine the DNA of our telecoms regulation (Oct. 2023), available at https://www.linkedin.com/pulse/digital-networks-act-redefine-dna-our-telecoms-thierry-breton/.

infrastructure operators in the Single Market, accelerate deployment of technologies and attract more capital into networks."[326]

CCIA urges USTR to continue engaging firmly to dissuade the advancement of discriminatory and anticompetitive rules forcing network usage fee in whatever name or form,[327] and welcomes U.S. government engagement on this issue,[328] which appears to have materially helped resist the adoption of this policy so far. Industry is pleased to see the engagement of the United States follow the government's consistent opposition to network usage fees. The United States cautioned the EU to "avoid discriminatory measures that distort competition" and argued that "it is difficult to understand how a system of mandatory payments imposed on only a subset of content providers could be enforced without undermining net neutrality" in its filing before the European Commission. [329] The United States and partner nations rejected this proposal when advanced by the European Telecommunications Network Operators' Association (ETNO) a decade ago.

Experimental Platform Regulation

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 adopted by the European Parliament and the Council of the EU on September 14, 2022.[330] The measure entered into force on November 1, 2022, and became applicable on May 2, 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 end and business users. These thresholds have been set at levels where primarily U.S. technology companies fall under scope, reflecting some policymakers' intent to ensure this outcome.[331] The list of "core platform services" furthermore carves out non-platform-based business models of large European rivals in media, communications, and advertising. As of October 2023, the European Commission has designed six companies as the so called "gatekeepers" under the DMA, and in total 22 of their services will be subject to the new rules. Five out of those six companies (the sixth is Chinese) and 21 of the 22 services are American.[332]

---

[326] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=COM:2023:638:FIN.

[327] https://blog.cloudflare.com/eu-network-usage-fees/.

[328] https://www.ntia.gov/other-publication/2023/united-states-comments-european-consultation-future-electronic.

[329] https://www.ntia.gov/other-publication/2023/united-states-comments-european-consultation-future-electronic.

[330] Official Journal of the European Union (Oct. 12, *2022):*

https://eur-lex.europa.eu/eli/reg/2022/1925

[331] *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.

[332] https://digital-markets-act-cases.ec.europa.eu/gatekeepers

Starting from March 7, 2024, companies designated as the gatekeepers, in relation to their designated core platform services, 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 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 their EU 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, previously only exercised in exceptional circumstances. Unlike traditional competition enforcement, the Commission will be able to impose these interventions without an assessment of evidence of harm, without taking into consideration any effects-based defenses, and without considering procompetitive justifications put forth by the targeted companies. It is also concerning that the EU is extending this DMA "gatekeeper" designation into new EU regulations including the Data Act.[333]

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.[334] The Digital Services Act was formally adopted on October 19, 2022, published in the Official Journal of the European Union on October 27, 2022, and entered into force on November 16, 2022.[335] The Digital Services Act entered into application for designated "very large online platforms" and "very large search engines" on August 28, 2023, and will enter into application for all services on February 17, 2024. These new rules will police how providers moderate for illegal content, counterfeiting, collaborative economy services, or product safety.

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[336], obligations to disclose the main parameters used in their recommendation systems, and requirements to appoint a compliance officer. Fines can reach up to 6% of annual turnover. Further, "very large online platforms and very large search engines"—defined as those with 45 million active users or more in the EU— only have 4 months to comply with the new

[333] 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.

[334] 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/.

[335]Official Journal of the European Union (Oct. 27, 2022): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:277:FULL&from=EN&pk_campaign=todays_OJ

[336] Feedback on the Digital Services Act's Draft Delegated Regulation, Rules on the Performance of Audits (June 2, 2023): https://ccianet.org/library/ccia-europe-draft-feedback-dsa-delegated-regulation-on-audits/

regulations, while most companies receive 15 months to prepare.[337] The European Commission designated on April 24, 2023, the very large online platforms and search engines. Out of the 19 services designated, 17 are U.S. firms, and only one firm is European.[338]

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.

Throughout the implementation, the European Commission continues to use the DSA to further regulate online services and potentially deviate from other legislations.[339] As the European Commission is building a database to collect the statement of reasons sent by online platforms to their users, further information than DSA requirements were asked to online services.[340]

Online marketplaces, including a large number of U.S. companies, are required to receive a number of information on traders before allowing them to reach consumers. As such, online marketplaces will have to adopt a very cautious approach and check the information provided, especially with the high fines set out in the DSA. In case of doubt, online marketplaces would be incentivized to take down traders, 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.[341] The GPSR was published in the Official Journal of the European Union on May 23, 2023.[342] This regulation updates the existing Product Safety Directive to respond to new challenges related to online purchases including via marketplaces.[343] Building on the DSA, the GPSR imposes further restrictions on online

---

[337] 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/.

[338] European Commission, Press release, Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines (April 24, 2023): https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413

[339] Mathilde Adjutor, The Digital Services Act's Moment of Truth: Implementation, Disruptive Competition Project (October 20, 2022), https://www.project-disco.org/european-union/102022-the-digital-services-acts-moment-of-truth-implementation/

[340] Letter on Transparency Database for Content Moderation Decisions (Aug. 29, 2023): https://ccianet.org/library/ccia-letter-on-transparency-database-for-content-moderation-decisions/

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

[342]Official Journal of the European Union (May 23, 2023): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R0988

[343] 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.

marketplaces by creating a stay down obligation forcing marketplaces to remove products identical to ones previously flagged by authorities.[344]

In addition, the European Commission proposed the revision of the liability of defective products.[345] As part of the revision, the European Commission proposed that online marketplaces be liable for defective products as a last resort if they fail to identify the relevant economic operator within a month. The revision also introduces changes which could be disproportionately damaging to the technological, such as the inclusion of software in the definition of product and the de facto reversing of the burden of proof for complex products.[346] While the revision is still under negotiations in the European Parliament, the Council of the European Union largely endorsed the Commission's proposal on June 14, 2023.[347]

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.[348] 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, age verification, 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 and academics regarding the implementation of what could result in an oppressive surveillance system.[349] The European Commission opened a public consultation through

---

[344] Press Release, Product Safety: Deal on New EU Rules Adds Complexity for Thousands of Online Marketplaces in Europe (Nov. 29, 2022): https://ccianet.org/news/2022/11/product-safety-deal-on-new-eu-rules-adds-complexity-for-thousands-of-online-marketplaces-in-europe/

[345] European Commission, Proposal for a directive on liability for defective products (Sept. 28, 2022): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0495

[346] Bauer Matthias, Sisto Elena, Increasing Systemic Legal Risks in the EU: The Economic Impacts of Changes to the EU's Product Liability Legislation, ECIPE (June 2023): https://ecipe.org/publications/economic-impacts-of-changes-to-eu-product-liability-legislation/

[347] Press Release, EU Product Liability: Council Position Is Missed Opportunity To Improve New Rules (June 14, 2023): https://ccianet.org/news/2023/06/eu-product-liability-council-position-is-missed-opportunity-to-improve-new-rules/

[348] 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.

[349] 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. *See* also Open letter by Academics and Researchers on CSA Regulation: https://docs.google.com/document/d/13Aeex72MtFBjKhExRTooVMWN9TC-pbH-5LEaAbMF91Y/edit; Joint industry call for protecting encryption and limiting detection orders in the CSA Regulation (September 6, 2023): https://ccianet.org/wp-content/uploads/2023/09/CSAM-Joint-call-for-safeguarding-encryption-and-limiting-detection-orders.pdf.

September 5, 2022, which CCIA responded to.[350] This proposal is still undergoing legislative scrutiny in the European Parliament and the Council of the EU.

The European Commission also proposed rules on "transparency and targeting of political advertising" in November 2021 as part of the measures to protect election integrity.[351] The proposal would require any political advertisement to be clearly labelled and introduces new rules on political targeting and amplification techniques, and could potentially introduce new legal concepts that go further than what is foreseen in current data protection legislation.[352] Failure to comply with these rules could result in fines of up to 4% of the total worldwide annual turnover of the preceding financial year.

Copyright Liability Regimes for Online Intermediaries

On May 17, 2019, the Copyright Directive was published in the Official Journal of the European Union.[353] The Member States had until June 7, 2021, to implement this new EU law. As of October 2023, six countries—Bulgaria, Denmark, Finland, Latvia, Poland, and Portugal—have yet to implement the new rules.[354] The European Commission has opened an infringement procedure against the other 23 member states for not transposing the bloc's copyright rules in time.[355]

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.[356] 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

---

[350] 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.

[351] Press Release, European Democracy: Commission sets out new laws on political advertising, electoral rights and party funding (25 November 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6118

[352] Claudia Canelles Quaroni, *How a De-Facto European Ban on Targeted Ads Could Pollute Your News Feed,* Disruptive Competition Project (May 2, 2023), https://www.project-disco.org/european-union/a-european-ban-on-targeted-ads-could-pollute-your-news-feed/

[353] 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.

[354] https://www.euractiv.com/section/copyright/news/eu-commission-sends-six-states-to-court-for-not-transposing-copyright-rules/.

[355] *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.

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

norms on intermediary liability. Absent obtaining a license from all relevant rightsholders, online services will be directly liable unless they: made best efforts to obtain a license; 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 "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."[357] However, despite this clarification, the ruling declined to exclude upload filters outright as a general obligation.

As Member States continue to 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.[358] 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.

---

[357] 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.

[358] *Id*.

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.[359] 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,"[360] 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 implemented this provision of the EU Copyright Directive as it created an analogous right for press publishers in October 2019. News publishers can now request money from platforms when platforms display their content online. Following this development, Google announced in September 2019 that it would change the way articles appear in search results instead of signing licensing agreements.[361] 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.[362] 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.[363] 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.[364]

Extraterritorial Regulations and Judgments

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

---

[359] *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/.

[360] 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.

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

[362] *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.

[363] *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.

[364] *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.

data subject objects to the processing, or the processing was unlawful.[365] Under the GDPR, the fine for noncompliance with these and other provisions can be up to 4% of a company's global operating costs. Putting the onus on companies to respond to all requests in compliance with the "right to be forgotten" ruling and Article 17 of the GDPR is administratively burdensome. For example, popular U.S. services have fielded hundreds of thousands of requests since the policy went into effect.[366] 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.[367] 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 citizens. The EU Member States and European Parliamentarians began the final negotiations and agreement is expected end of 2023. The regulation may apply as early as 2025 in all 27 EU Member States.

Lawmakers see the AI Act as an opportunity to set global norms: like GDPR, the AI Act 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. While the definition of AI is still being debated, EU lawmakers demonstrated their intention to align the AIA definition of the OECD definition to ensure international alignment. 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 numerous requirements such as conformity assessments, 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.

---

[365] GDPR art. 17.

[366] 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.

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

Various unclear definitions of AI, foundation models, general-purpose 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. Additionally, the vague wording of certain prohibited systems risks banning low risk applications, such as biometric categorisation used to protect children online and to fight the dissemination of child sexual abuse material (CSAM).[368]

Further, 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. Compliance requirements for "high risk AI" are administratively cumbersome and may not be technically possible for firms to adhere to with certainty, given obligations such as requiring "error-free datasets" and imposing responsibility in an opaque manner between AI developers ("providers") and deployers ("users").

Finally, recent amendments imposing stringent requirements on cutting-edge technologies and essential building blocks, such as foundation models and general-purpose AI, would depart from the AI Act's original risk-based approach and disproportionately impact developers of such systems. Ongoing discussions on the pursuit to impose a two-tiered AI regulatory framework whereby the most stringent obligations only on the largest foundation model and general-purpose AI developers could disproportionately impact and discriminate against U.S. companies.[369]

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.[370] 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').[371] One of the first EU cybersecurity schemes under development relates to cloud services and features overt discriminatory requirements against non-EU cloud providers.

---

[368] CCIA Position Paper with EU Trilogue Recommendations on the Artificial Intelligence Act (July 2023), https://ccianet.org/wp-content/uploads/2023/07/CCIA-Europe-Position-Paper-with-EU-trilogue-recommendations-on-the-AI-Act.pdf.

[369] https://www.bloomberg.com/news/articles/2023-10-06/biggest-ai-systems-poised-for-stricter-set-of-eu-rules; AI Act: CCIA Europe Warns Against Asymmetric Regulation Ahead of Next EU Trilogue (October 23, 2023), https://ccianet.org/news/2023/10/ai-act-ccia-europe-warns-against-asymmetric-regulation-ahead-of-next-eu-trilogue/.

[370] 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.

[371] 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

In September 2022, the European Commission introduced a Cyber Resilience Act proposal (CRA) 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. [372] 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 CRA throughout their supply chain. This would affect cloud storage, messaging and email, online marketplaces, search engines, and even social networks. Many experts have criticized the vulnerability disclosure requirements included in this measure, that requires notifying national authorities of known vulnerabilities within 24 hours of discovery—even before a patch has been developed. This deviates from global norms, and could inadvertently increase cybersecurity risks.[373]

Media Freedom

The European Commission introduced the European Media Freedom Act (EMFA) on September 16, 2022, with a dual goal of supporting media freedom and diversity and protecting journalists.[374] In particular, the EMFA introduces a special treatment of media content on very large online platforms.[375] Recent legislative developments suggest that this special treatment could become a fully-fledged content moderation exemption of media content, meaning that the EMFA would contradict the horizontal rules established in the Digital Services Act.[376] Industry is concern regarding a lack of clarity around how this set of rules interacts with these other digital 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.

---

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

[373] https://www.euractiv.com/section/cybersecurity/news/cyber-resilience-act-disclosure-requirement-concerns-raised-by-experts.

[374] 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.

[375] Mathilde Adjutor, *European Media Freedom Act Shouldn't Revive the Dreaded Media Exemption*, Disruptive Competition Project (May 25, 2023): https://www.project-disco.org/european-union/emfa-shouldnt-revive-the-dreaded-media-exemption/

[376] Press Release, Media Freedom Act: EU Parliament Risks Enabling Spread of Harmful Content With Media Exemption (Sept. 7, 2023): https://ccianet.org/news/2023/09/media-freedom-act-eu-parliament-risks-enabling-spread-of-harmful-content-with-media-exemption/

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.[377]

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.[378] This includes online platforms. Under the regulation, there is a 24-hour timeline for removing harmful content. Further, international companies are obligated to open a representative office within country, while naming a liable legal and content removal point of contact. There are no safe harbor protections for foreign companies, and the regulation stipulates an average of $200k in licensing fees (which could conflict with the existing Media law of 2018).

Additional E-Commerce Barriers

Industry reports 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.[379]

P. France

Transposition of European Law

On May 10, 2023, the French Government presented a Bill to secure and regulate the digital environment ("Projet de loi visant à sécuriser et réguler l'espace numérique"). The bill's purpose is notably to adapt French Law to the European Digital Services Act, Digital Markets Act, and Data Act.[380] The ongoing legislative scrutiny by the Senate and National Assembly could create some deviations from the recently adopted European legislation, by creating disproportionate additional barriers for U.S. firms.

---

[377] *Freedom on the Net 2023: Egypt*, https://freedomhouse.org/country/egypt/freedom-net/2023; *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. 4, 2023).

[378] *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.

[379] *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.

[380] Projet de loi visant à sécuriser et réguler l'espace numérique, Légifrance (May 10, 2023): https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047533100/

The bill also includes certain provisions which would impose important fines on a list of allegedly unfair practices by Cloud Services Providers (CSPs) or mandate a certain level of interoperability between these services. Moreover, a very concerning amendment pursued by the French Senate and the National Assembly would introduce discriminatory SecNumCloud certification for non-European CSPs hosting broadly defined sensitive data, including health data, handled by central and local public authorities.[381] Additional discriminatory requirements, such as the obligation for CSPs to inform users of potential risks of foreign governmental access to their data, have been introduced during the legislative process.

Taxation of Digital Products and Services

On July 24, 2019 French legislation implemented a 3% tax on revenue generated in France derived from digital intermediary services and digital advertising services.[382] 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.[383] 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.[384] Based on French officials' own admission, the majority of firms that will pay the tax will be American.[385]

---

[381] Projet de loi visant à sécuriser et réguler l'espace numérique, Article 10 bis A, French National Assembly (adopted on October 12, 2023 following prior agreement with the French Senate): https://www.assemblee-nationale.fr/dyn/16/amendements/1674/AN/1138.

[382] 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"].

[383] *See* Submission of CCIA In Re Section 301 Investigation of French Digital Services Tax, Docket No. USTR 2019-0009 (filed Aug. 19, 2019), https://ccianet.org/wp-content/uploads/2020/07/Comments-of-CCIA-USTR-2020-0022-Section-301-Digital-Services-Taxes-.pdf at 6-8.

[384] *See, e.g.*, Assemblée nationale, Projet de loi de finances pour 2019, https://www.gouvernement.fr/action/le-projet-de-loi-de-finances-2019 (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.]).

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

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.[386]

Additionally, since 2017, France has imposed a tax on video content, on streaming services, and video-sharing websites ("TVC") that supply content in France on a cross-border basis and are not established in the country. Industry reports that the taxes are primarily being collected from U.S. companies and the funds go towards subsidizing the production of original French content and programming through the French National Film Fund (CNC). The tax was originally called the "YouTube tax." Suppliers subjected to the TVC also pay corporate income tax and the French DST, leaving U.S. suppliers facing double and, in some cases, triple taxation.

The French government is now considering the possibility of introducing a new tax on streaming music services with a similar goal of using revenue from foreign companies to subsidize original French content, leaving industry concerned of a new discriminatory taxation revenue stream that could leave U.S. services paying four streams of taxation, with several serving as cross-subsidies for local industries. Industry asks USTR to continue to remain vigilant of digital taxation and to work with counterparts to reconsider discriminatory treatment of streaming and video-sharing platforms via taxation as it has done through DSTs imposed on the sector.

Restrictions on Cloud Services

ANSSI, the French cybersecurity authority, has adapted its cybersecurity certification and labeling initiative, SecNumCloud, to explicitly discriminate against non-French cloud providers in March 2022 as well as over 600 companies that operate "vital" and "essential" services.[387] 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 (Article 19.6).[388] The certification standard is no longer entirely voluntary or preferred—tenders have been published with SecNumCloud verification as a requirement.[389] The only companies that are verified under SecNumCloud are French.[390] 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

---

[386] 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.

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

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

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

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

defining "sensitive data," and subsequently declaring when SecNumCloud would be required.[391] Further, some legislators are trying to expand certification requirements in subsequent legislation to health data.[392]

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.[393]

France is bound by the EU's international trade commitments under the WTO GPA and GATS agreements, such as agreeing to not confer preferential treatment to local competitors as compared to companies from other GPA and GATS signatories. France's treatment of cloud providers contravenes the commitment to "not treat a locally-established supplier less favourably than another locally-established supplier on the basis of degree of foreign affiliation or ownership." Industry is concerned about the French legislature's consideration of an amendment that would extend SecNumCloud ownership requirements to private entities active in the healthcare and other sectors.

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.[394] The NetzDG law mandates removal of "manifestly unlawful" content within 24 hours, and provides for penalties of up to 50 million euros.[395] 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"[396] have led to companies removing lawful content, erring on the side of

---

[391] 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.

[392] https://www.assemblee-nationale.fr/dyn/16/amendements/1514/ESPNUM/765

[393] *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/.

[394] Beschlussempfehlung und Bericht [Resolution and Report], Deutscher Bundestag: Drucksache [BT] 18/13013, http://dip21.bundestag.de/dip21/btd/18/130/1813013.pdf (Ger.).

[395] Id. § 3(2).

[396] 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/.

caution in attempts to comply.[397] Since coming into force in January 2018, the law has led to high-profile cases of content removal and wrongful account suspensions. Companies have repeatedly raised concerns regarding the law's specificity and transparency requirements[398] and groups have expressed concerns about its threats to free expression.[399]

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.[400] Cases arising under this law will also have implications on extraterritoriality.[401]

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.[402]

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.[403] The intention of this reform was 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

---

[397] *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.

[398] 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.

[399] *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.").

[400] 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/.

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

[402] *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/.

[403] 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*

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 German Federal Cartel Office (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.

Since 2021 the German Competition Authority has already initiated proceedings and/or made a finding of "paramount significance" against Apple,[404] Amazon,[405] Google,[406] Meta,[407] and Microsoft.[408] Like the EU's Digital Markets Act, these rules 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 are exclusively U.S. companies.

---

[404] Available at https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Meldungen%20News%20Karussell/2023/05_04_2023_Apple_19a.html.

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

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

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

[408] Available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/28_03_2023_Microsoft.html?nn=3591286

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.[409] 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,[410] 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.[411] Hundreds of people have reportedly been arrested under the law,[412] as human rights experts have alerted world leaders to the harms of the law.[413] As noted elsewhere in these comments further, website blocks are barriers to maintaining a free and open internet which is critical to digital trade.

Cybersecurity of critical information infrastructure bill

In 2022, the Hong Kong government announced a plan to introduce a bill to strengthen the cybersecurity of critical information infrastructure in Hong Kong. Internet service providers may be included and considered "critical."[414] The government began preparatory work on the bill in May 2022,[415] and 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

---

[409] *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/.

[410] *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.

[411] *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/.

[412] *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.

[413] *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.

[414] *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/.

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

law. Any new data localization requirements will put U.S. 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.[416] 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. In July 2023, the government introduced a new branch to prosecute cybercrimes, to be established at the Department of Justice, which will closely cooperate with the Cyber Security and Technology Crime Bureau under the Hong Kong Police Force.

Privacy Law Anti-Doxxing Provisions

Hong Kong's Personal Data (Privacy) (Amendment) Ordinance of 2021 entered into force on October 8, 2021, which included concerning anti-doxxing provisions.[417] 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. Hungary

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Act No. 50 of 2013 on the Electronic Information Security of State and Local Government Bodies ("Act") imposes rules on how state and local government bodies and organizations providing essential services manage data.[418] State and local government institutions are only

---

[416] 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.

[417] 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.

[418] State and local government bodies that are included as part of these requirements include central government administration bodies; "Sándor-palota" (the office of the President of Hungary); the Office of the Parliament (National Assembly); the Office of the Constitutional Court of Hungary; the National Office for the Judiciary and courts; Prosecution offices; the Office of the Commissioner for Fundamental Rights of Hungary; the

able to process data that they manage in systems operated and stored in the territory of Hungary and in closed systems used for the purposes of defence and diplomacy. If the supervisory authority for the security of electronic information systems approves it, or an international treaty applies, this data could be allowed to be processed outside of Hungary, but it still must be processed within the territory of the EEA States. For companies not registered in Hungary that provide electronic information systems, a representative based in Hungary must be appointed ensure compliance with the rules. For organizations providing services deemed as critical—which can include the energy, transportation, agricultural, and health industries—electronic information systems can only be hosted in EU Member States.

T. India

India is a region of continued concern for U.S. internet exporters. India has an increasingly vibrant e-commerce market, illustrated by the high value of digital exports and imports.[419] 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.

The Central Government is developing a regulatory overhaul of the digital governance framework in India with the forthcoming "Digital India Act" ("DIA"). India's Ministry of Electronics and Information Technology held a public consultation on March 9th, 2023 regarding the proposed DIA and released the broad framework.[420] The DIA is set to overhaul the existing regulatory framework governing India's information technology ecosystem. The DIA is expected to introduce new rules with respect to competition, liability of digital services, cybersecurity, and consumer protection. The draft of the new legislation has not been released, but officials have said it is forthcoming.[421] The lack of transparency and proper consultation to date surrounding the DIA—and how it would impact existing obligations under the IT Act and associated amendments—continues to concern industry.

State Audit Office of Hungary; the Central Bank of Hungary; Metropolitan and county government offices; the Offices of the representative body of local governments; the Hungarian Defence Forces.

[419] 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.").

[420] *Proposed Digital India Act to overhaul outdated legislation*, Lexology (April 26, 2023) https://www.lexology.com/library/detail.aspx?g=05e0bc72-1d4e-4daf-81f3-1cb6f92f1547; *See* MeiTY presentation outlining proposed Digital India Act: https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf.

[421] *How the Digital India Act will shape the future of the country's cyber landscape*, The Hindu (Oct. 9, 2023) https://www.thehindu.com/sci-tech/technology/how-the-digital-india-act-will-shape-the-future-of-the-countrys-cyber-landscape/article67397155.ece

Taxation of Digital Products and Services

In March 2020, the Indian Parliament expanded the scope of India's existing "equalization levy" in its amended national 2020 Budget.[422] This included a new 2% 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.

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

As a number of industry groups observed (including CCIA), the Indian tax represents the broadest framing of a unilateral tax on e-commerce firms, and runs directly counter to the Indian Government's commitment to reaching a multilateral solution in ongoing negotiations at the OECD on the taxation challenges of digitalization to the global economy.[423]

The new equalization level follows previous protectionist tax measures in India against foreign digital services. In 2016, the government introduced a 6% level on foreign digital advertising businesses.

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.[424] The uncertainty of this status quo has resulted in U.S. digital firms continuing to pay the taxes.[425] 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."[426] The U.S. International Trade Commission included

---

[422] *Taxation of the digitalized economy: Developments summary*, KPMG (Oct. 10, 2023), https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/digitalized-economy-taxation-developments-summary.pdf.

[423] *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.

[424] *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.

[425] *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.

[426] 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.

India's DSTs in its 2021 Year in Trade Report,[427] 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.

Restrictions on Cross-Border Data Flows

CCIA has raised concerns with the government of India's practices around data localization in previous NTE comments.[428] 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.

After years of development and prior iterations, the Digital Personal Data Protection Bill was passed and entered into law on August 11, 2023, with extraterritorial reach.[429] The bill gives the Indian government broad discretion in interpreting terms in the law such as "potential impact on the sovereignty and integrity of India;" "risk to electoral democracy;" "security of the State;" and "public order." The law institutes affirmative consent for all data processing and includes excessively narrow definitions for activities that could be deemed as legitimate causes for data processing. The law also allows the Central Government to deny the export of data to a country if it so chooses and is able to create a list of jurisdictions where personal data cannot be exported to from India, with no avenue for recourse, such as standard contractual clauses. The law also allows for data localization for certain sectors.[430]

Government-Imposed Restrictions on Internet Content and Related Access Barriers

India is a priority region of concern for U.S. digital service exporters, given the vibrant digital economy and market opportunities with increased government control over online speech. There is great concern with the speed at which Indian policymakers and political leaders have increased censorship practices and increased restrictions on companies that fail to take down content political leaders deem "objectionable." This has been combined with a dramatic increase in the aggression by which enforcement agencies go after U.S. firms in the market and novel enforcement tactics.[431]

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

---

[427] 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

[428] *2020 CCIA NTE Comments.*

[429] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

[430] https://www.huntonprivacyblog.com/2023/08/22/india-passes-digital-personal-data-protection-act/.

[431] *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/.

Twitter between 2019-2021.[432] The Indian government conducted 84 internet shutdowns in 2022, according to Access Now, the most of any country globally.[433]

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.[434] In 2021, amendments to the IT Act went into effect imposing additional requirements under the Intermediary Rules and imposing new obligations on intermediaries.[435] 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. 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. 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.[436]

On October 28, 2022, the Central Government notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules in the Gazette of India.[437] The initial rules require social media intermediaries to make "reasonable efforts" to refrain from hosting any information that belongs to somebody else; harms children; infringes on any copyright or patents held; is deceiving or otherwise reflects misinformation; threatens India; contains malware; and constitutes a wide range of "obscene" content. Under the additions from this amendment, social media intermediaries will also be required to acknowledge user complaints within 24 hours and subsequently address their requests within 15 days—if the user's request seeks the removal of content, the complaint in question will need to be addressed within 72 hours. The rules establish Grievance Appellate Committees to hear challenges to platforms' content moderation and potentially reverse the decisions of platforms. These panels—the precise

---

[432] USITC, Foreign Censorship Part 2, *supra* note 48.

[433] Access Now, (2023) https://www.accessnow.org/wp-content/uploads/2023/05/2022-KIO-Report-final.pdf.

[434] 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.

[435] The full text is available at https://www.meity.gov.in/writereaddata/files/Revised-IT-Rules-2021-proposed-amended.pdf.

[436] *'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/.

[437] *See* proposed text of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 amendments here: https://www.meity.gov.in/writereaddata/files/IT%20Intermediary%20Rules%2C%202021%20updated%20on%2028.10.2022.pdf.

number to be decided upon is unknown—will be implemented within three months of the release of the rules.

India's Ministry of Electronics and IT amended its Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 on April 6, 2023, with additions regarding fact-checking and social media.[438] The proposal would prohibit social media firms and internet providers from "publishing, hosting or sharing false or misleading information about 'any business' of the government," with the validators of fact to be government agencies including the Press Bureau of India. Failure to comply with the rule could result in a loss of the safe harbor protections.

On July 7, 2023, the Telecom Regulatory Authority of India (TRAI) released a consultation paper dubbed "Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services."[439] As part of this consultation, TRAI seeks comment on bringing OTT providers into the licensing and registration framework required of telecommunications operators and on the merits of "selective banning" of OTT services. The consultation raises concerns regarding duplicative regulations for OTT services—including regulations still being developed through the Draft Telecommunications Bill, thereby complicating the process of operating in the market for the U.S. providers that are prominent in the market; applying telecommunications-style regulations for online services providers despite the fundamental differences between the functions and uses of the services; and destructive harms to freedom of expression and the open internet. In particular, the goal of empowering government entities and regulators to selectively block access to OTT services in India brings serious concerns with respect to internet freedom, privacy, and security. TRAI sought feedback from the public.[440]

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

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.[441]

---

[438] See text here: https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf; *India considers banning news identified as 'fake' by govt on social media*, Reuters (Jan. 18, 2023) https://www.reuters.com/world/india/india-considers-banning-news-identified-fake-by-govt-on-social-media-2023-01-18/.

[439] See the TRAI press release at: https://www.trai.gov.in/sites/default/files/PR_No.59of2023.pdf and the full text of the consultation paper at: https://www.trai.gov.in/sites/default/files/CP_07072023_0.pdf.

[440] CCIA filed comments and counter comments with TRAI https://ccianet.org/library/ccia-comments-on-trai-ott-regulation-consultation/.

[441] 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.

The legislation would redefine "telecommunication services" to include a wide range of internet-enabled services that bear little resemblance to the telephony and broadband services previously governed by this regulatory regime. Telecommunications services providers would then be subject to onerous obligations including licensing requirements; government access to data; encryption requirements, internet shutdowns, seizure of infrastructure, and possibly monetary obligations for the sector. This will undermine digital security and freedom of expression and impose a first of the kind global authorization/licensing requirement for any digital firm.

The provision of licenses could 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 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.[442] 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.

A TRAI consultation paper released in July 2023, "Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services,"[443] also put forward similar proposals to impose telecommunications licensing obligations onto internet-enabled services.[444] Among the questions posed by TRAI was whether a "collaborative framework" between OTT providers and telecommunications infrastructure providers would be necessary, evoking similar language to the "network usage fee" debate that has already gained momentum in India.

Further, industry reports that telecommunications licensees in India are obligated to connect to equipment that has been tested and received certification by the Mandatory Testing and Certification Framework (MTCTE). This mandatory testing and certification regime is in effect for certain IT and telecommunications products to determine safety, functionality, and security, but the scope of the obligation has been expanded recently to apply to cloud software suppliers, which imposes telecom product-specific rules on non-telecom-related products.

---

[442] *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.

[443] See the TRAI press release at: https://www.trai.gov.in/sites/default/files/PR_No.59of2023.pdf and the full text of the consultation paper at: https://www.trai.gov.in/sites/default/files/CP_07072023_0.pdf.

[444] Comments of CCIA To TRAI in OTT Regulation Consultation (2023), https://ccianet.org/library/ccia-comments-on-trai-ott-regulation-consultation/.

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.[445] 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.[446]

Regulations on Cloud Services

In 2020, the DPIIT extended its demand for minimum local content to the procurement of software and services.[447] As per the Notification, the local requirement to categorize a supplier as a "Class I" supplier is 50% and a "Class II" 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.

DPIIT's order imposed a significant compliance burden for U.S. and other foreign software and cloud service providers to by requiring that they demonstrate their contribution to the local market as a condition of participation. This framework fails to consider how foreign cloud services providers contribute to India's technology sector and boost local providers' competitiveness on the global stage by providing upskilling training, cloud innovation centers, quantum computing laboratories, and more. Even if cloud services providers are not bidding directly for government contracts, investment partners would be required to verify their percentage of local content. In cases where cloud services are a significant proportion of cost in a public procurement bid, the percentage of local value add from a cloud services provider becomes crucial. Industry is concerned that the Indian government is planning to revise the order further and raise the minimum local content requirement for Class I suppliers to 60% and Class II suppliers to 30%.

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

---

[445] 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.

[446] *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/

[447] *See* full text of the order: https://dpiit.gov.in/sites/default/files/PPP%20MII%20Order%20dated%2016%2009%202020.pdf.

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.[448] After pressure, the Indian government agreed in June 2022 to delay the rules for three months,[449] but VPN operators had already left the market due to the regulatory uncertainty and impending invasive oversight, undermining digital security and services exports to the country.[450]

Experimental Platform Regulation

On December 22, 2022, an Indian parliamentary panel recommended that India adopt a "Digital Competition Act," which would include European Digital Markets Act-like ex-ante regulations for "systemically important digital intermediaries." The proposed rules appear to be largely targeted at U.S. tech companies. Additionally, the panel gave recommendations on: "anti-steering practices; platform neutrality; bundling and tying; data usage; mergers and acquisitions; deep discounting; exclusive tie-ups; search and ranking; restricting third-party applications; and advertising policies."

In October 2022, the Competition Commission of India issued far-reaching orders seeking changes to how the Android operating system and the Google Play store function in India.[451] While ostensibly seeking to address competition issues, the order, which is under appeal, may lead to a fragmented, more expensive and less sustainable market for applications, and introduce significant cybersecurity risks into the mobile ecosystem.

U. Indonesia

Taxation of Digital Products and Services

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. Companies determined to have a significant economic presence will be declared permanent establishments and as a result subject

---

[448] 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/.

[449] 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.

[450] 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/.

[451] See text of the orders at: https://www.cci.gov.in/antitrust/orders/details/1070/0 and: https://www.cci.gov.in/antitrust/orders/details/1072/0.

to domestic tax regulations. 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.[452] While structurally different from digital services taxes adopted in some European countries, the tax is similarly concerning insofar as it looks to unilaterally 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.

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.[453] 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).[454] U.S. trade officials should continue to monitor developments.

Further, industry reports that Indonesia continues to act in violation of its WTO-binding tariff commitments by imposing tariffs on a set of imported technology products that should be granted duty free treatment thanks to the commitments made through the commitments made through Information Technology Agreement (ITA). Indonesia has only introduced ITA commitments that track with five categories of goods/HS codes (Semiconductors, Semiconductors Equipment, Computers, Telecommunications Equipment and Software, and Electronic Consumer Goods). Industry reports concern that Indonesian customs has also pursued reclassification of technology goods with similar functions into dutiable HS codes that would fall beyond the 5 categories as a method of increasing revenue, despite the fact that the reclassified HS codes would generally also be protected by Indonesia's ITA commitments. This practice broadly harms the IT industry and imposes burdens on U.S. investors and their workers alike.

Required Filing of Customs Declarations for 'Intangible Goods'

On January 14, 2023, Indonesia's Ministry of Finance issued Regulation No. 190/PMK.04/2022 to require entities importing intangible goods such as software and other digital products transmitted electronically to file a Customs declaration.[455] The Regulation requires a Customs declaration to be made within 30 days of an entity receiving payment for the importing of intangible goods through Customs' online declaration portal with numerous details about each

---

[452] https://taxnews.ey.com/news/2020-0604-indonesian-government-proposes-key-tax-changes.

[453] 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.

[454] 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.

[455] https://www.globalcompliancenews.com/2023/01/20/https-insightplus-bakermckenzie-com-bm-international-commercial-trade-indonesia-new-regulation-on-self-consumed-imported-goods-what-indonesian-importers-should-consider_01162023/.

transaction including country of origin, sender information, and import information. The regulation went into effect on January 14, 2023, but how it will be administered is unclear. For example, if every download of an app on a mobile phone will trigger a customs filing requirement. Should the WTO moratorium fail to renew, customs duties under PMK 190 on digital goods could be charged in addition to the non-resident VAT imposed on the utilization of digital taxable goods and services in August 2020 (Perppu 1/2020).[456] Industry continues to be concerned about the implications of this regulation even without new customs duties. CCIA appreciates USTR's efforts to solicit answers to the many vague aspects of Regulation 190 and urges continued vigilance as the Indonesia government implements the rules.[457]

Customs Duties on Electronic Transmissions

Indonesia issued Regulation No.17/PMK.010/2018 (Regulation 17) in 2018.[458] 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. If a tariff rate (currently zero) is specified, the policy would also conflict with Indonesia's commitment under the WTO's moratorium on customs duties on electronic transmissions, dating back to 1998[459] and most recently reaffirmed in June 2022.[460] 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, scheduled to be held in February 2024. 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.[461] 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.[462] More than half of existing cables

---

[456] https://www.pajak.go.id/sites/default/files/2020-04/Perpu%20Nomor%201%20Tahun%202020.pdf.

[457] https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/G/TFAQ/IDN1.pdf&Open=True.

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

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

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

[461] 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

[462] *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.

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.[463]

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 the ICT Ministry specifically asks for foreign operators to partner with a local network operator that has been operational for five years and completed 100% of construction commitments for the first five years; the local partner to be part of the consortium; a minimum of 5% stake by the local partner; and an 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.[464] 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 did not provide guidance until June 14, when the government sent around a "Circular Letter" that stated that the six month grace period started on January 21, 2022, and that therefore the ESPs

---

[463] 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.").

[464] *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/.

had to comply by July 20, 2022.[465] 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.[466]

Further, ESPs must comply with strict timelines for content removal, including 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.[467]

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 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.[468]

The phenomenon of content restrictions continues to be relatively high—between January and June 2022, Meta reported that the company restricted access to "1,458 items reported by the Ministry of Communication and Information Technology (KOMINFO) for allegedly violating local laws" in Indonesia.[469] 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.[470] The rules have yet to be introduced, but CCIA urges USTR to monitor

---

[465] 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/.

[466] *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/.

[467] 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.")

[468] USITC, Foreign Censorship Part 2, *supra* note 48.

[469] Meta, Transparency Center, Indonesia Country Report, https://transparency.fb.com/reports/content-restrictions/country/ID/ (last visited Sep. 27, 2023).

[470] *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/.

developments on this issue, given the speed with which the rules could be introduced and declared in effect.

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,[471] storing and processing of data offshore by any "Electronic Systems Providers (ESPs)" will require prior approval from the government.[472] These requirements present market access barriers for foreign services when delivering products and services online.

GR 71/2019 regulates the activities of Electronic System Operators (ESOs), generally defined as any person, government administrator, business entity, or member of society that provides, administers, and/or operates an electronic system individually or collectively for users. GR 71 amends Indonesia's previous regulations (GR 82/2012), and allows private sector ESOs to store systems and data outside Indonesia, subject to certain restrictions. However, GR71 requires data localization for public sector ESOs, which creates market access barriers for U.S. cloud service providers servicing the Indonesian public sector market.

Furthermore, the implementing regulations for GR71 continue to present significant barriers to digital trade and inhibit the ability of U.S. firms to participate in the e-commerce market in Indonesia.[473] The Ministry of Communications Circular 4/2022 requires public sector organizations to obtain clearance from the ICT Ministry and the Ministry of State Apparatus Utilization and Bureaucratic Reform for any IT procurement to ensure maximum utilization of the state-built National Government Data Center to store data. This requirement presents a challenge for cloud adoption by public agencies and poses additional barriers and operational costs to U.S. cloud services providers.

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.[474] 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.

---

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

[472] *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.

[473] https://www.globalcompliancenews.com/2021/01/17/indonesia-indonesia-regulates-foreifn-private-electronic-system-operators11122020/.

[474] *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.[475] Data controllers must ensure that any data flows must only go to countries which have equivalent or higher 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. The law also applies extraterritorially if the data transfer has any legal consequences in Indonesia or to its citizens. This applicability covers more processing activities than typically seen in other data frameworks, and could make it challenging to determine the personal data that falls within scope and could conflict with requirements for data protection in other jurisdictions.

In April 2023, Indonesia's Constitutional Court clarified ambiguities in the Personal Data Provision Law (PDP) after it was enacted in October 2022.[476] Petitioners expressed the belief that "Controller" did not include legal entities, and therefore legal entities are not eligible to conduct personal data processing. The court found that "person" includes legal entities, and they therefore can be data controllers. Applicants also questioned the personal or household data processing exemption, requesting clarification about whether "small or household scale businesses" which also process personal data, are exempted and therefore left unregulated. The court clarified that PDP applies to non-commercial personal or household activities and that the only processing activities excluded are personal, intimate, non-commercial and/or non-professional. Another applicant argued that the PDP did not adequately define "national defense and security" which is a justification used in the PDP to limit a data subject's rights.[477] The court clarified that the phrase is defined through the principle of public interest as defined by prevailing laws and regulations, subject to, for example, relevant regulations like the State Defense Law. The drafts of the implementing regulations of the PDP are in the formulation process.

On August 31, 2033, the Ministry of Communications and Information Technology sought comment on its draft regulation for the implementation of the PDPL that included proposals for cross-border data transfers. The PDPL requires that for data to be transferred to foreign jurisdictions, the data must receive the same protections as they would in Indonesia—the new draft regulations seek to provide entities seeking to transfer data to jurisdictions that do not meet an adequate level of protection to leverage cross-border agreements, standard contract clauses, and enforceable group company rules to do so.[478]

---

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

[476] *Indonesia: Clarification of certain provisions of the PDP Law by the Constitutional Court*, Baker McKenzie (June 13, 2023) https://www.lexology.com/library/detail.aspx?g=b1598b5d-3731-49fa-82d7-9ecb47b42a4a.

[477] *Constitutional Court Rulings Illuminate Certain Provisions of the PDP Law*, Rajah & Tann (May 8, 2023) https://www.lexology.com/library/detail.aspx?g=187d88a5-0f37-4e82-a8a0-eb3e0c2fd7b1.

[478] https://www.lexology.com/library/detail.aspx?g=95ae64c5-b9a7-493a-bbb6-e48c5d23bf69.

Criminal Code

After a decade-long revision process, the Parliament passed a new Criminal Code on December 6, 2022, which increases liability for digital platforms, including provisions relating to religious blasphemy, insulting the President and the Vice President, and expressing views counter to the national ideology (Pancasila). Corporations are now subject to criminal law under the code. The draft includes provisions subjecting corporations to criminal law, meaning business decisions, administrative issues, and negligent behavior could be penalized criminally (Article 45- Article 50). There is much ambiguity and uncertainty about the interpretation of the clauses and how they will be enforced (i.e., if all Indonesian laws applicable to individuals will then be applied to corporations). Detailed provisions will be stipulated in the implementing regulations. The new provisions could potentially impact how platforms moderate content for topics such as misinformation and slander (such as insults to the President and Vice President).

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.[479]

Financial service regulators have the authority to further regulate financial sector data in compliance with the aforementioned GR 71. The amended regulations issued by the Indonesian financial regulator, the Otoritas Jasa Keuangan ("OJK"), allow some financial data to be transferred and stored outside of Indonesia with approvals from the respective regulator.

While the Bank of Indonesia has adopted a risk-based approach in its payment regulations, it still considers cloud services as a high-risk activity, which requires financial institutions to seek its approval before moving workloads to the public cloud (Regulation No. 22/23/PBI/2020). Meanwhile, with Regulation No. 11/POJK.03/2022, the OJK only requires banks to submit approvals if the data center is located offshore. There is no need to submit approvals for cloud use in-country, thus explicitly discriminating against cross-border data processing.

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

[479] 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/.

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.

Forced Revenue Transfers for Digital News

In February 2023, Indonesia's government announced that it was in the process of drafting a Presidential Decree to direct specific digital platforms to pay news organizations for news content that appears on those platforms. Digital platforms that would qualify are those that host content from Indonesian news outlets and make up at least 1% of all internet traffic within Indonesia, and/or platforms with over 1 million daily active users in Indonesia in a 3-month period. However, local reporting has made it clear that U.S. companies are targets of this regulation. The government process in drafting the legislation has been opaque, as multiple versions of the draft bill have been leaked.

The consolidated draft of the bill changes frequently, but the overall goal—a mechanism for forcing revenue transfers between news organizations and internet platforms—has been consistent. Industry is concerned that if the draft decree moves quickly, it will be without sufficient due process or consultation with impacted stakeholders.

The draft proposal seeks to empower the Press Council, an independent body made up of members of the press and media companies, to implement the regulations, prescribe further regulations, and oversee arbitration between digital platforms—greatly compromising any presumption of neutrality and objectivity between disputing parties. Under this regulation, Indonesia's Press Council would establish the rules of engagement and simultaneously oversee mediation or arbitration if any disputes materialize—an authority they do not have under the country's Press Law. The draft regulation would also direct digital platforms to share and disclose algorithm changes to news publishers and disclose commercially sensitive user activity to news publishers.

In July 2023, the Press Council reiterated its calls to the Indonesian government to pass the regulation.[480] Reports circulated in late July that the Communications and Information Ministry shared a draft of the regulations.[481] However, that draft has not been made public and has yet to advance to receive the president's signature, although industry reports that the fundamental problems of the legislation were not addressed.[482]

---

[480] https://dewanpers.or.id/berita/detail/2454/Dewan-Pers-Minta-Pemerintah-Percepat-Prioritas-Pemberlakuan-Publisher-Rights.

[481] https://www.centennialasia.com/the-asian-pulse/daily-news/indonesia-to-require-google-and-meta-to-prioritize-verified-news-outlets/.

[482] https://indonesia.googleblog.com/2023/07/rancangan-peraturan-untuk-masa-depan-media-di-Indonesia.html ("The regulation may favor a limited set of news publishers and impose restrictions on our ability to surface diverse

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%, provided that each of these services is not ancillary to the main business line. Legislation took effect in November 2020 that aims to add clarity for e-commerce firms.[483]

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.[484] 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.

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% 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 Indonesian government could also implement a threshold for ICT equipment and add similar requirements for software and applications. Adding a requirement for these digital products would harm firms that offer services over the internet, including cloud services. Indonesia's issuance of Presidential

---

information from the remaining thousands of publishers across Indonesia, including hundreds of small publishers grouped under the Serikat Media Siber Indonesia (SMSI). This would impact Indonesians seeking to find a plurality of opinions online, and could ultimately mean they will find less impartial, and less relevant information… While this regulation was initially proposed with the stated goal of supporting a healthy news industry, the current draft would be detrimental to a vast number of publishers and creators who are transforming and innovating. New powers granted to a single, non-government body, formed by and including representatives of Dewan Pers, will only benefit a select number of traditional publishers by limiting which content can be shown on our platforms."); https://www.kompas.id/baca/english/2023/08/11/en-meta-menolak-raperpres-jurnalisme-berkualitas.

[483] 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.").

[484] *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.

Instruction Number 2 Year 2022 adds to these obligations by mandating that government agencies plan, allocate, and achieve a target of at least 40% of the national budget for goods and services to leverage MSMEs and cooperative products from domestic production.[485]

In December 2022, Indonesia's Ministry of Trade re-issued a new version of the 2020 proposal, Regulation No. 50, that would impose a de facto local presence requirement for e-commerce suppliers (Article 25.2, requiring establishment of an exclusive, dedicated representative). The rules, if adopted, would also direct the prioritizing of local goods and services (Article 21), and empower the government to demand data about the company and associated business actors.

In September 2023, Indonesia announced it would prohibit e-commerce transactions from taking place on social media services by amending Regulation of Minister of Trade Number 50 of 2020 on Provisions for Business Licensing, Advertising, Development and Supervision of Business Sector in Trading Through Electronic System.[486] The Trade Minister, Zulkifli Hasan, argued that the action seeks to "prevent the domination of the algorithm and prevent the use of personal data in business interests" and "create a fair, healthy and beneficial electronic commerce ecosystem."[487] Given the proliferation of innovative methods of reaching consumers through social media applications and websites, forcibly restricting online platforms from hosting sales through their services represents a hindrance to their business practices in a key market.

Restrictions on Imports

On September 27, 2023, the Ministry of Trade ("MOT") issued Regulation No. 31/2023 that excludes foreign merchants from selling any goods that are valued less than $100 to Indonesian customers through online marketplaces.[488] The regulation introduces other discriminatory requirements that will hinder imports and foreign investment in Indonesia, such as mandating that foreign e-commerce platforms obtain a permit from the Ministry of Trade in order to participate in the Indonesian market and requires platforms that meet certain criteria to appoint a locally-based representative. Companies with a marketplace business model are barred from serving as a manufacturer and selling their products with their own branding. Regulation No. 31/2023 will hinder U.S. exports to the market and the ability of U.S. providers to participate in the market.

The Ministry of Trade has previously issued Regulation No. 87/2015, which imposes obligations on the imports of goods classified in specific HS codes, including servers. The entity importing the goods must appoint a company verified by the Indonesian Government to inspect its shipment in the origin before receiving Customs approval. The regulation was repealed and replaced by Regulation No. 20/2021 ("Reg 2021"), which went into effect on November 19,

---

[485] *See* Press Release, Cabinet Secretary of the Republic of Indonesia, President Issues Instruction on Domestic Product Use Intensification for Gov't Goods/Services Procurement (Apr. 9, 2022), https://setkab.go.id/en/president-jokowi-issues-instruction-on-domestic-product-use-intensification-for-govt-goods-service-procurement/.

[486] https://setkab.go.id/en/govt-to-amend-regulation-on-social-media-use-for-e-commerce/.

[487] https://apnews.com/article/indonesia-tiktok-ecommerce-ban-china-62e5ef9f366d8cfd4a94427393bb5aba.

[488] *Indonesia: The New E-Commerce Regulation*, BAKER MCKENZIE (Oct. 10, 2023), https://insightplus.bakermckenzie.com/bm/consumer-goods-retail_1/indonesia-the-new-e-commerce-regulation-heightened-levels-of-responsibility-for-e-commerce-platforms-operators.

2021, and implemented new HS codes.[489] Servers, cooling equipment, hard disk drives, network interface cards and battery back-up units are all included under the scope of the regulation, and the additional burdens can impose costs rising to $1,600 per shipment, which significantly adds to the supply chain costs for foreign companies. Although the regulations allow capital goods to be imported into Indonesia without these required burdens when they can gain an exemption letter from the MOT, the government has not provided sufficient transparency and certainty for applying and receiving the exemption.

V. Italy

Taxation of Digital Products and Services

Italy's 2020 Budget introduced a 3% digital services tax closely aligned with the EU's original proposal.[490] 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: the "provision of advertising on a digital interface targeted to users of the same interface;" 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 the "transmission of data collected from users and generated by the use of a digital interface."[491]

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.[492] 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 United States.[493] However, U.S. officials should work to ensure that this discriminatory tax is removed even if implementation of the OECD solution is delayed beyond 2024.

---

[489] *Indonesia: New Integrated Import Guidelines*, BAKER MCKENZIE (2022), https://www.bakermckenzie.com/-/media/files/insight/publications/2022/01/thought-piece_new-integrated-import-guideline.pdf.

[490] 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.

[491] *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).

[492] *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.

[493] 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.

Experimental Platform Regulation

On August 27, 2022, Law No. 118, the "2021 Annual Competition Law," went into effect.[494] The law presumes economic dependence—which entities can challenge—for firms that offer intermediation services on digital platforms that facilitate end users or suppliers.[495] 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 as through the enforcement of unilateral conditions or added fees.[496] 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.[497]

Implementation of the EU Audiovisual Services Directive

Italy implemented the EU Audiovisual Media Services Directive ("AVMS-D") in 2022. 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 to the Government the adoption of 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 to up to 25% 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.[498] The quotas remained, with a slight reduction in the quota to 20% following 2024, which still reflects an excessively high bar.[499]

W. Japan

Restrictions on Cross-Border Data Flows

The Japanese Ministry of Communications (MIC) expanded the application of the Telecommunications Business Act (TBA) to foreign suppliers of internet-enabled services in

---

[494] 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/.

[495] *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/.

[496] *Id*.

[497] *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.

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

[499] *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").

2021, capturing suppliers even if they lacked a juridical presence in Japan.[500] This change mandates that foreign over-the-top (OTT) services, which encapsulate search, digital advertising, and other services that facilitate communications using third-party facilities to provide notification and register as a local service provider with a local representative, and observe obligations under its Telecommunications Business Act. MIC amended the TBA in 2022 to apply its privacy and data protection obligations to large platform providers and to apply third-party data transfer information—such as the usage of third-party cookies—to all products. Amendments to the TBA implementing requirements for telecommunications providers to disclose a wide array of information to users when transmitting data went into effect on June 23, 2023.[501]

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 came into effect from April 2022.[502] 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.[503] The APPI requires a review of the policy once every three years so discussion of revisions are expected to commence in 2023.

Experimental Platform Regulation

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).[504] In these interim reports, the DMCH proposed several new avenues for *ex ante* digital platform regulation in mobile apps and voice assistants and wearables. Any resulting heavy-handed ex-ante regulation that fails to account for broader market dynamics and incorporates a robust market analysis could disproportionately harm U.S. digital firms. 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 analytics (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;

---

[500] *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/

[501] https://elaws.e-gov.go.jp/document?lawid=359AC0000000086; https://www.dataguidance.com/news/japan-amendments-telecommunications-business-act-enter.

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

[503] *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/.

[504] 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.

and overly relying on similar actions taken in other jurisdictions that have yet to be genuinely tried and tested.[505]

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.[506] Platforms that use advertisers' ads on their websites—such as search engines, portal sites, and social networking services, primarily through 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 serve as intermediaries between advertisers and website operators primarily through auctions would be designated if they sell at least 50 billion yen (roughly $345.7 million) each fiscal year in Japan. An intent to target U.S. firms is evident in 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—which identified only Google, Facebook, and Yahoo! in its analysis of the market.[507] As the rules are implemented, it will be crucial to monitor the extent to which METI oversight unduly targets U.S. companies. Industry reports concerns that METI will require providers of platforms to undergo unnecessary administrative procedures such as provision of information not pertinent to the law; accordingly, it 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."

The DMCH released its final report observing the mobile ecosystem on June 16, 2023.[508] Despite some minor improvements, such as broadening the scope of its analysis to include more than just two U.S. providers, several concerning proposals remain.[509] Self-preferencing practices are expected to be prohibited by the DMCH following the report's proposal to impose requirements on vertically integrated participants to give third parties "equal access" to features or services. By regulating self-preferencing only for certain market actors while allowing other similar providers to do so, the proposed rules may result in undue discrimination against U.S. firms. Other major concerns that warrant USTR attention during implementation are the DMCH's proposals regarding mandated user data sharing, anti-steering obligations, and procedures, all of which could unreasonably disadvantage the targeted U.S. firms.

---

[505] 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.

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

[507] 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.

[508] https://www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_230616.pdf.

[509] https://ccianet.org/wp-content/uploads/2023/08/2023-08-18-CCIA-Comments-on-Japan-DMCH-Final-Report_English.pdf.

X. Kenya

Restrictions on Cross-Border Data Flows

Kenya released a new ICT Policy in August 2020, which requires that Kenyan data remains in Kenya, and that it is stored safely and in a manner that protects the privacy of citizens.[510] This provision conflicts with the 2019 Data Protection Act, which enables cross-border data transfers subject to conditions set out by the Data Commissioner. The Ministry of ICT proposed an amendment to the ICT policy guidelines in July 2023 that would remove the 30% local ownership requirement and invited public comment, but the change has yet to be finalized.[511]

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Data Protection Act does not require the localization of personal data, and under Section 50, the Cabinet Secretary is empowered to decide the types of personal data that must be stored and processed in Kenya due to protection of strategic interests of the state or revenue. However, industry reports that the Data Protection Regulations of 2020 required the localization of a wide array of data such as national civil registration systems, population register and identity management, primary and secondary education, electronic payment systems, revenue administration, health data, and critical infrastructure. At a minimum, a company must store a copy of data that is categorized under these definitions in a data center located in Kenya.

Taxation of Digital Products and Services

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

Y. Korea

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

The Ministry of Science & ICT has promulgated regulations made pursuant to amendments to the Telecommunications Business Act passed in 2020, imposing obligations on OTT suppliers, including foreign suppliers, for network management issues outside their control.[512]

---

[510] *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/.

[511] https://weetracker.com/2023/07/12/kenya-ict-ownership-rule/.

[512] 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.

The rules subject predominantly U.S. internet services to disproportionate levels of risk and responsibility regarding network management over which they have no control. The 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 remain the most relevant to 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 Usage Fee Legislation

Seven proposals have been made by the Korean National Assembly to mandate "network use fee" payments by certain content providers between 2021 and 2022. While in the past these proposals have been justified as necessary to help fund the costs of extending and adding capacity to local broadband markets, they are likely to distort investment incentives and lead to discriminatory treatment of content and application providers.[513] Such proposals follow years of demands by local telecommunication providers that U.S. content and application providers contribute financially to telecommunications network operators through network usage fees.[514] In 2022, these proposals were consolidated into what was called the "Netflix Free Ride Prevention Act."[515] The legislation would effectively mandate that foreign content access providers—namely U.S. firms such as Google, Meta, and Netflix—enter into paid contracts with internet service providers for the content demanded by ISPs' customers. Such a requirement 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 United States, by targeting U.S. content providers and requiring contracts and extractionary fees for any company meeting arbitrary data transfer thresholds.[516]

The legislation has now stalled as public opposition has materialized, including from a non-profit organization operating in Korea called OpenNet that collected 268,000 signatures in opposition to the proposal from September 7, 2022, to October 31, 2022.[517] The legislation has remained stalled in committee, warranting cautious optimism, but given the history of the issue, industry remains concerned that network usage fees could re-emerge and gain momentum.

---

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

[514] *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/.

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

[516] *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/.

[517] https://koreajoongangdaily.joins.com/2022/11/01/business/tech/Korea-network-usage-fee-Google/20221101172720310.html.

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 (Principles on Access and Use of the Internet).[518]

CCIA has appreciated the engagement of USTR and the Department of Commerce on this issue in the past and encourages continued vigilance. 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.

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. It has accomplished this through the Korea Internet & Security Agency (KISA) Cloud Security Assurance Program (CSAP), a set of requirements designed to ensure that public institutions relying on commercially-supplied cloud computing services benefit from secure and reliable cloud offerings. Industry reports that the three main technical requirements have prevented all global CSPs from being able to obtain the CSAP: physical separation of government data, requiring dedicated data centers; non-recognition of Common Criteria (CC) certification of equipment; and use of domestic encryption algorithms. In addition, requirements to store and process data domestically and rely exclusively on Korean nationals for the management of services severely affects foreign suppliers' ability to compete in the market.

On January 31, 2023, Korea's Ministry of Science and ICT (MSIT) promulgated a revised version of the CSAP. Despite introducing some minor flexibility with respect to data deemed low-tier (i.e., with respect to physical separation), U.S. services remain stymied at every level of CSAP certification—Low, Moderate, and High—with the result that public sector contracts go exclusively to Korean national firms.

While burdensome requirements at the low tier remain (e.g., with respect to encryption), these changes may open up a small portion of the public sector market to global CSPs, by allowing logical versus physical separation of data for this category. This key burden remains for medium and high-tier systems, which require the use of physical infrastructure separate from public cloud offerings. While recent advancements in AI technology are expected to benefit the Moderate tier of the public sector the most, their ability to utilize the most advanced global AI services may be significantly hindered by physical separation requirements. Given Korea's interest in developing its AI capability, allowing for logical separation in the Moderate tier, and alignment with international standards, should be a priority.

[518] 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.

The CSAP obligations have resulted in U.S. firms being effectively unable to qualify to bid on certain cloud computing procurement contracts, despite WTO and KORUS FTA commitments that should provide U.S. firms with that right, and which prohibit the use of technical requirements as a means of denying market access.

Also key to a more open market is a more open and transparent policy dialogue involving the National Intelligence Service (NIS), which has played a major role in cloud computing regulation, and creation of its independent National Cloud Computing Security Guide. The NIS Guidelines set stricter cybersecurity requirements than the CSAP guidelines, as well as other cybersecurity validation programs that impact CSAP, including by requiring that cloud facilities, equipment and personnel be under the exclusive legal jurisdiction of Korea. Therefore, reform of these Guidelines to allow for U.S supplier participation in the Moderate tier, and NIS's increased involvement in policy discussions is crucial for ensuring more secure and reliable public services through the cloud.

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. Similar restrictions have been considered for the education sector.

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 common model for app distribution, widely used in the U.S. but which differs from local equivalents. Further, policymakers supportive of the bill have made clear their intent to single out specific U.S. companies with the new law.[519] This 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.[520] 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

[519] 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.

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

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 usage process inconvenient, that act may constitute an act of forcing a specific payment method (own company payment)."[521]

U.S. operators of application marketplaces are disincentivized to operate in a region where it is unclear how the app 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.

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

Location-based data restrictions

Korea's restrictions on the export of map data continue to disadvantage foreign providers that use such data for services offered in Korea. Foreign-based services providers that offer apps and services that rely on map-based functions—such as traffic updates and navigation directions—are unable to fairly compete against their Korean rivals that generally do not rely on foreign data processing centers and therefore do not need to export map data. Korea is the only significant market in the world that restricts the export of map data in this manner.

Exporting map data requires approval from the Korean government. To date, Korea has never approved the exporting of map data, despite numerous applications by international suppliers. U.S. stakeholders have reported that Korean officials have stated that export approval is dependent on agreement to blur certain satellite imagery of the country--imagery that can be used in conjunction with map data, that Korea seeks to blur ostensibly for security reasons. While competing Korean providers do voluntarily blur select locations at the request of the Korean government, such imagery (provided by third-parties) is readily viewable on foreign mapping services available outside of the country. Thus, it is unclear how restricting the availability and denying the export of such data for foreign suppliers would address the general security concern, since high-resolution imagery of Korea is widely available as a stand-alone commercial product from over a dozen different suppliers. Accordingly, the most logical explanation is that Korea is simply seeking to protect its domestic suppliers from foreign competition.

Personal Information Protection Act

Korea's Personal Information Protection Act of 2011 has always imposed stringent requirements on the transfer of personal data outside Korea, requiring online service providers to provide customers with extensive information about the data transfer, such as the destination of the data, the third party's planned use for the data, and the duration of retention. However, less stringent

[521] 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.

requirements apply to data transfers to third parties within Korea, which "effectively privilege Korean over foreign suppliers in any data-intensive sector without materially contributing to privacy protection," as USTR has highlighted.[522]

Two years after PIPA's introduction, on May 18, 2023, the Personal Information Protection Commission released amendments for public consultation which aim to reinforce the rights of data subjects by introducing the right to data portability and took effect on September 15, 2023.[523] The amendments provide Korea's Personal Information Protection Commission ("PIPC") the authority to impose fines based on global, rather than local revenue. Since most Korean firms subject to this law have negligible foreign sales, such penalties disproportionately affect foreign (and mainly U.S.) suppliers, subjecting them to significantly higher financial risk than their local competitors. This amended law also grants the PIPC the authority to order the suspension of cross-border transfer of personal data based on a generalized risk of breaching privacy protections, absent evidence of specific violations. Such arbitrary authority could affect legitimate personal data transfer by U.S. companies to their U.S. headquarters, jeopardizing significant cross-border trade between Korea and the United States.

Targeted Enforcement on U.S. Companies

In September 2022, the Korean Personal Information Protection Commission ("PIPC") levied more than $70M in fines against two U.S. companies for alleged violations of the Personal Information Protection Act (PIPA). These are the biggest fines ever imposed by the PIPC, and were based on a new interpretation of the law with no court or regulatory precedents: the PIPC had concluded that the ad tech service provider, rather than the third-party publishers (website or app operators), must obtain consent for the user's personal data for personalized ads on the publishers' sites and apps. It appears that PIPC narrowly and arbitrarily scoped their investigation to only impact 2 U.S. companies, even though several domestic ad service providers also use behavioral data for personalized ads.

Taking this narrow approach to enforcement held U.S. companies to an unprecedented level of responsibility, and effectively absolved domestic ad service providers and third-party publishers of their responsibility to obtain consent for using behavioral information for personalized ads. Given there was no clear standard established by regulatory authorities or court precedents in Korea, and no establishment of harm to the user, the PIPC could have first clearly set forth the standards to be complied with by business operators in the form of guidelines and recommend them to comply with such standards.

Artificial Intelligence Legislation

On February 14, 2023, the National Assembly Science, ICT, Broadcasting and Communications Committee advanced the "Law on Nurturing the AI Industry and Establishing a Trust Basis," following 12 different bills related to artificial intelligence that have been introduced in the

---

[522] https://ustr.gov/sites/default/files/2022%20National%20Trade%20Estimate%20Report%20on%20Foreign%20Trade%20Barriers.pdf.

[523] https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do.; https://iapp.org/news/a/south-korea-cabinet-approves-enforcement-amendments-to-pipa/.

previous three years.[524] While the bill does not discriminate based on nationality or size, it includes increased and unclear obligations on systems of AI determined to be "high-risk," including methods for detailing how an AI system reaches its final decision. The broad classification of what constitutes high-risk is comparable to that of the EU AI Act and could envelop more services than appropriate.

Data Center Legislation

In late 2022, in response to a fire a major data center, the National Assembly passed the amendments to the Broadcasting Communications Development Act ("BCDA"), the Telecommunications Business Act ("TBA"), and the Act on the Promotion of Information and Communications Network Utilization and Information Protection ("Network Act") to encourage resiliency of data centers. The legislation entered into force in July 2023. Among the requirements of this law are extensive demands for data related to data center security that could jeopardize companies' cybersecurity and nondisclosure agreements, and making sensitive data related to infrastructure, security, and commercially sensitive trade secrets vulnerable to exposure.

Z. Malaysia

Cabotage Policy on Submarine Cable Repairs

In November 2020, the new Minister of Transport abruptly revoked an exemption from 2019 to the Merchant Shipping Ordinance 1952 that permits non-Malaysian ships to conduct submarine cable repairs in Malaysian waters.[525] The exemption was key in reducing the time required to conduct submarine cable repairs. This action appears to be based on pressure from a single competing Malaysian shipping company that sought beneficial treatment. The cabotage policy adds complexity, time, and cost for submarine cable owners that need to conduct repairs for cables that land in Malaysia. Due to the high costs of vessels for submarine cable repairs and the scarce availability of ships, submarine cable owners require regional and global economies of scale to recoup the large annual investments that are directly undermined by restrictive cabotage policies such as Malaysia's that obstruct 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.[526]

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

---

[524] https://www.lexology.com/library/detail.aspx?g=fa073ec6-81a1-44fd-87ce-c8d3f5f7a706; https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_Y2B1M0R6G2I2P1B0V2X9H4Z0X3M3J2.

[525] *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/.

[526] *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).

hindrance" to submarine cable projects.[527] Although reports throughout 2023 have suggested the Malaysian government could bring the cabotage exemption back for submarine cable repairs,[528] the exemption has yet to be enacted, and the very uncertainty that comes with billions of dollars of investment in crucial telecommunications infrastructure being dependent on an exemption that can so easily be rescinded upon another government change.

Restrictions on Cloud Services

The Malaysian Communications and Multimedia Commission (MCMC) crafted rules that subject data centers and cloud service providers to licensing obligations under the Communications and Multimedia Act 1998 (CMA 1998).[529] 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 make mandatory payments to the Universal Service Fund. These new rules went into effect on January 1, 2022.[530]

Forced Revenue Transfers for Digital News

The Malaysian Communications and Multimedia Commission ("MCMC") announced on Sep. 5, 2023 its intent to move forward with a news remuneration proposal.[531] At time of filing, no text has been released. The MCMC announcement suggested an interest in extraction and redistribution of revenues similar to that of Canada and Australia. The MCMC invoked the online news and news media bargaining laws passed in these countries and focused on "the imbalance in income for traditional Advertising Expenditure (ADEX) between digital platforms and local media to ensure fair compensation for news content creators."[532] This legislation warrants careful monitoring, both due to Malaysia's market size and the broad goals of the

---

[527] *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.

[528] *See* https://www.thestar.com.my/business/business-news/2023/05/05/anthony-loke-mot-to-provide-clarity-to-tech-giants-on-cabotage-policy.

[529] MALAYSIAN COMM. & MULTIMEDIA COMM'N, Frequently Asked Questions (FAQ) on Licensing Cloud Service Providers (Dec. 17, 2021), https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/FAQ-Regulating-Cloud-Service.pdf.

[530] *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.

[531] https://www.mcmc.gov.my/skmmgovmy/media/General/PressRelease/MS_MCMC-CONSIDERS-REGULATORY-FRAMEWORK-TO-ADDRESS-ONLINE-HARM-AND-IMBALANCE-MEDIA-ADEX.pdf.

[532] https://www.mcmc.gov.my/skmmgovmy/media/General/PressRelease/MS_MCMC-CONSIDERS-REGULATORY-FRAMEWORK-TO-ADDRESS-ONLINE-HARM-AND-IMBALANCE-MEDIA-ADEX.pdf.

legislation. These goals include sweeping issues with deep impacts on internet policy, such as addressing the impact of artificial intelligence and "fair competition, strengthen intellectual property rights, protecting consumers from online harms and privacy," as the government release states.[533]

AA. Mexico

Taxation of Digital Products and 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 (e.g., web blocking) 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,[534] and the kill switch was removed in the previous Budget. However, the fact that few companies registered under the government's new rules (35 companies in Mexico, compared to more than 100 in Chile in the same timeframe, mainly due to Mexico's incredibly complex registration process) led the government 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.[535] The regulation empowers tax authority to work with the telecom regulator to block non-resident internet platforms, preventing them from reaching Mexican users. There is no indication to date that the provision has been used and the vast majority of U.S. internet companies have registered and have been complying with these fiscal obligations.

Nevertheless, if widely used, this blocking technique 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.

Additionally, industry reports that 2020 legislation mandates that U.S. businesses that store product in Mexico must register for a local tax ID with the Tax Administration Service (SAT) and file monthly tax reports. The process to obtain this tax ID, dubbed a Registro Federal de Contribuyentes (RFC), imposes significant costs and burdens on firms and has developed into

---

[533] *Id*.

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

[535] 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.

the primary barrier for U.S. small and medium-sized enterprises that are pursuing expanding their markets to sell to consumers and businesses in Mexico.

U.S. firms must have a local Mexican address and local Mexican legal representative that shares at least 50% of the firm's tax liability to obtain an RFC, while also paying income tax on all revenue earned in Mexico. Firms are subjected to an arduous and bureaucratic registration process that includes apostilling of documentation in the United States; the use of a certified translator to produce all documentation in Spanish; use of a Mexican Notary to legalize documentation; waiting anywhere from one to four months for a SAT appointment; and registering the RFC in SAT's offices. These steps all must be conducted absent electronic streamlined processes, and thus can take over five months and impose costs over $5,000, which are not including the costs of complying with other income tax obligations.

In an August 2023 presidential decree, the government of Mexico introduced temporary 5-25% tariff rate increases on a set of various imports.[536] Metals, textiles, chemicals, oil, soap, paper, electronics, and furniture were among the products facing rate changes, which were introduced without prior public notice or consultation. The decree also pauses previously-planned tariff rate reductions. These tariff rate changes heighten the cost of importing into Mexico with little adjustment time for importers with the goal of conferring certainty to domestic industry players and addressing distortions in trade. The decree has an expiration date of July 31, 2025 (with exceptions for some sections).

Barriers to Energy Access

Mexican policymakers continue to establish obstacles for companies pursuing connection to the electricity grid and clean and reliable energy for purchase. These obstacles include diverting energy consumers to buy energy from the state-owned utility, the Federal Electricity Commission (CFE), and garnering disproportionate transmission infrastructure requests as part of the procedure to connect to the grid with the National Center for Energy Control (CENACE). The government, on the other hand, continues to bar entities from seeking all off-grid and private energy sources. U.S. companies are therefore unable to sufficiently locate their energy needs in Mexico, which compromises their clean energy targets. Industry appreciates the United States seeking dispute settlement consultations with Mexico under the USMCA over the matter.

Trade Facilitation and Border Obstacles

U.S. exporters report sustained challenges at the U.S.-Mexico border, as industry notes that the Mexican government has still not fully adhered to its commitments to customs facilitation made in USMCA, and instead is moving to impose new customs barriers that hinder U.S. small businesses from availing themselves of the open access promised to them under the agreement. U.S. exporters are facing a significant uptick in inspections and competing requests for information from several agencies simultaneously as conditions for going through customs. SAT's customs automation interface consistently falters, including after recent changes were

[536] *Mexico Imposes Temporary Import Duties*, WHITE & CASE (Aug. 21, 2023), https://www.whitecase.com/insight-alert/mexico-imposes-temporary-import-duties-25-more-588-non-fta-tariff-items.

abruptly made to tariff levels. These issues have further lengthened the wait times for crossing the border.

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 Intellectual Property Rights Chapter inappropriately narrows the application of this framework for internet services.

Likewise, the provision implemented through the amendment of in Article 232 Quinquies fr. II of the Copyright Law establishes administrative offenses fines when ISPs fail to 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.

Restrictions on Cloud Services

The National Banking and Securities Commission and the Central Bank of Mexico have issued Draft Provisions Application to Electronic Payment Fund Institutions ("IFPE"s) that significantly affect cloud computing service suppliers, who already report lengthy and uncertain approval processes from financial sector regulations in order to use secure U.S.-based cloud computing services. The new regulations could also lead to U.S. cloud services being disadvantaged in the region compared to local data center firms.

Article 50 of the draft provisions would require IFPEs that use cloud computing services to have a secondary infrastructure provider, once they reach certain transaction thresholds. Either this provider must have in-country infrastructure, or its controlling company must be subject to a different jurisdiction than that of the first cloud provider. A similar 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 store data in Mexico.

Article 49 would establish an authorization model based on 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.

The National Banking and Securities Commission administers approvals, a process that industry is concerned requires extensive resources and discriminates against non-Mexican providers, as data centers in Mexico are eligible for a shorter and more streamlined notification process. These rules represent a *de facto* data localization requirement, as U.S. and foreign firms are already subjected to a time-consuming and complicated process for approval. Industry is encouraged by the United States' statements that these obligations on cloud services providers

and electronic payment fund institutions could hinder U.S. competitiveness in the Mexican market.[537]

BB. Nepal

Government-Imposed Content Restrictions and Related Access Barriers

On Aug. 8, 2023, Nepal's Cabinet passed the National Cyber Security Policy, which adopted a "National Internet Gateway" similar to that passed and pursued by Cambodia in 2021.[538] This measure seeks to implement a government-owned intranet and an internet filtering system—a national internet gateway—that would restrict what content is visible online in the country. As the civil society group Article 19 details, the concern is that "if Nepal's national internet gateway is modeled on others in the region it would mean centralizing control of all internet traffic in and out of the country through a government-appointed operator, potentially supercharging surveillance and censorship capabilities while leaving open very serious questions about data privacy and protection, and the risk of criminal penalties for telecommunication companies."[539]

Taxation of Digital Products and Services

Nepal passed legislation on May 29, 2022 that would implement a 2% digital services tax (DST) to be collected from a specified list of digital services provided by non-residents to users in Nepal. The DST took effect on July 17, 2022 without any public consultation on the law itself or the procedures implementing the tax. The DST applies exclusively to non-resident companies; contradicts existing international tax principles; creates an additional burden of taxation with the potential of double taxation for non-resident companies; and establishes a disproportionate compliance burden for U.S. and other foreign companies due to the additional resources needed to comply with the DST's payment and reporting obligations.

CC. New Zealand

Taxation of Digital Products and Services

In June 2019, the New Zealand Government released a discussion document outlining two options relating to tax reform: (1) to apply a separate digital services tax to certain digital transactions, or (2) to change international income tax rules at the OECD.[540] The first option, the national DST, would be a 3% tax on gross turnover attributable to New Zealand of certain digital businesses. The businesses in scope include intermediation platforms, social media platforms, content sharing sites, search engines and sellers of user data. U.S. firms are specified throughout

---

[537] https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/january/readout-ambassador-jayme-whites-meeting-mexicos-under-secretary-economy-alejandro-encinas.

[538] https://api.giwms.gov.np/storage/22/posts/1691665949_27.pdf; https://myrepublica.nagariknetwork.com/news/govt-approves-national-cyber-security-policy-2023/.

[539] https://www.article19.org/resources/nepal-revise-cybersecurity-policy-to-avoid-further-internet-fragmentation/.

[540] 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/.

the discussion document as firms in the scope of the proposed tax. As with other DSTs, the tax may conflict with WTO commitments on national treatment, and as proposed, could be considered a proscribed 'covered tax' under various tax treaties designed to prevent double taxation, including the agreement with the United States.

On August 31, 2023, the government introduced a Digital Services Tax Bill that would empower the government to introduce, at an appropriate time, a 3% tax on gross revenues of large international firms with digitalized business models that earn revenue in New Zealand.[541] The effective date is expected to be January 1, 2025, which could be extended by an Order in Council if the government deems the progress of the Pillar One of the OECD's multilateral solution to be adequate.

CCIA urges New Zealand to eschew the proposed unilateral approach and continue its support for a multilateral solution with other nations.

Forced Revenue Transfers for Digital News

On December 4, 2022, the Minister of Broadcasting, Willie Jackson, announced the Government of New Zealand's plan to issue legislation mandating that "big online digital companies such as Google and Meta" pay news businesses from New Zealand for local news content that the platforms "host and share" on their services.[542] In the announcement, Jackson explicitly committed to developing legislation based on Australia's News Media Bargaining Code and Canada's Online News Act, Bill C-18.

On August 16, 2023, the government introduced the legislation, dubbed the "Fair Digital News Bargaining Bill," that would require designated digital platforms to pay news businesses for the ability to host news content, explicitly including news hyperlinks.[543] An impact assessment conducted by the New Zealand government reflected a clear targeting of two U.S. companies through this effort, and divulged that the government believes $40-$60 million per year could be extracted from registered digital platforms subjected to the law for the benefit of news businesses.[544] The bill has been referred to the Parliament's Economic Development, Science and Innovation Committee, which is soliciting public comment until November 1, 2023.

New Zealand's bill tracks closely with Canada and Australia's versions, with a few notable changes. Although New Zealand's version includes more specific parameters for designating digital platforms, news businesses can themselves apply to have a digital platform registered to

---

[541] Digital Services Tax Bill, available at https://www.taxpolicy.ird.govt.nz/bills/53-dst-23.

[542] https://www.beehive.govt.nz/release/big-online-platforms-pay-fair-price-local-news-content.

[543] *See* text of the legislation at: https://bills.parliament.nz/v/6/fc7faac0-2ec0-4e47-7ab5-08db9ebb2302?Tab=hansard.

[544] *Proactive release of Cabinet Material: Supporting commercial bargaining for online news*, Minister for Broadcasting and Media (Dec. 9, 2022) https://mch.govt.nz/sites/default/files/projects/cab-rel-online-news-151222.pdf at 11 ("Should the Government introduce a news media and digital platforms bargaining framework, the expected scale of the revenue that could flow from digital platforms to New Zealand news media organisations could be between $40 and $60 million per annum (about one-fifth of what is estimated to have been agreed in Australia)").

be subjected to the mandatory bargaining code. This power undermines any incentive of platforms to negotiate deals to obtain exemptions, as any disgruntled news businesses could seek designation regardless of whether they have bargained in good faith with the digital services providers. The legislation also contains concerning provisions regarding mandatory sharing of information and acting on requests for information or investigation from foreign regulators.

DD. 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,[545] and was condemned by the Economic Community of West African States.[546] 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.[547] Additionally, the government imposed one outright internet shutdown in 2022, a reflection of the concerning level of digital barriers U.S. online services providers experience in the country.[548]

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.

On June 12, 2023, Nigeria's president signed the 2023 Data Protection Bill into law, which established a Data Protection Commission and will regulate the collection, storage, and use of personal data of data subjects in Nigeria.[549] The law establishes rules and restrictions governing

---

[545] *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.

[546] *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.

[547] *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/.

[548] Access Now, supra note 47.

[549] https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf; https://placng.org/Legist/buhari-proposes-data-protection-law-to-nass/; https://www.itedgenews.africa/breaking-president-tinubu-signs-data-protection-bill-into-law/; https://fpf.org/blog/nigerias-new-data-protection-act-explained/.

cross-border data flows, including procedures for determining that a specific destination jurisdiction has adequate protections or authorization for the use of standard contractual clauses. The law also empowers the regulator to develop stricter restrictions on the ability to export data for different categories of personal data. The law applies to data controllers and processors extraterritorially. This concerns industry as it is often difficult to resolve differences involving various jurisdictions. The scope raises ambiguities regarding the respective operations of data controllers and processors.

A complicating factor is the emergence of a new agency in Nigeria, the Nigeria Data Protection Bureau, which was created in February 2022.[550] 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.[551] As the Data Protection Bill will be implemented by a brand-new agency, CCIA urges the U.S. government to ensure U.S. digital services exports are not adversely affected.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Nigeria NITDA's Content Development Guidelines of 2019/2020 requires all "sovereign data" to be stored locally.[552] While the guidelines fail to define sovereign data, industry reports that it is understood that all public sector workloads would fall under this category. The previous administration advanced the NITDA Bill and National Shared Services Corporation (NSSC) Bill to the National Assembly earlier in 2023. The Bill sought to broaden NITDA's supervisory rights over digital services providers and ICT use by companies, broaden NITDA's 1% tax on foreign digital platforms, introduce new requirements for ICT services, and empower NITDA to oversee the telecom industry. The NSSC Bill's target was to aggregate the provision of ICT infrastructure and services—including cloud services—to Nigerian federal agencies under a single, state-owned corporation. The goal was for government-controlled Galaxy Backbone to exclusively offer ICT infrastructure, services, and operations to Nigerian government entities. The National Assembly did not pass either of these bills before the elections that led to the change in administration, but industry remains wary that the new administration could advance the legislation again.

Taxation of Digital Products and Services and Other Restrictions

The 2020 Finance Act introduces income tax obligations for non-resident companies providing digital goods and services in Nigeria.[553] While the law applies to all non-resident companies earning above a certain threshold, extensive media coverage and analysis by experts has repeatedly mentioned the targeting of U.S. multinationals. The law specifically references non-

---

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

[551] *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.

[552] National Information Technology Development Agency, Guidelines for Nigerian Content Development in ICT (Aug. 2019), https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf.

[553] 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.

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,[554] 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.[555] Non-resident digital services firms are also required to pay 6% of their yearly turnover as well.[556]

Another restriction is developing in Nigeria, whereby the government requires all advertising of any kind to be approved by the Advertising Regulatory Council of Nigeria under penalty of fines. 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.[557]

EE. Pakistan

Government-Imposed Restrictions on Internet Content and Related Access Barriers

After prior iterations, and consultations the Ministry of Information Technology and Telecommunication (MoITT) released the "Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021," that were published and enacted on October 13, 2021.[558] 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, failing which the government would have the ability to 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;

---

[554] 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.

[555] *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/.

[556] *Id.*

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

[558] 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/.

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. Local and foreign companies have raised concerns over provisions that would pose significant obstacles to participating in Pakistan's market, including requirements to use mechanisms to monitor and block livestreaming content, take down content within short timeframes when the authorities issue demands, and disclose data to authorities in decrypted and readable formats. These rules greatly jeopardize the ability of U.S. firms to operate in Pakistan and undermine freedom of expression in what is a sizable market.[559]

Additionally, the Pakistani government implemented one outright internet shutdown in 2022 to counter protests, which as previously stated, imposes large economic losses and harms human rights.[560] In the case of Pakistan, the outlet *Rest of World* reported that representatives from the local tech sector said the internet shutdown set the industry "10 steps back" in Pakistan, and brought broad uncertainty that experts fear will depress foreign investment and catalyze an exodus of high-skilled workers.[561]

Restrictions on Cross-Border Data Flows

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 addressing 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.

On May 19, 2023, MoITT released an updated draft of the Personal Data Protection Bill. This bill has a broad scope, applying to both to digital and non-digital operators, and includes

[559] Asia Internet Coalition, *Letter to the PM on Removal and Blocking of Unlawful Content* (Dec. 2020), https://aicasia.org/policy-advocacy/pakistan-aic-submits-a-letter-to-the-pm-on-removal-and-blocking-of-unlawful-content/.

[560] ACCESS NOW *supra* note 47.

[561] *Pakistan's 4-day internet shutdown was the final straw for its tech workers*, Rest of World (June 8, 2023) https://restofworld.org/2023/pakistan-internet-outage-tech-workers/.

extraterritorial application.[562] The legislation includes concerning data localization requirements for "Critical Personal Data"—which itself is broadly defined. Additionally, the legislation grants the government of Pakistan effective veto power over cross-border data flows by stating that personal data can be exported if a data subject gives explicit consent and it "does not conflict with the public interest or national security of Pakistan."[563] Cross-border data flows are not sufficiently supported in the bill, as even for "non-critical" data, explicit consent is required for some cross-border data transfers. The bill does not specify whether such consent is necessary only for jurisdictions with inadequate data protection or for all jurisdictions.[564] The bill includes a sweeping mandate for defining "sensitive personal data" that explicitly includes financial data, which has broad implications for online services, as the government is granted obligatory access to such data under this legislation. The bill also includes burdensome requirements for data processing as well as a grant of broad powers to the regulator, with few guardrails. Pakistan's federal cabinet advanced the bill on July 26, 2023, and it now awaits Parliament's approval to becomes law.[565]

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Pakistan established a Cloud First Policy in 2022 that implements data localization requirements on broad categories of data identified as "restricted," "sensitive," and "secret." Further, the State Bank of Pakistan (SBP) prohibits financial institutions from storing and processing fundamental data troves on offshore cloud services. 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.

FF. Peru

Copyright Liability Regimes for Online Intermediaries

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

---

[562] *Draft of the Personal Data Protection Bill, 2023*: https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf; *Pakistan – MITT releases final draft of the personal data protection bill*, Allen & Overy (June 5, 2023) https://www.jdsupra.com/legalnews/pakistan-mitt-releases-final-draft-of-5697630/.

[563] *Draft of the Personal Data Protection Bill, 2023:* https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf Section 32(1)(b).

[564] *Submission on the Draft Pakistan Personal Data Protection Bill, 2023*, US Chamber of Commerce (July 21, 2023) https://www.uschamber.com/international/submission-on-the-draft-pakistan-personal-data-protection-bill-2023.

[565] *Pakistan needs to press pause on its data overhaul*, Atlantic Council (July 26, 2023) https://www.atlanticcouncil.org/blogs/new-atlanticist/pakistan-needs-to-press-pause-on-its-data-overhaul/.

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.[566] 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, and SOC 1, 2, and 3.

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.[567]

GG. Philippines

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. Subsequently, Senate Bill 1289 or the Online & Social Media Membership Accountability Bill,

[566] 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).

[567] Article 5.7(g)

was introduced in the legislature.[568] The bill would require electronic authentication that compels users to submit 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. Such a requirement would dampen free expression and represent an undue burden on online platforms serving customers in the Philippines.

Taxation of Digital Products and Services

The Income Tax Convention of 1976 is now in force in the Philippines. 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."[569] The Bureau of International Revenue (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 processing timelines, 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.

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.[570] This favorable treatment for Philippines entities is worsened by Commonwealth Act. No. 138 and Republic Act No. 9184,[571] 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 15% or less of the foreign bidder's offer.[572] These rules reflect general preference for domestic contractors and therefore hinder foreign entities from gaining access to government procurement work.

---

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

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

[570] *The 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184* (as of 31 March 2021), https://www.gppb.gov.ph/wp-content/uploads/2023/07/Updated-2016-Revised-IRR-of-RA-No.-9184-as-of-03-July-2023.pdf.

[571] Commonwealth Act No. 138 of 1936: https://elibrary.judiciary.gov.ph/thebookshelf/showdocs/29/53756; *The 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184* (as of 31 March 2021), https://www.gppb.gov.ph/wp-content/uploads/2023/07/Updated-2016-Revised-IRR-of-RA-No.-9184-as-of-03-July-2023.pdf.

[572] *Id.*

Data and Infrastructure Localization Mandates and 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 as a condition for providing cloud services to the public sector.[573] Absent an SEC license, entities seeking public sector procurement are forced to work with domestic entities, reflecting a *de facto* obligation.

Industry reports that the Philippines government is currently considering a draft Executive Order dubbed "Policy Guidelines on Data Localization of Data Stored in the Cloud" with concerning data localization provisions. The EO requires all data that is in any way connected to government work be processed and stored in the Philippines. This would include data that is non-sensitive and commercial, sensitive data. Further, the EO explicitly states that the following entities are required to use local infrastructure for processing: "Core operations of Bangko Sentral Supervised Financial Institutions deployed on private cloud;" "Health information systems of health service providers and insurers;" "Subscriber information of service providers located in the Philippines;" "All National Security Systems;" and "All sensitive personal information processed by private entities which are also classified as confidential under existing laws."[574] The application of the Executive Order is so broad that commercial services are highly likely to be subject to the data localization mandates, and outcome that will severely restrict the ability for online services providers—and non-digital services providers such as financial services—to operate in the Philippines.

Internet Transactions Legislation

A proposed bill, dubbed the Internet Transactions Bill, was passed by the Senate on September 26, 2023.[575] The legislation 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.[576] The proposed legislation would grant the Trade Minister broad powers to issue takedown orders as well as other obligations for online platforms providers such as mandatory registration to the Online Business Registry. Industry is concerned that the proposal would introduce obstructive requirements on electronic commerce platforms to have regulatory oversight such as mandatory collection of valid business certificates of merchants and subsequent submission to the government authority.

---

[573] See Government Procurement Policy Board Resolution No. 14-2021, https://www.gppb.gov.ph/wp-content/uploads/2023/05/GPPB-Resolution-No.-14-2021.pdf.

[574] https://globaldataalliance.org/wp-content/uploads/2023/09/09262023gsadatalocalcloud.pdf.

[575] https://legacy.senate.gov.ph/press_release/2023/0926_prib1.asp.

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

HH. Poland

Taxation of Digital Products and Services

As part of its broad tax reform initiative, the Polish Government has proposed the introduction of a minimum corporate tax levy, based on revenue.[577]

There is also a proposal for introduction of a media advertisement tax, which would be applied to all broadcasts, publishers, and large tech companies.[578]

II. Russia

After Russia invaded Ukraine, its actions towards U.S. digital firms became increasingly hostile. As a result of aggressive regulatory action and discriminatory practices, U.S. firms have been exiting the market, which has resulted in a significantly smaller U.S. presence. Russia's long-sought pursuit of an isolated internet infrastructure and ecosystem has accelerated, as has its removal from the global financial and business system. Russian authorities have seized many firms' financial assets, as was the case with Google.[579] Meanwhile, a state-run company has bought the search engine, news feed, and blogging services of Google's local competitor Yandex, expanding the Kremlin's control of the domestic internet.[580] This has left Russia with a largely isolated internet.[581] According to Meta's internet disruption center, services were down in Russia for the entirety of its July-December 2022 reporting period.[582]

Government-Imposed Content Restrictions and Related Access Barriers

Russia continues to serve as a model of government-imposed control of internet services and online speech. As detailed below, Russia has passed many new laws that grant Russian authorities with greater control over online communications and services, and impose a number of obligations on services to comply with government demands. Over the past several years,

---

[577] 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.

[578] KPMG, *Taxation of the digitalized economy* (Oct. 10, 2023), https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/digitalized-economy-taxation-developments-summary.pdf at 51.

[579] 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 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/.

[580] *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/.

[581] *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.

[582] Meta, Internet Disruption, https://transparency.fb.com/data/internet-disruptions/ (last visited Sep. 29, 2023).

Russia's telecommunications regulator has veered away from its primary objective towards a quasi-intelligence agency, orchestrating the Kremlin's censorship and surveillance activities.[583]

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 2022, Russia enacted a "fake news" law which prohibited the publication of what the government determined to be falsehoods about the war in Ukraine—including calling the war an "invasion."[584] The campaign to control news in Russia has been prominent online. In August 2023, Google was found guilty by a Russian court for leaving up YouTube videos on the war in Ukraine after being ordered to take them down for being "prohibited" and "false" information, according to Russian state news reports.[585]

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.[586] Russia blocked use of Facebook in March 2022.[587] 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 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 equalled 5-10% and 8% of the company's yearly turnover earned in Russia, respectively. Despite the tension, a leading lawmaker for information policy in the Duma suggested in June 2022 that YouTube is not yet under threat of being blocked in Russia.[588]

Other enforcement actions Russia has taken regarding what it has deemed "misinformation" or "fake news" include its block of Soundcloud in October 2022 for spreading "false

---

[583] *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.

[584] *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/.

[585] https://y3r710.r.eu-west-1.awstrack.me/L0/https:%2F%2Fdmp.politico.eu%2F%3Femail=hgreenfield@ccianet.org%26destination=https:%2F%2Ftass.ru%2Fekonomika%2F18528253/1/0102018a03a9ff25-8f1e85bd-ae96-492c-9c3a-a428857af1bb-000000/Swsk7GchjsZ0Wa7mgMxXBYmk1Ao=335.

[586] *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.

[587] 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.

[588] *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/

information,"[589] a $373 million of Google in July for repeated "fake news,"[590] and a $33,000 fine of Twitch in August 2022 for hosting a brief video with purported "fake" information about the invasion of Ukraine.[591]

Other laws include Federal law N482-FZ and Federal law N511-FZ, which came into effect in 2021.[592] 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 past years, U.S. firms experienced an increase in demands by the Roskomnadzor, which regulates internet services, to take down content, including through requests pursuant to these new rules. Firms that Russian authorities determine have not sufficiently complied with demands have experienced an uptick in throttling and restriction in services.[593]

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 law permits 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.[594] In March 2019, Russia passed two laws aimed at eliminating "fake news." The Federal Law on Amending Article 15-3 of the Federal Law on Information, Information Technologies and Protection of Information[595] and the Federal Law on Amending the Code of Administrative Violations,[596] establish penalties for "knowingly spreading fake news" and establish a framework for ISPs to block access to websites deemed to be spreading "fake news."

---

[589] *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/

[590] *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/.

[591] *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/.

[592] 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/putin-regime-will-never-tire-imposing-internet-control-developments-digital-legislation-russia.

[593] *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.

[594] *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/.

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

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

In December 2019, Russia adopted a law that requires the pre-installation of Russian software on certain consumer electronic products sold in Russia.[597] The law took effect in early 2021.[598] The scope of devices includes 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 also 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.[599] 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."[600] That action followed a revelation in mid-March from a senior Duma member that at least 20 VPN services were being blocked in Russia as would others if deemed to be in violation of Russian law.[601]

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[602] resulted in an estimated $200,000 in losses, [603] 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.[604]

---

[597] 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.

[598] *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.

[599] 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.

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

[601] 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/.

[602] 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/

[603] 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/.

[604] USITC, Foreign Censorship Part 2, *supra* note 48, at 74.

Further, these restrictions are not limited to Russia. 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.[605] In July 2022, Russian-backed separatists blocked Google due to purported spread of "disinformation" in a breakaway region of eastern Ukraine.[606] Regional internet outages have occurred throughout Ukraine since Russia began its war campaign in the country,[607] with some areas experiencing blackouts for multiple days—in some cases due to reported Russian cyberattacks.[608] All of these actions represent deeply concerning damage 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 has to "land" by establishing a local unit that will represent its interests in Russia and will be liable for its activities.[609] 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) they are in Russian or a Russian local language; (ii) they have ads targeted at Russian users; (iii) the website/app owner processes Russian user data; or (iv) websites/apps receive money from Russian individuals and legal entities. Amongst other requirements, foreign companies will also be required to install Russian Government-provided software which will count 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 on Russian companies or users advertising with such foreign platforms or transfering money and make payments, and potential full or partial blocking or throttling of the noncompliant website or applications. Such local presence requirements, coupled with onerous

---

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

[606] *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/.

[607] *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.

[608] *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.

[609] 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.

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.[610] 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.[611] 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.[612] As Article 19 highlights, establishing a 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 or other political issues; and easier to threaten jail time to company representatives residing in the country.[613] Fines, and threats of jail time for employees leave U.S. digital service suppliers with few options.

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.[614] The court's announcement of the fines on Telegram cite "repeated violations" of the country's data localization laws.[615] In June 2022, a Moscow court fined Google 15 million roubles ($260,000) for being found to have repeatedly declined to adhere to data localization laws.[616] These court cases and fines are likely to continue—Roskomnadzor had also announced that an administrative case against Apple had begun in late May.[617]

---

[610] *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.

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

[612] *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/.

[613] 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/.

[614] *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.

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

[616] *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/.

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

On March 1, 2023, amendments were made to Russia's Federal Law on Personal Data.[618] These amendments establish, as a pre-condition for cross-border personal data transfers, transfer impact assessments as well as a requirement to file reports with the data protection authority. It also establishes that Russia "may suppress outgoing data flows in an extra-judicial procedure." The Federal Service for Supervision of Communications, Information Technology, and Mass Media announced on March 1, 2023 that new provisions in line with the amendment are now in force.[619]

JJ. Saudi Arabia

Restrictions on Cross-Border Data Flows

The Communications and Information Technology Council of Saudi Arabia (CITC) issued the Cloud Computing Regulatory Framework in 2018, with revisions made in 2019.[620] The rules contain a provision on data localization that may restrict access to the Saudi market for foreign internet services.[621] 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 hosted and stored when using cloud computing services must be located with the country.[622] The (NCA) has imposed data localization through the ECC framework for government entities and state-owned enterprises and Critical National Infrastructure (CNI). The regulation includes a data localization obligation for these bodies, noting that an "organization's information hosting and storage must be inside the Kingdom of Saudi Arabia."[623] A separate localization mandate relating to cybersecurity services stipulates that "cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia." This requirement includes a wide range of customers such as financial services, aviation, and oil and gas that by their design rely on the

---

[618] https://www.lexology.com/commentary/tech-data-telecoms-media/russia/gorodissky-partners/russia-adopts-new-rules-on-cross-border-data-transfers.

[619] https://www.dataguidance.com/news/russia-new-procedures-data-transfers-enter-effect.

[620] *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.

[621] *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.").

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

[623] NATIONAL CYBERSECURITY AUTHORITY, *Essential Cybersecurity Controls ECC 1:2018*, *available at* https://documents.pub/document/essential-cybersecurity-controls-ecc-a-1-2018-itig-iraq-2019-08-12-2-4.html?page=1.

steady and free flow of data across borders to sustain and strengthen their operations and protect them from cyber threats.

Industry reports that the Cloud Cybersecurity Controls issued by the NCA also obligate companies offering cloud computing services in-country—such as systems used for storage processing, disaster recovery centers, and systems used for monitoring and support—to store data locally. The controls permit level 3 and 4 data to be hosted abroad, but entities would be required to seek the exemption to avoid localization mandates.

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.[624] 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."[625] Entities that seek to process personal data are required to register and pay an annual fee, and non-Saudi companies that process the personal data of Saudi residents are mandated to have a local representative.[626] 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 with a user's express consent except for 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.

Experimental Platform Regulation

In July 2022, the Saudi Arabian Communications & Information Technology Commission published its Draft Competition Regulations for Digital Content Platforms with the goal of regulating large online digital services platforms.[627] The draft regulations contained concerning provisions such as arbitrary thresholds to determine designated services providers under the law rather than utilization of a robust market analysis to illustrate a market failure; vague definitions for what targeted online services providers are prohibited from doing, such as "inappropriately and anti-competitively" favoring their own services; and attempts to bring untested regulatory proposals from elsewhere in the world to the Saudi market without (1) those regulations first showcasing whether or not they work and (2) demonstrating the need for such regulations in the

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

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

[626] *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/.

[627] https://istitlaa.ncc.gov.sa/en/transportation/citc/crdcp/Documents/Competition%20Regulations%20for%20Digital%20Content%20Platforms.pdf.

Saudi market first.[628] The regulations have not yet been adopted by the Saudi government but given the spread of these policies and their potential to hinder the ability of U.S. firms to operate and innovate in markets such as Saudi Arabia, industry urges USTR to monitor developments in the country closely.

KK. Singapore

Government-Imposed Content Restrictions and Related Access Barriers

The Protection from Online Falsehoods and Manipulation Bill became effective starting on October 2, 2019.[629] 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.[630] 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.[631] Stakeholders have raised concerns with enforcement of these laws since they went into effect,[632] 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.[633] The use of POFMA has moderated throughout past 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.[634] 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

---

[628] https://ccianet.org/library/ccia-comments-on-the-saudi-arabian-citcs-draft-competition-regulations-for-digital-content-platforms/.

[629] 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.

[630] *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/.

[631] *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.

[632] *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.

[633] *Freedom on the Net 2023: Singapore* (2023), https://freedomhouse.org/country/singapore/freedom-net/2023.

[634] *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.[635]

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. The guidelines were finalized on July 17, 2023, and went into effect on July 18, 2023, with Facebook, HardwareZone, Instagram, TikTok, Twitter, and YouTube the initial companies named as subject to the Code.[636] The guidelines released by IMDA for companies' adherence to the Code include vague directions to address specified content including "content that is likely to cause harassment, alarm, or distress;" "content relating to vice, unlawful gambling, illegal moneylending, trafficking in persons, cheating, fraud, and extortion;" and "content relating to the incitement of violence, mass disorder, or rioting, whether in general or targeted at persons based on their characteristics."[637] While many of these directions could apply to objectionable content that most online services suppliers would normally prohibit or restrict from their platforms, the directions could also apply to reasonable content such as satire, art, or protests, depending on the situation. 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.[638]

On November 9, Singapore's Parliament passed legislation imposing new obligations on social media providers called the Online Safety (Miscellaneous Amendments) Bill.[639] The bill took effect in February 2023.[640] The bill requires large "online communications services" ("OCS"), which include social media services, to comply with a Codes of Practice, as well as empower the Infocomm Media Development Authority to regulate specified categories of "egregious content" that can be accessed through an OCS. The law makes providers of "electronic services"—defined as online services that connect to Singapore and are not explicitly communications or internet service providers—liable for content posted on their platforms. The legislation requires services to remove "egregious content" from its platforms, which includes content that "advocates or instructs on suicide or self-harm;" "advocates or instructs on violence or cruelty"

---

[635] *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.

[636] https://protect-eu.mimecast.com/s/ORryCDkKMTWvBx5iqySSw?domain=sites-twobirds.vuture.net.

[637] https://www.imda.gov.sg/-/media/imda/files/regulations-and-licensing/regulations/codes-of-practice/codes-of-practice-media/guidelines-for-code-of-practice-for-online-safety.pdf.

[638] 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.

[639] https://www.lexology.com/library/detail.aspx?g=cf562568-bd0c-488c-84ef-51a458e1a061; https://www.parliament.gov.sg/docs/default-source/default-document-library/online-safety-(miscellaneous-amendments)-bill-28-2022.pdf.

[640] https://www.allenandgledhill.com/sg/publication/articles/23174/legislation-to-tackle-harmful-content-on-online-services-accessible-to-users-in-in-force.

against other people; "advocates or instructs on sexual violence;" shows nudity of a child; restricts or harms public health measures; stokes racial or ethnic hatred; and promotes or instructs terrorism. The Infocomm Media Development Authority of Singapore will be empowered to issue demands to remove content or restrict service to specific users, and if companies fail to comply, the IMDA can block the service provider in question.

A separate bill, the Online Criminal Harms Bill ("OCH Bill"), passed on July 5, 2023.[641] The law gives the Singapore government more powers to issue "Government Directions" when there is reasonable suspicion that online activity is being carried out to commit a crime specified in the First Schedule of the OCH Bill, or when it is suspected that any website, account or online activity is being used for scams or malicious cyber activities. These include: offenses relating to terrorism and internal security, harmony between different races, religion or classes, trafficking of controlled drugs and psychoactive substances, unlawful gambling, illegal moneylending, and sexual offenses (*e.g*. distribution of child sexual abuse material or voyeuristic and intimate images without consent).

Foreign Interference (Countermeasures) Act

The Foreign Interference (Countermeasures) Act (FICA) was passed on October 4, 2021 and went into effect in July 2022.[642] 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.[643]

LL. South Africa

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Industry reports concern that South Africa's Cloud Computing Policy, which is expected to be published by the Department of Communications and Digital Technologies (DCDT) by the end

[641] https://www.lexology.com/library/detail.aspx?g=25b4c254-d7a0-41f5-b263-7847a82e15fb; https://www.parliament.gov.sg/docs/default-source/default-document-library/online-criminal-harms-bill-17-2023.pdf.

[642] *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.

[643] 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.

of 2023, contain references to data sovereignty and explicitly incentivizes the use of local providers in government cloud outsourcing. Private sector consultations on the latest draft are ongoing, but a data localization provision in a major market for U.S. suppliers would prove to be a significant barrier to participation in the market.

MM. Spain

Taxation of Digital Products and Services

On October 7, 2020, the Senate approved legislation to impose a digital tax of 3% of revenue derived from online advertising services, the sale of online advertising, and the sale of user data.[644] 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.[645] However, Spain was among the countries that imposed a DST with whom the United States reached an interim agreement, and any payments made under the Spain DST can be accredited upon implementation of the OECD Pillar 1 solution.[646]

NN. Taiwan

Experimental Platform Regulation

The Taiwan Fair Trade Commission (TFTC) released the finalized version of the White Paper on Competition Policy in the Digital Economy in December 2022, addressing 14 competition issues related to the digital economy, including market definitions, platform operators' practices, price discrimination, data privacy, bargaining between platforms and news media, algorithms, and false advertising. [647] The TFTC presents its enforcement position and response measures for

---

[644] 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

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

[646] *See* https://home.treasury.gov/news/press-releases/jy0419.

[647] https://www.ftc.gov.tw/internet/english/doc/docList.aspx?uid=1942.

each issue based on analysis and enforcement precedents. It also suggests amending current laws and regulations to address these issues, such as reviewing market definition guidelines, expanding laws on concerted actions, and strengthening the TFTC's authority on market surveys. The TFTC plans to integrate information technology into case analysis and leverage talents in this field to enhance enforcement in the digital economy.

Forced Revenue Transfers for Digital News

In May 2023, the Education and Culture Committee approved a motion directing the Ministry of Digital Affairs to develop a news media bargaining law.[648] The government is currently in the process of engaging in dialogues with digital firms as it develops the law, with the third round of dialogues concluding in September 2023 with no agreement. Despite the cooperation between industry and government, industry remains concerned and urges the U.S. government to continue to push back on mandatory revenue transfers from digital services providers to local news businesses.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In August 2023, the Financial Supervisory Commission (FSC) announced updated amendments to the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, which stipulate the rules for financial institutions to obtain FSC's permission prior to using cloud computing services.[649] The new amendments seek to simplify the application process, which requires submitting up to 17 documents, responding to duplicate audit requests and a lengthy review process. Industry remains wary that failure to simplify the process could discourage financial institutions from using cloud computing services, all of which limits market access for U.S. cloud services providers.

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' ability to contract with firms in these sectors, who themselves state regulatory uncertainty restricts them from adopting cloud services.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

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 service suppliers, regulators clearly indicate a preference for data localization, stating that "in principle, where customer data is outsourced to a cloud service provider, the location for processing and storage shall be within the

---

[648] https://www.taipeitimes.com/News/taiwan/archives/2023/05/23/2003800275.

[649] https://www.fsc.gov.tw/en/home.jsp?id=54&parentpath=0,2&mcustomize=multimessage_view.jsp&dataserno=202308180003&dtable=News.

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."

If an institution seeks approval for overseas outsourcing, it has to bear the over-burdensome documentary requirements which may cause unnecessary compliance cost; even if an institution 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.

Regulations have been promulgated in both the financial services and health industries that advance the data localization issue in both sectors. For financial services, industry reports that regulations require that material financial customer data are stored in Taiwan, unless the regulatory agency grants an exemption. Similarly, in the healthcare sector, regulations governing Electronic Medical Records Management mandate that medical data remain stored in Taiwan absent the granting of an exemption. For both types of data, industry is left with vague and unclear regulations delineating the manner in which an exemption can be obtained.

Through a September 2023 draft amendment to the Cybersecurity Management Act (CSMA), sectoral regulators would be directed to adopt rules delineating the criteria and the procedure behind the labelling of a critical infrastructure (CI) provider. The draft defines CI as "physical or virtual systems or networks, used in the critical fields formally announced by the Cabinet, once discontinued from operation or becoming less effective, would lead to significant negative impact upon the national security, public interests, living standard of citizen and economic activities." The draft does not detail how the Cabinet should select and choose the so-called "critical fields," which foments uncertainty.

Restrictions on Over-the-top (OTT) Services

The National Communications Commission (NCC) in Taiwan has revealed a preliminary legislative proposal for 2023 that seeks to enhance regulations on OTT content,[650] including audits prior to broadcast and more requirements and prior approvals on transfer of control and ownership. Given the growing popularity of OTT TV services, the NCC emphasizes the need for consumer protection and may impose rules similar to those applied to cable and satellite TV operators, in addition to general obligations on content provision.

Ban on China-Branded Goods

On September 22, 2023, the Taiwanese Government announced a draft amendment to the Cybersecurity Management Act (CSMA) that would prohibit government agencies from utilizing 'China-Branded' products.[651] Although the ban is imposed directly on Taiwanese government agencies, there are indirect effects on solution providers that will be contractually obligated to comply with the prohibition. The definitions are poorly-defined or opaque, such as that serving as the basis for "China-branded," as well as the scope of ICT products. The draft also does not

[650] https://www.lexology.com/commentary/tech-data-telecoms-media/taiwan/shay-partners/nccs-plan-to-amend-broadcasting-bills.

[651] *Taiwan Digital Ministry Proposes Modest Amendments to Cybersecurity Management Act*, BOWER GROUP ASIA (Oct. 2, 2023), https://bowergroupasia.com/taiwans-digital-ministry-proposes-modest-amendment-to-cyber-security-management-act/.

define "products that endanger national cyber security" or the criteria and procedure governing the decision process over whether a product should be deemed to threaten national cyber security. A supplier may not have awareness that its products are banned from public sector adoption and has no mechanism to request an appeal. U.S. and other foreign firms participating in the market face obstacles to conducting business in the country due to the vague outlines of the proposal that introduces practical obstacles. A public consultation is ongoing.

OO. Tanzania

Taxation of Digital Products and Services

Tanzania adopted a 2% DST as part of its 2022-2023 Budget and issued regulations on July 1, 2022.[652] The DST is imposed on revenue made by any non-resident person soliciting a Tanzanian-sourced payment from an individual. The DST does not apply to payments made in the course of conducting business through services rendered on a digital marketplace. The Tanzanian DST does not include a minimum threshold, which means U.S. companies are subjected to the DST after the first dollar of in-scope revenue. CCIA urges USTR to encourage Tanzania to participate in the OECD/G20 Inclusive Framework's efforts to address the tax challenges arising from the digitalizing global economy instead of imposing discriminatory taxes.

PP. Thailand

Government-Imposed Content Restrictions and Related Access Barriers

CCIA has previously raised concerns with the Computer Crime Act, amended in 2016.[653] 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.[654]

In 2019, Thailand passed a controversial Cybersecurity Law following amendments in 2018. Industry has criticized the law due to provisions that enable government surveillance.[655] Under

---

[652] *Will 2023 See Higher Digital Service Subscription Costs?,* PwC (2023), https://www.pwc.co.tz/press-room/will-2023-see-higher-digital-service-subscription-costs.html.

[653] https://ccianet.org/wp-content/uploads/2022/10/CCIA-Comments-2023-National-Trade-Estimate-Reporting.pdf.

[654] *Freedom on the Net 2023: Thailand* (2023), https://freedomhouse.org/country/thailand/freedom-net/2023; https://www.nationthailand.com/in-focus/40010570.

[655] *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.").

the new law, officials are granted authority to "search and seize data and equipment in cases that are deemed issues of national emergency."[656]

The Thailand Electronic Transactions Development Agency (ETDA) introduced the Draft Royal Decree on the Supervision of Digital Platform Services in August 2021 and approved by the cabinet in late October 2021.[657] The 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.

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.[658] The government has been conducting hearings to develop implementing regulations and laws for the broader Decree, which are still under way.[659]

Restrictions on Cross-Border Data Flows

The Personal Data Protection Act went into effect on June 1, 2022, which tracks with some of GDPR, but veers from it with respect to some data transfer provisions.[660] As a general matter, the law 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 creates liability for U.S. online services, as they may be subject to its reach if

---

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

[657] 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/.

[658] 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

[659] https://www.lexology.com/library/detail.aspx?g=0ca26c82-75fd-4065-a8b7-4a56c853f26e.

[660] 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/.

they decline to establish a business presence in Thailand but have Thai individuals that use their services.[661]

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. This draft, called the "Notification of the personal data protection committee on rules and principles of appropriate personal data protection for international transfer" was published in September 2022.[662] 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 highly restrictive for businesses that would be obligated to wait for consent from each of its customers in Thailand to approve what is usually seen as a standard business decision requiring swift action.

Experimental Platform Regulation

On December 23, 2022, Thailand issued a Royal Decree ("the Decree") affecting operators of digital platforms.[663] The Decree focuses on digital platforms that service more than 5,000 monthly users in Thailand and annual revenue in Thailand of around $1.5 million, regardless of the origin of the service provider. A "Digital Platform Service" is defined as "a service that provides an electronic medium for managing data and connecting businesses, consumers, or service receivers through computer networks for the purpose of electronic transactions, with or without a service fee." This could include a wide variety of websites and services, as it appears to include any digital service that connects users and merchants regardless of payment. The Decree imposes a series of duties on providers. First, the Digital Platform Service provider must notify the Electronic Transactions Development Agency ("EDTA") prior to commencement of business and existing providers must notify the EDTA within 90 days after the decree becomes effective. Second, the Digital Platform Service provider must provide an annual report to the ETDA. Third, the ETDA may impose transparency requirements on some Digital Platform Service providers regarding specific details related to the services. Fourth, the ETDA is authorized to gather information about the platform from other state agencies. Finally, certain overseas platform providers who fall within certain criteria must appoint an agent based in Thailand. Penalties for non-compliance include suspension of business and criminal liability. The Decree went into effect on August 20th, 2023.

---

[661] DLA PIPER, *Data Protection Laws of the World: Thailand*, https://www.dlapiperdataprotection.com/index.html?t=law&c=TH.

[662] 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.

[663] https://www.lexology.com/library/detail.aspx?g=6b9472b0-4d5c-4761-a6d5-ffc92c10b9e1; https://www.lexology.com/library/detail.aspx?g=11ddcb45-1ce3-495a-be39-26eb7c4e1ae6.

QQ. 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.[664] CCIA has previously identified laws that preemptively block websites on vague grounds, and specific instances of blocking by Turkish authorities.[665] 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.[666]

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,"[667] in July 2020 that grants the government sweeping new powers to regulate content on social media.[668] The law went into effect October 1, 2020, and authorities were quick to take action against U.S. firms, imposing fines,[669] advertising bans, and bandwidth restrictions within months.[670] 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.

---

[664] *Freedom on the Net 2023: Turkey* (2023), https://freedomhouse.org/country/turkey/freedom-net/2023.

[665] 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.

[666] USITC, Foreign Censorship Part 2, *supra* note 48 at 74

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

[668] *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.

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

[670] *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 passed the "Law Proposal on the Amendment of the Press Law and Some Laws" in October 2022. The law introduced restrictions on the operations of online platforms—with stricter requirements for larger companies—while also clamping down on freedom of expression in the name of combatting online disinformation.[671]

The law will require platforms to disclose their algorithms and the personal information of users to the government upon demand. The law criminalizes 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.[672]

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.[673] 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 law gave 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

---

[671] 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.

[672] *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.

[673] *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.

that provider to a level rising up to 95% restriction on the usual bandwidth capacity or outright block the service.[674]

A new ruling published by the ICTA in April 2023 introduces significant regulations for social network providers, including the appointment of representatives, reporting obligations, data storage requirements, protection of children, handling security breaches, information sharing with judicial authorities, and sanctions for non-compliance.[675] The decision imposes administrative fines and advertising bans for violations, grants inspection authority to the ICTA, and holds social network providers responsible for user-generated content. The decision came into effect on April 1, 2023, without a transition period.

Elsewhere, the Information Technologies and Communication Authority (BTK) issued a new decision regarding procedures and principles for social network providers, effective from April 1, 2023.[676] This decision updates the responsibilities and obligations of social network providers in accordance with the additional article 4 of Law No. 5651. The decision outlines the obligations, implementation, and regulations for social network providers, including the appointment of a representative in Turkey, responding to content-related applications, reporting to the BTK, creating an advertisement library, and storing user data in Turkey. Additionally, social network providers must inform judicial authorities about certain crimes, provide separate services for children, protect user rights, establish an effective application mechanism for removing content, share information with law enforcement, submit requested information to the BTK, and create a crisis plan. Detailed sanctions are outlined for non-compliance, including administrative fines based on the breached obligation and frequency of the breach.

Taxation of Digital Products and Services

Turkey enacted a 7.5% digital tax which became effective March 1, 2020. The legislation also permits the President of Turkey to either reduce the rate to 1%, or double the tax to 15%.[677] The global revenue threshold for this tax is 750 million euros, with a local threshold of 20m TYR. The tax applies to revenue generated from the following services: first, "all types of advertisement services provided through digital platforms;" second, "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 third, services "related to the provision and operation services of digital platforms where users can interact with each

[674] *New Regulations Expected for OTT Service Providers* (July 2022), https://gun.av.tr/insights/articles/new-regulations-expected-for-ott-service-providers.

[675] https://www.lexology.com/library/detail.aspx?g=a799c704-d8c6-4235-a0cc-2f40dc78d586; https://www.lexology.com/library/detail.aspx?g=43c9b557-836e-444a-b86c-56c7bfc5f278.

[676] https://www.lexology.com/commentary/tech-data-telecoms-media/turkey/zdastanli-ekici-attorney-partnership/btk-issues-new-decision-on-procedures-principles-and-regulations-that-apply-to-social-network-providers-in-turkey.

[677] 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.

other."[678] 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.[679] In November 2021, Turkey struck a 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.[680]

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In 2019, a Presidential Circular on Information and Communication Security Measures imposed localization requirements on government workloads determined to be "strategic."[681] In 2020, industry reports the Digital Transformation Office published guidelines detailing the applicability of the localization requirements to be inclusive of critical information and data. However, the vaguely-defined residency requirements under the Presidential Circular continue to represent a hurdle as the legislation supersedes the DTO Guidelines. Industry reports that the Central Bank of Turkey imposes similar restrictions on cloud outsourcing, and bars the use of cloud for certain workloads.

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.[682] The Regulation establishes a framework for use of cloud services as an outsourced service, but only applies for services located in Turkey.[683]

Restrictions on Cross-Border Data Flows

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.[684] However, industry reports that conditions make it hard to transfer data under these frameworks. Turkey has still not yet announced a list of countries that

---

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

[679] *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.

[680] 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.

[681] Presidential Circular on Information and Communications Security Measures No. 2019/12, *available at* https://cbddo.gov.tr/en/presidential-circular-no-2019-12-on-information-security-measures.

[682] *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.

[683] *Id*.

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

meet the standard of adequate level of protection as of 2023.[685] Further, the Data Protection Board has yet to grant approval to companies that have sought the ad-hoc approval. The adequacy decision has been postponed several times since 2021—the latest timeline for the announcement is expected to be towards the end of 2024.

Experimental Platform Regulation

In October 2022, the Turkish Competition Authority released a draft amendment to Law No. 4054 on the Protection of Competition to impose a wide range of obligations and prohibitions on "Core Platform Services."[686] The rules largely track with the EU's Digital Markets Act, while adding concerning new restrictions on services providers. The rules stipulate that "Undertakings Holding Significant Market Power" would be required to "enable the interoperability of core platforms services and/or ancillary services and fulfil the technical requirements for this" while also prohibiting such "Undertakings" from self-preferencing their own products and services. Further, prohibitions on the cross-service utilization of data could obstruct U.S. services suppliers' operations in Turkey.[687] The process behind the development and advancement of this legislation is concerningly opaque and fast-moving, potentially being written into law.

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 went into effect on January 1, 2023.[688] Firms that facilitate sales equalling or topping ten billion Turkish lira net ($538.3 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.[689] E-commerce providers are also 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.

---

[685] https://academic.oup.com/idpl/article/13/1/25/7025584.

[686] https://www.mondaq.com/advicecentre/content/1540/Law-No-4054-on-the-Protection-of-Competition-Competition-Law; https://competitionlawblog.kluwercompetitionlaw.com/2022/10/25/a-new-age-for-digital-markets-in-turkey-the-draft-amendment-to-the-law-no-4054-on-the-protection-of-competition/.

[687] https://ccianet.org/wp-content/uploads/2022/11/CCIA-Comments-on-the-Draft-Amendment-to-Law-No.-4054-of-the-Protection-of-Competition-in-Turkey.pdf.

[688] *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/.

[689] *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.").

A new collection of regulations on e-commerce was published in the Turkish Official Gazette in December 2022 and went into effect on January 1, 2023.[690] The regulation aims to define procedures and principles for e-commerce operations and supervision, ensuring a fair competitive environment and the development of electronic commerce. The Regulation addresses violations of intellectual and industrial property rights. Complaints can be filed against such violations, and the relevant e-commerce intermediary service provider must remove the infringing goods within 48 hours and inform the e-commerce service provider and right holder. E-commerce service providers can object to the complaint with solid explanations and evidence. If the objection is deemed valid, the offering for the goods can be republished within 24 hours. Further complaints about the same product and claim will not be processed without additional proof of rights. The examination is limited to the information and documents provided by the e-commerce service provider and allows individuals to seek judicial or administrative remedies. It complements existing legislation that partially addressed these issues by clarifying the responsibilities of hosting service providers in removing illegal content upon notification and addressing the limitations of the "warn & remove" method.

RR. Uganda

Taxation of Digital Products and Services

The Ugandan government adopted a digital services tax (DST) that institutes a 5% tax on revenue earned by non-residents offering digital services to Uganda-based consumers, which went into effect on July 1, 2023. In-scope digital services include online advertising services; data services; services provided via an online marketplace or online intermediary; digital content services; online gaming services; cloud computing services; and other services rendered via a social media website or a search engine.[691] U.S. digital services providers would be subjected to the DST after the first dollar of revenue it earns, as the law does not include thresholds for in-market activity.

SS. United Arab Emirates (UAE)

Licensing Requirements for Social Media Influencers

The 2018 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 as well as those that have paid associations with brands or foundations.[692] 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

[690] https://www.lexology.com/library/detail.aspx?g=c4af283b-27e1-447e-abc3-e26b0532ee65.

[691] *A Look Into Uganda's Digital Services Tax*, GLOBAL VOICES (Oct. 17, 2023), https://globalvoices.org/2023/10/17/a-look-into-ugandas-digital-services-tax/.

[692] https://www.hg.org/legal-articles/license-requirements-for-social-media-influencers-in-uae-57336.

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.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The UAE Cybersecurity Council (CSC) mandates that data workloads at the federal (UAE) and Emirate-level are hosted in servers in the UAE.[693] Industry reports that this longstanding obligation is imposed on government agencies and state-owned commercial enterprises alike. Similar localization requirements are now imposed on data processing for the financial services and healthcare sectors. The UAE Central Bank's outsourcing guidelines ban financial services institutions—not including subsidiaries of foreign banks—from storing and processing personal data outside the country. The UAE 2019 Health Law also obligates processors to conduct activities for health data within the UAE. Further, industry reports that Abu Dhabi ADHICS Standards disallow hosting information sharing systems on cloud services.

TT. United Kingdom

Government-Imposed Content Restrictions and Related Access Barriers

The UK Parliament passed the "Online Safety Bill" on September 19, 2023, [694] a law 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."[695] The bill aims to compel the "biggest and most popular social media platforms," search engine providers, messaging services, cloud storage providers, and other content platforms to implement a litany of measures 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.[696]

One July 2022 amendment added 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.[697] 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.

---

[693] U.S.-U.A.E. BUSINESS COUNCIL, Promoting Free and Secure Data Flows, Data Privacy and Localization, https://usuaebusiness.org/focusareas/promoting-free-and-secure-data-flows-data-privacy-and-localization/.

[694] https://www.gov.uk/government/news/britain-makes-internet-safer-as-online-safety-bill-finished-and-ready-to-become-law.

[695] Policy Paper: Online Safety Bill Factsheet (Apr. 2022), https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet.

[696] *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/

[697] 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.

Following the Online Safety Bill's passage, providers of end-to-end encrypted services suggested they may leave the UK market due to the undermining of private firms' digital security.[698]

Taxation of Digital Products and Services

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%. The tax is to be paid on an annual basis, with accruals beginning April 1, 2020. The tax applies to revenues of "digital services activity" which are "social media platforms," "internet search engines," or "online marketplaces." The practical effect of the tax is that a handful of U.S. companies are contributing the majority of the tax revenue. The UK was among the countries that imposed a DST with whom the United States reached an interim agreement, and any payments made under the UK DST can be accredited upon implementation of the OECD Pillar 1 solution.[699]

Threats to Encryption and Security of Devices

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.[700] The UK also recently joined the United States and Australia in a concerning request to Facebook regarding undermining the security of user communications.[701]

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.[702] 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.[703]

Restrictions on Cross-Border Data Flows

On March 8, 2023, the Secretary of State for Science, Innovation and Technology introduced the Data Protection and Digital Information (No. 2) Bill to Parliament.[704] The new proposal will

---

[698] https://techcrunch.com/2023/09/21/meredith-whittaker-reaffirms-that-signal-would-leave-u-k-if-forced-by-privacy-bill/.

[699] https://home.treasury.gov/news/press-releases/jy0419

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

[701] 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/.

[702] *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/.

[703] *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.

[704] https://bills.parliament.uk/bills/3430.

increase fines for nuisance calls and texts, reduce the amount of consent pop-ups, and reorganize the Information Commissioner's Office, among other new provisions.[705] It will also use existing transfer mechanisms, so if a company is compliant with current U.K. data laws or the GDPR, the company will continue to be compliant with the new U.K. law. This reform bill was co-designed with business from the start and is meant to be easier to understand and easier to comply with than the "barrier-based European GDPR." The Bill is currently in the Report stage of the House of Commons, though a final date has yet to be announced.

Regulation of Digital Markets

On April 3, 2023, Ofcom released a market study of the largest providers of cloud services and also a proposal to refer the UK Cloud services market to the Competition and Markets Authority (CMA) for investigation.[706] Ofcom published its final report, including referring a market investigation to the CMA with a focus on two U.S. companies, on October 5, 2023.[707] The CMA put forward its framework for its investigation on October 17, 2023, and said it would hold a consultation for public feedback until November 9, 2023, with a final conclusion estimated for April 2025.[708]

On April 25th, 2023, the Department for Business and Trade introduced the Digital Markets, Competition and Consumers Bill. [709] The bill includes some specific changes to consumer protection laws (e.g., new rules around subscription services) but it also creates a new competition law framework for digital companies that the Competition and Markets Authority (CMA, and its new Digital Markets Unit) designate as having "strategic market status" (SMS). This is expected to mean that a relatively small set of firms, overwhelmingly U.S. headquartered initially, will be subject to a much more intrusive competition law regime than the wider economy. The resulting interventions include firm-specific codes of conduct, which can include: regulation of prices and other commercial terms allowing CMA to create transfers to domestic vested interests (including a final offer mechanism similar to the Australian news media bargaining code, but not limited by sector); requiring interoperability and data sharing; which services will be offered to consumers and how and when (e.g. choice screens) and restrictions in other areas such as how complaints are handled and how data is used. The bill also allows for pro-competition interventions (PCIs) that would function similarly to existing market investigations, but are intended to move faster for those SMS firms. These powers would be backed up with large potential fines (up to 10% of global turnover) and novel investigatory powers (e.g., being able to require firms conduct experimental changes in their services). The potential for firms to challenge CMA decisions would be constrained with a shift from full-merits appeal to the Competition Appeals Tribunal to judicial review only and while, in

---

[705] https://iapp.org/news/a/uk-introduces-draft-data-protection-reform/.

[706] https://www.ofcom.org.uk/consultations-and-statements/category-2/cloud-services-market-study; https://www.lexology.com/library/detail.aspx?g=74dffdfd-b065-4faa-9da9-e86b2d757047; https://www.ofcom.org.uk/consultations-and-statements/category-2/cloud-infrastructure-market-investigation-reference.

[707] https://www.ofcom.org.uk/news-centre/2023/ofcom-refers-uk-cloud-market-to-cma-for-investigation.

[708] https://www.gov.uk/government/news/cma-outlines-scope-of-market-investigation-into-cloud-services.

[709] https://bills.parliament.uk/bills/3453; https://www.mayerbrown.com/en/perspectives-events/publications/2023/05/the-uk-digital-markets-competition-and-consumers-bill-major-reform-of-cma-powers.

principle, the new law allows for a consideration of consumer benefits, this will be limited in important ways (e.g., countervailing consumer benefits being used as a defence after a finding that a code of conduct has been breached, versus at the outset). The bill is in the Report stage in the House of Commons, and it is anticipated that the bill could receive the Royal Assent by Spring 2024.

UU. 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, a key vehicle for localization, took effect January 1, 2019, and implementation continues through a range of related decrees. The law is expansive and includes data localization mandates, local presence requirements, and content regulations. Under the law and subsequent decrees, 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 August 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.[710] CCIA appreciates USTR citing the problematic nature of the Decree in the 2023 NTE Report.[711] The Decree was issued without Vietnam conducting any consultation regarding the final drafts, which were kept confidential by the government, contravening obligations Vietnam undertook in CP-TPP at Article 14.13. The Decree is unclear regarding the scope of localization requirements for domestic and foreign companies; fails to delineate between domestic companies and Vietnamese companies (rendering foreign companies forced to incorporate locally); lacks clarity regarding whether all data sets need to be kept in Vietnam or whether a copy suffices; and includes unclear obligations with respect to local presence and data processing.[712] The Law on Cybersecurity appears to be in conflict with the Location of Computing Facilities (Article 14.13) and Local Presence (Article 10.6) provisions of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("CPTPP")—implicating the many U.S. companies that are incorporated in CPTPP member countries and that do business in Vietnam. Although Vietnam negotiated a five-year moratorium on dispute settlement in CPTPP with respect to cybersecurity measures, this moratorium expires in January 2024.[713] Vietnam remains legally bound by these obligations, even during the moratorium on dispute settlement.

---

[710] 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.

[711] https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf.

[712] 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.

[713] Id.

The Vietnamese government finalized its Personal Data Protection Decree (PDP), which was issued as Decree No. 13/2023/ND-CP in April 2023 and is went into effect on July 1, 2023.[714] The Decree prescribes de facto data localization conditions including maintenance of extensive records relating to each individual data transfer and 'registration' of transfer of 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. CCIA appreciates USTR detailing the PDP as a barrier in its 2023 National Trade Estimates Report, where it noted that "[m]any of these requirements appear infeasible for companies seeking to supply services in Vietnam on a cross-border basis" since most services require data transfers. Given the broad number of service sectors where Vietnam took on full national treatment obligations for cross-border services as part of its accession to the WTO, these restrictions raise serious compliance issues.

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 the government. It also establishes procedures for the service provider to both terminate access for a user posting "prohibited" content and share information regarding the user (information service suppliers may not have, if data is encrypted). "Prohibited" content is vaguely defined as any content that is critical or disparaging of the Vietnamese government. Companies have already been fined under this provision.[715]

Besides regulatory roadblocks, U.S. companies face challenges from technical intervention, at the behest of the government, 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.

The Authority of Broadcasting and Electronic Information issued a regulation (Decree 6) that regulates video on-demand services in the same manner as broadcast television,[716] departing from global norms on video on-demand regulations. The draft, which came into effect in January 2023, 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

---

[714] https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx; https://www.lexology.com/library/detail.aspx?g=678126ac-2536-4947-91a5-7328d8764309; https://www.lexology.com/library/detail.aspx?g=cc6cccb6-f317-4d54-963b-babaf71db4b1.

[715] *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/.

[716] https://www.tilleke.com/insights/new-decree-will-impact-over-the-top-tv-services-and-on-demand-content-in-vietnam/; https://vanban123.vn/Nghi-dinh/Decree-No-71-2022-ND-CP-dated-October-01-2022-on-amendments-to-some-articles-of-government-s-Decree-No-06-2016-ND-CP-on-management-provision-and-use-of-radio-and-television-services-585839/.

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

Vietnam issued of Decree 71 in October 2022,[717] continuing Vietnam's long-running effort to regulate internet-enabled subscription video services, particularly those provided on a cross-border basis. It remains unclear whether wholly-owned foreign firms can supply such services and many popular foreign services have entered into partnerships with Vietnamese ISPs. This decree also limits foreign-controlled advertising on such services.

In July 2023, the Vietnamese government published a new draft of amendments to the Ministry of Information and Communication Decree 72/2013 first put forward in July 2021.[718] Per the proposed rules, all foreign enterprises providing cross-border services with over 100,000 Vietnamese unique visitor access per month must collect and store a wide range of data of Vietnamese users. This data can then can be demanded by local authorities upon written request. These cross-border services suppliers are also obligated to monitor and remove information and services deemed illegal and to respond to takedown demands of the Ministry of Information and Communications ("MIC") and work to prevent such content. Companies lack guidance on how to achieve these goals or conduct such scanning of content at issue. The content-related obligations to prevent violations of domestic laws and policies online are onerous and sweeping, especially in light of the broad definitions of what prohibited acts could entail. In addition, digital platforms, including cross-border providers, are required to take down illegal content within 24-hours once notified by MIC and a deadline of 48 hours to temporarily block content following user complaints. The Decree includes concerning and poorly-defined obligations for online platforms that involve the online services suppliers entering into cooperation agreements with Vietnamese press agencies regarding information that cites from content produced by these news publishers.

Further, the Decree requires all apps offered on app stores to be licensed, while also mandating that online, multi-player, and interactive game providers must secure licenses for publication in Vietnam. The processes associated with this licensing process are onerous, particularly for foreign companies, as it effectively mandates foreign suppliers to work through local publishers. A public consultation closed on September 15, 2023. CCIA appreciated USTR citing a past iteration of Decree 72 in its 2023 National Trade Estimates Report, where the agency noted that the regulation would "impose burdensome, impractical, or technically infeasible requirements on a wide range of suppliers of Internet services and content providers."

[717] https://vanban123.vn/Nghi-dinh/Decree-No-71-2022-ND-CP-dated-October-01-2022-on-amendments-to-some-articles-of-government-s-Decree-No-06-2016-ND-CP-on-management-provision-and-use-of-radio-and-television-services-585839/.

[718] https://www.lexology.com/library/detail.aspx?g=df9e2ee7-3b01-48b2-82a0-3eb3ad6057b4; https://www.lexology.com/library/detail.aspx?g=1d0af706-6b52-4c9b-b5a5-1d1577a4b343.

Additional Restrictions on E-Commerce

On September 25, 2021, the government issued Decree 85 on E-commerce,[719] 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 requires local and cross-border e-commerce platforms to provide vendors' information to authorities upon request and remove, within 24 hours, marketing for goods that violate Vietnamese laws. The law also includes social media services providers for promotional and other sales-adjacent operations. The Decree came into effect on 1 January 2022.

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.[720] 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 which include a local cloud standard and cloud framework, respectively, and set forward cloud technical and national infrastructure standards and considerations for state agencies and smart cities projects which offer preferential treatment to local private cloud providers.[721] These decisions aim to create a preferential framework for domestic cloud service providers, which would be inconsistent with Vietnam's government procurement obligations under CPTPP. The MIC Minister has stated a desire for Vietnamese firms to attain a stronger hold in cloud computing and digitalization infrastructure, comparable to what they have with facilities-based telecommunications networks.[722] While the 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.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

The Vietnamese Ministry of Information and Communications has proposed the Draft Law on Telecommunications to replace the current telecommunications law for the digital age with several iterations emerging from Oct. 22, 2022, to June 2023.[723] The bill would expand dozens

---

[719] https://kpmg.com/us/en/home/insights/2021/10/tnf-vietnam-taxation-ecommerce-digital-based-transactions.html; https://www.vietnam-briefing.com/news/vietnams-passes-regulation-e-commerce-decree-85.html/.

[721] *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.

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

[723] https://www.connectontech.com/vietnam-new-draft-telecoms-law-regulating-ott-communication-and-cloud-services/.

of existing regulations to include over-the-top (OTT) communications services and cloud services providers. In doing so, the legislation would classify OTT communications providers as telecommunications services and subsequently require them to enter into paid contracts with Vietnamese telecommunications providers to offer service in the country, though the specific structure required of this relationship is not yet clear.

Recent drafts have replaced mandatory paid contracts with a requirement to notify the Vietnamese government of market presence which reflects progress worthy of cautious optimism. However, the process has lacked transparency and such obligations have not been definitively dismissed. If Vietnam were to follow through with the prior draft which requires OTTs to form commercial agreements with telecommunications providers and to establish a representative office, the draft bill would impose unnecessary and unduly burdensome requirements for foreign providers. Vietnam could as a result run afoul of its commitments in the CPTPP, which generally bans local presence requirements. Additionally, this mandatory framework would likely give licensed operators significant leverage in demanding anticompetitive concessions that are clearly unnecessary because Vietnamese consumers are currently able to access a wide array of high-quality digital services with ease, suggesting that there is no market failure in need of remedying. Moreover, requiring commercial agreements could negatively impact consumer choice, as many providers may be unable to negotiate such agreements and choose to pre-emptively exit the market. This scenario would subsequently reduce the value of the internet to consumers and would in turn hurt network operators, as demand for online content drives demand for broadband access.

Requiring platforms to have a local representative office would impose significant costs and thus serve as a barrier for services to access the market. As long as there is a contact channel among companies and regulators to address regulatory concerns, the requirement of a local representative is not necessary. Since many OTT services (e.g., e-mail) are covered by Vietnam's WTO commitments, requiring a local presence could also be viewed as inconsistent with national treatment obligations governing specifically-listed cross-border value-added services.

The draft contains several other concerning provisions for U.S. digital exporters even beyond OTT messaging services as the definition of OTT could scope in services with a central function of processing, sending, transmitting, and receiving information through a telecommunications network. This could effectively include every conceivable internet-enabled service.

Various iterations of the Draft Telecommunications Bill have included onerous provisions regarding cloud services, although, recent drafts of these rules have loosened some of these requirements to be friendlier to industry and investment. However, lack of transparency in the drafting process and a history of burdensome and protectionist proposals means that vigilance remains warranted. Problematic provisions remain. Cloud computing customers are granted new rights to specify the telecommunications supplier that a cloud supplier uses. Cloud services providers are also subject to vague requirements to remove data deemed illegal by the Vietnamese government, which would impinge on both abilities to operate as well as privacy and the freedom of expression of users.

Taxation of Digital Products and Services

The Tax Administration Law, effective July 1, 2020, taxes cross-border e-commerce and other digital services.[724] The Ministry of Finance issued Circular 80 providing guidance on Law on Tax Administration and its Decree 126 in September 2021.[725] 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 allows digital suppliers to seek exemptions under bilateral tax treaties but the process for obtaining such benefits remains unclear. 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 ("GCC") 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 that 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.

Industry reports delays and inconsistent application of implementation of the regulations and approvals conferred by the GCC. These onerous obligations and the subsequent follow-ups restrict companies invested in Vietnam from importing essential hardware. Circular 23/2022/TT-BQP of Ministry of Defense,[726] applicable for cryptographic certification requirement, was passed in 2022, but industry reports that the Vietnamese government has not completed an enforcement mechanism. The lack of certainty surrounding this regime brings extra obstacles to importers unsure of what to expect when the regulation enters into force.

---

[724] *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/.

[725] *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.

[726] MINISTRY OF NATIONAL DEFENSE OF VIETNAM, Circular 23/2022, available at https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Circular-23-2022-TT-BQP-regulation-on-technical-specification-in-civil-cryptography-products/533307/tieng-anh.aspx.

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—both for digital and non-digital services—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.