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

In re Request for Comments on Significant Foreign Trade Barriers for the 2026 National Trade Estimate Report	Docket No. USTR–2025–0016

COMMENTS OF

THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

REGARDING FOREIGN TRADE BARRIERS TO U.S. EXPORTS

FOR 2026 REPORTING

October 29, 2025

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 90 Fed. Reg. 44,448 (Sept. 15, 2025),[1] 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.[2] 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. CCIA welcomes the opportunity to document various regulations and policy frameworks that serve as market access barriers for internet services.

CCIA welcomes USTR's renewed attention to digital trade barriers as a core element of its mission, and its focus in vigorously enforcing existing commitments designed to address such barriers. The internet remains an integral component of international trade in both goods and services, and 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 US$282 billion for the United States in 2024.[3]

However, U.S. strategic trade and technology interests face growing threats from countries that continue to adopt discriminatory or unbalanced regulations, or regulations designed primarily to extract value from cross-border suppliers and thus undermine market access for internet-enabled products and services. For the 2026 NTE, CCIA has identified significant barriers to trade facing U.S. digital services exporters in the following areas: (1) asymmetric platform regulation; (2) customs-related restrictions and import barriers for goods; (3) barriers to the deployment and operation of network infrastructure; (4) data and infrastructure localization mandates and restrictions on cloud services, (5) discriminatory local content quotas and audiovisual services mandates, (6) forced revenue transfers for digital news, (7) government-imposed restrictions on internet content and related access barriers, (8) imposing legacy telecommunications rules on internet-enabled services, (9) potential challenges to the development of AI, (10) restrictions on

[1] U.S. Trade Representative, (2025, September 15), *Request for Comments on Significant Foreign Trade Barriers for the 2026 National Trade Estimate Report,* Federal Register, https://www.federalregister.gov/documents/2025/09/15/2025-17782/request-for-comments-on-significant-foreign-trade-barriers-for-the-2026-national-trade-estimate.
[2] For more, visit www.ccianet.org.
[3] U.S. Bureau of Economic Analysis, (2025, July 3), *U.S. Trade in ICT Services and Digitally Deliverable Services, by Country or Affiliation*, BEA Data, https://apps.bea.gov/iTable/?reqid=62&step=6&isuri=1&tablelist=359&product=4.

cross-border data flows, (11) taxation on digital products and services, and (12) threats to the security of devices and services.

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 now represents a significant portion of the global economy, and failure to keep it open threatens the prosperity of all.

The real gross output of the digital economy in the U.S. grew at an annual rate of 7.1% between 2018 and 2022, much faster than the overall economy's growth rate of 2.2% over the same period.[4] According to U.S. Department of Commerce, the digital economy generated $2.6 trillion of value added to U.S. GDP, or 10% of total U.S. GDP, in 2022.[5] The digital economy accounted for 8.9 million jobs that same year, which generated $1.3 trillion in total compensation, with the average annual wage consistently increasing from 2006 ($85,595) to 2021 ($154,427). Digital trade specifically supported 3 million jobs in the United States in 2022.[6] U.S. companies generated $729.7 billion in digitally-deliverable services exports globally in 2024, with a trade surplus of $282 billion.[7] Digitally-deliverable services are an essential part of U.S. export strength, as they represented 66% of all U.S. services exports in 2024. 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 most of the overall services trade reflects its importance to U.S. economic strength, competitiveness, and national interests.[8] The surge in investment in AI over the past several years, with the United States outpacing other countries, further cements the critical importance of the digital ecosystem to the broader economy. Private investment in AI in the United States increased 50% between 2023 and 2024, reaching over $150 billion.[9]

---

[4] Highfill, T. & Surfield, C., (2022), *New and Revised Statistics of the U.S. Digital Economy, 2005–2021,* U.S. Bureau of Economic Analysis, https://www.bea.gov/sites/default/files/2022-11/new-and-revised-statistics-of-the-us-digital-economy-2005-2021.pdf.

[5] U.S. Bureau of Economic Analysis, (2023), *How Big is the Digital Economy,* https://www.bea.gov/sites/default/files/2023-12/digital-economy-infographic-2022.pdf.

[6] Heiber, J. G. & Isco, I., (2024, March 19), *How Digital Trade Benefits the American Economy,* U.S. Chamber, https://www.uschamber.com/international/trade-agreements/how-digital-trade-benefits-the-american-economy.

[7] U.S. Bureau of Economic Analysis, (2025, July 3), *U.S. Trade in ICT Services and Digitally Deliverable Services, by Country or Affiliation,* BEA Data, https://apps.bea.gov/iTable/?reqid=62&step=6&isuri=1&tablelist=359&product=4.

[8] Nasr, A, (2024, July 11), New Government Data Shows Digital Services Exports Continue to Drive U.S. Trade, *Disruptive Competition Project,* https://project-disco.org/21st-century-trade/new-government-data-shows-digital-services-exports-continue-to-drive-u-s-trade/.

[9] Stanford University Human-Centered Artificial Intelligence, (2025), *2025 AI Index Report, Economy,* https://hai.stanford.edu/ai-index/2025-ai-index-report/economy.

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. For transformative technologies like AI, access to these markets is critical to achieving scale and recouping the substantial investments required for development. By focusing on policies to promote export of the AI stack, the Administration has recognized these needs and opportunities.[10] However, U.S. businesses face growing obstacles to reach these markets, and these changing dynamics are not only driven by competitive market forces. Countries recognize the immense value that a robust digital industry contributes to the national economy, and with the predominance of U.S. companies in this sector, governments are increasingly adopting policies designed to favor domestic innovation and specifically target U.S. companies, ushering in a new form of discrimination. The increasing spread of barriers to digital trade makes this a tangible threat in need of vigilance from U.S. trade policy leaders. According to a recent report from the OECD, barriers to digitally-enabled services increased by 25% globally between 2014 and 2023, a trend "driven by increasing regulatory hurdles that affected communication infrastructures and data connectivity."[11] As such, USTR's continued leadership and engagement on proposed and enacted barriers is vital to U.S. economic interests.

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. Asymmetric 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. This trend raises significant concerns that an untested policy is spreading before its effects, both intended and unintended, have been adequately evaluated. In many cases, platform regulation serves as a backdoor for industrial policy explicitly designed to advantage local competitors, dressed up as competition policy, employing thresholds designed specifically to ensure that leading U.S. internet services are the exclusive or predominant target of the regulations. Such rules are often tailored to specifically impede the legitimate business models of U.S. companies, including their administration of app stores and their treatment of their own products and services relative to those of competitors. In all instances, policymakers struggle to separate pro-competitive conduct from the hypothetical harms they seek to regulate. The effectiveness of such proposals in

[10] White House, (2025, July 23), *Promoting the Export of the American AI Technology Stack,* https://www.whitehouse.gov/presidential-actions/2025/07/promoting-the-export-of-the-american-ai-technology-stack/.
[11] Organization for Economic Cooperation and Development, (2024, June 24), *Revitalising Services Trade for Global Growth,* https://www.oecd-ilibrary.org/trade/revitalising-services-trade-for-global-growth_3cc371ac-en.

promoting innovation in the tech sector is highly questionable.[12] 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 gloss over the discriminatory nature of their measures. While these prescriptive laws state that they seek to promote competitive digital markets, countries contemplating such rules should consider the potential adverse consequences that raise prices, impede innovation, and limit choice for consumers and small businesses.

B. Customs-Related Restrictions and Import Barriers for Goods

U.S. goods exporters face an array of customs-related barriers, impacting e-commerce and the export of inputs for digital infrastructure such as data centers. Common measures include arbitrary caps and low or uncertain *de minimis* thresholds for express shipments; opaque import licensing and quota schemes for ICT and other goods; and preshipment inspection mandates tied to select HS codes that add per-shipment fees and delay clearance. The cumulative effect is longer wait times at borders, higher working-capital needs, greater inventory risk, and increased uncertainty that disproportionately burdens new entrants and small U.S. exporters. These policies operate as non-tariff barriers that risk conflicting with best practices in the WTO Trade Facilitation Agreement, and trading partners are encouraged to address these barriers to facilitate e-commerce flows and ICT investment from U.S. firms.

C. Barriers to the Deployment and Operation of Network Infrastructure

The deployment and operation of global network infrastructure, from subsea cables to satellite constellations, is fundamental to the functioning of the modern internet, enabling cross-border service delivery. Yet in many jurisdictions, this infrastructure faces market access barriers that collectively discourage foreign investment, slow the rollout of innovative technologies, and limit access to affordable, high-quality digital infrastructure worldwide.

Subsea cables carry more than 95% of global internet, voice, and data traffic, account for more than US$10 trillion in economic activity annually, and significantly lower the costs of connectivity.[13] While U.S. hyperscalers are investing tens of billions of dollars to maintain and

[12] MacCarthy, M., (2019, October 22), To Regulate Digital Platforms, Focus on Specific Business Sectors, *Brookings Institution*, https://www.brookings.edu/blog/techtank/2019/10/22/to-regulate-digital-platformsfocus-on-specific-business-sectors/.

[13] Mauldin, A., (2023, May 4), Do Submarine Cables Account for Over 99% of Intercontinental Data Traffic? *Telegeography,* https://blog.telegeography.com/2023-mythbusting-part-3; Cariolle, J., Houngbonon, G.V., Silue T., & Strusani, D., (2024), The Impact of Submarine Cables on Internet Access Price, and the Role of Competition and Regulation, *World Bank Group*, https://documents1.worldbank.org/curated/en/099223207092441042/pdf/IDU1cabee90a10d73147681a3421d7461517cbab.pdf; Gallagher, (2024, October), *Hidden Dangers: Undersea Cables and Mitigating Economic Risk,* https://www.ajg.com/news-and-insights/features/hidden-dangers-undersea-cables-and-mitigating-economic-risk/; Mauldin, A., (2022, April 26), TeleGeography predicts $10bn worth of new subsea cables by 2024, *Capacity Global*, https://capacityglobal.com/news/telegeography-predicts-10n-worth-of-new-subsea-cables-by-2024/.

expand such networks to connect their global data centers,[14] they face impediments to cable laying and repair. Requirements to use narrowly-designated landing sites and routes through territorial waters or to partner with domestic firms impose unnecessary costs and limit providers' flexibility to optimize networks; and protectionist measures such as cabotage rules, multi-ministry approvals, and punitive customs interpretations, such as taxing repair vessels as imports, delay critical maintenance and raise costs. Given the critical role that submarine cables play in supporting the global digital economy, U.S. trading partners should ensure that submarine cable operators can freely choose suppliers for installation, maintenance, and repair services, including from foreign providers, while guaranteeing that any permitting requirements are transparent, objective, and non-discriminatory.

Driven by rapid advances in satellite technology, massive private investment, and growing demand for universal connectivity, low Earth orbit (LEO) constellations are expanding at an unprecedented pace, helping fuel a global SATCOM market expected to generate annual revenues of US$40 billion by 2030 and contributing to a projected US$1.8 trillion space economy.[15] However, extensive and highly variable licensing and regulatory regimes, coupled with long-term investment risks and compliance costs, continue to create substantial market access barriers for LEO broadband providers. Requirements to incorporate locally, source infrastructure domestically, or localize data centers and DNS resolution impose heavy operational burdens and effectively exclude many foreign providers. Other measures, such as denying interference protections to new entrants, requiring emergency shutdown capabilities, or mandating content decryption within national borders, create legal and technical risks that disincentivize deployment. In some cases, proposed space laws and licensing regimes explicitly favor domestic satellite operators or domestically headquartered providers, while subjecting foreign constellations to onerous registration and compliance requirements designed to capture only U.S. systems. Collectively, these measures undermine market access, fragment global networks, and threaten the scalability of satellite-based services. As demand for resilient, low-latency global connectivity grows, ensuring fair, transparent, and non-discriminatory conditions for the deployment and operation of digital infrastructure will be critical to sustaining digital trade and economic growth.

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

A growing number of governments are imposing data localization mandates, including requirements for local data storage, infrastructure, and corporate presence, that create significant

[14] Jacques, R., (2023, October 26), Interview: Orange Wholesale Chief Says Hyperscalers, Cloud, AI Fundamentally Changing Subsea Cable, *TelcoTitans*, https://www.telcotitans.com/7371.article.
[15] International Telecommunications Union, (2025, February 11), *Space Connect: The rise of LEO satellite constellations,* https://www.itu.int/hub/2025/02/space-connect-the-rise-of-leo-satellite-constellations/; Young, M. & Thadani, A., (2022), *Low Orbit, High Stakes: All-In on the LEO Broadband Competition*, Center for Strategic & International Studies, https://www.csis.org/analysis/low-orbit-high-stakes.

barriers to cross-border digital trade. While often justified as necessary for privacy, national security, or law enforcement access, these policies are frequently protectionist in nature, designed to exclude foreign competitors and advance domestic technology sectors under the banner of "digital sovereignty." In practice, forced localization undermines rather than strengthens security by concentrating sensitive data in a single jurisdiction, creating attractive targets for cybercriminals and foreign intelligence agencies, and weakening international cooperation on law enforcement and cybersecurity.[16] Localization also carries significant economic costs, reducing trade volumes, increasing compliance burdens, and raising prices for consumers while failing to stimulate domestic innovation.[17] Moreover, these requirements themselves erode one of the United States' key strategic advantages, its global leadership in data processing and cloud infrastructure.[18] By forcing data processing capacity abroad, these measures undercut U.S. workers and weaken a sector that underpins global commerce. Finally, localization mandates often fail to comply with countries' WTO obligations applicable to underlying services, as they are often vague, discriminatorily applied, and not demonstrably necessary to achieve legitimate policy goals.

Beyond direct localization mandates, governments are increasingly adopting regulations that disadvantage foreign cloud service providers and restrict their ability to compete. These include certification schemes designed to exclude non-local suppliers, security requirements tailored to domestic firms, restrictions on VPN use, and rules mandating access to encrypted data or government interception capabilities. Some jurisdictions, such as the EU, Korea and Canda have proposed building exclusive cloud infrastructure to keep data within their borders, while others, including Indonesia, Mexico, and China, have enacted measures that limit foreign participation through onerous operational, content, or data handling requirements. These policies directly target U.S. companies, who lead in the global cloud services market, supporting billions of

---

[16] Chander, A. & Lê, U.P., (2015), Data Nationalism, *Emory Law Journal, 64*(3), 678-739; Swire, P., (2023), *The Effects of Data Localization on Cybersecurity*, Georgia Tech Scheller College of Business, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4030905; Krishnamurthy, V., (2016), *Cloudy with a Conflict of Laws*, Berkman Klein Center for Internet & Society, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733350.

[17] Cory, N., (2019, April 1), *The False Appeal of Data Nationalism: Why the Value of Data Comes From How It's Used, Not Where It's Stored*, Information Technology & Innovation Foundation, https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where/; Bauer, M., Ferracana, M. F., & van der Marel, E., (2016), *Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization*, Global Commission on Internet Governance, https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf; Bauer, M., Lee-Makiyama, H., van der Marel, E., & Verschelde, B., (2014), *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, European Centre for International Political Economy. https://ecipe.org/publications/dataloc/; Leviathan Security Group, (2015), *Quantifying the Cost of Forced Localization*, https://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization; Cory, N., Dascoli, L. & Clay, I., (2022), *The Costs of Data Localization Policies in Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam*, Information Technology & Innovation Foundation, https://itif.org/publications/2022/12/12/the-cost-of-data-localization-policies-in-bangladesh-hong-kong-indonesia-pakistan-and-vietnam/; Brehmer, H. J., (2018), Data Localization The Unintended Consequences of Privacy Litigation, *American University Law Review 67*(3), 927-969.

[18] Statista, (2025, March 21), *Leading countries by number of data centers as of March 2025*, https://www.statista.com/statistics/1228433/data-centers-worldwide-by-country.

dollars in economic activity and thousands of high-paying U.S. jobs.[19] By raising compliance costs, fragmenting digital markets, and undermining the scalability and efficiency of cloud infrastructure, data localization requirements and related restrictions distort trade, impede innovation, and threaten the open, cross-border flow of digital services that underpins a core U.S. sector.

E. Discriminatory Local Content Quotas and Audiovisual Service Mandates

Some governments are pursuing regulatory frameworks that compel foreign streaming and audio-visual services to finance, distribute, or give preferential treatment to locally produced content. Such measures range from mandatory payments into local promotional funds, investment quotas tied to revenue or production budgets, "discoverability" rules that manipulate recommendation systems, to mandatory "prominence" requirements for domestic broadcasters. They often apply selectively to foreign services, excluding domestic operators or affiliated platforms from equivalent obligations. By forcing streaming services to dedicate a fixed share of revenue to narrowly defined domestic works or requiring them to reorder interfaces to highlight national content, such regimes discriminate against U.S. suppliers and U.S. content and undermine competitive neutrality. They also act as performance requirements prohibited under many trade agreements, compelling companies to structure operations and investments in ways that favor domestic industries regardless of consumer demand or commercial viability. To support sustainable cultural production without distorting digital markets, U.S. trading partners should pursue transparent, non-discriminatory policies that incentivize voluntary investment and international co-production rather than imposing mandatory, nationality-based content requirements.

F. Forced Revenue Transfers for Digital News

A troubling trend is the spread of laws forcing U.S. online platforms to pay news publishers for content the publishers themselves allow or actively place on those platforms. Rather than facilitating or promoting negotiated payment for full articles, a standard commercial practice, these measures demand compensation for mere snippets, headlines, or links. Such policies distort the internet ecosystem, where a rising share of adults now access news via social media,[20] and impose significant costs on service providers. Some countries pursue this through so-called "neighboring rights" or "ancillary copyrights," compelling payments for the "privilege" of quoting news content in violation of trade and IP norms, including TRIPS.[21] Others, like

---

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

[20] Pew Research Center, (2025, September 25), *Social Media and News Fact Sheet*, https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/.

[21] 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* (1979). Moreover, if the function of quotations in this context – driving

Australia, bypass copyright entirely: its 2021 News Media Bargaining Code empowers the government to force platforms to negotiate payments with publishers based on a flawed analysis of the economics of news sharing. Canada followed with the Online News Act, requiring select platforms to pay publishers for any use of their content, even links or brief excerpts, in a law that clearly targets U.S. firms, leading to canceled partnerships, reduced reach for smaller outlets, and diminished user access to information.[22]

The proliferation of these measures poses serious risks for trade, competition, and the free flow of information. Australia and Canada's actions, despite strong free trade commitments with the United States, have emboldened other governments to pursue similar revenue-transfer schemes. If widely adopted, such policies could cost U.S. companies billions of dollars annually simply for indexing or linking to lawful content, or push them to exit news aggregation and indexing altogether, harming publishers and users alike.[23] Previous attempts in Germany, Spain, and France produced sharp declines in traffic and revenue for local media, and increased media concentration, yet new laws continue to advance in Indonesia, New Zealand, Türkiye, and potentially Brazil, where proposals also include restrictions on content moderation. Regulators in the UK, Japan, South Africa, Malaysia, and India are examining comparable initiatives. These discriminatory policies, often based on flawed economic reasoning and narrowly targeted at U.S. firms, risk fragmenting the global internet, distorting media markets, and effectively subsidizing foreign publishers at the expense of U.S. digital services.

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

Government-imposed censorship, filtering, and outright shutdowns remain among the most severe barriers to cross-border digital trade. Around the world, governments continue to block access to foreign platforms, throttle services, and suppress online speech, often under the pretext of safeguarding public order or national security. Between June 2023 and May 2024, more than half of the global online population experienced temporary or permanent restrictions on social

---

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.

[22] Kahn, G., (2023, November 7), In Canada's Battle with Big Tech, Smaller Publishers are Caught in the Crossfire, *Reuters Institute*, https://reutersinstitute.politics.ox.ac.uk/news/canadas-battle-big-tech-smaller-publishers-are-caughtcrossfire.

[23] United States International Trade Commission, (2017), *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, https://www.usitc.gov/publications/332/pub4716.pdf; CCIA, (2024, May 14), *Link Tax Failures: Global Efforts Continue to Uproot the Internet's Foundation and Journalism Ecosystem*, https://ccianet.org/library/link-tax-failures-global-efforts-continue-to-uproot-internets-foundation-and-journalism-ecosystem/.

media platforms, and at least 25 countries systematically blocked messaging or social media services, frequently in response to protests or political unrest.[24] Such actions are increasingly common in both authoritarian and democratic states. These disruptions are not only repressive but economically damaging: Access Now recorded 296 shutdowns in 51 countries in 2024,[25] while studies have found that shutdowns cost economies almost US$8 billion in 2024, and inflicted cascading harms on content creators, advertisers, and SMEs that depend on online platforms to reach customers.[26] National firewalls and state-controlled network gateways further disadvantage foreign services by degrading their performance relative to domestic competitors, if not outright blocking access. These practices often violate countries' WTO obligations, including GATS commitments on market access, national treatment, transparency, and due process, particularly when they are applied in opaque, discriminatory, and non-necessity-based ways.

In parallel with these overt forms of censorship, governments are enacting unbalanced and trade-distorting content regulations that impose significant compliance burdens on foreign service providers and interfere with their ability to operate across borders. The erosion or absence of clear and predictable intermediary liability protections, long a cornerstone of the modern internet, further compounds these challenges. Safe harbor frameworks, such as those enshrined in U.S. law under 17 U.S.C. § 512, enable platforms to host user-generated content and scale services globally without facing disproportionate legal risk for user activity. Yet many jurisdictions either fail to adopt comparable protections or apply them in unduly narrow and discriminatory ways, excluding commercial platforms from coverage or imposing onerous monitoring, filtering, or takedown obligations that exceed international norms. This fragmentation creates significant legal uncertainty, deters foreign investment, and forces companies to choose between costly compliance, market exit, or the risk of civil and criminal liability. While some measures aim to address illegal or harmful content, many go far beyond what is necessary, requiring companies to remove lawful speech based on vague definitions of harm, disclose proprietary algorithms, or compromise encryption through traceability mandates. Others compel the appointment of local employees subject to criminal liability or mandate preferential treatment for domestic services. Trade policy should therefore prioritize the establishment of proportionate liability frameworks rooted in due process and minimal restrictiveness, ensuring that content-related obligations are applied equally to domestic and foreign services and that they comply with international trade commitments.

---

[24] Freedom House. (2024). *Freedom on the Net 2024*. https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf; Skeadas, T., Mirza, R., & Vishwanath, M. (2023). *Digital Disruption: Measuring the Social and Economic Costs of Internet Shutdowns & Throttling of Access to Twitter*. Tech Policy Press. https://www.techpolicy.press/digital-disruption-measuring-the-social-and-economic-costs-of-internet-shutdowns-throttling-of-access-to-twitter/; Surfshark. (n.d.). *Internet shutdown tracker*. https://surfshark.com/research/internet-censorship.

[25] Access Now. (n.d.). *Shutdown Tracker Optimization Project (STOP) Dashboard v.1*. https://www.accessnow.org/keepiton-data-dashboard/.

[26] Migliano, S. (2025, January 2). *Government Internet Shutdowns Cost $7.69 Billion in 2024*. Top10 VPN. https://www.top10vpn.com/research/cost-of-internet-shutdowns/.

H. Imposing Legacy Telecommunications Rules on Internet-Enabled Services

Some foreign jurisdictions are seeking to apply outdated telecommunications-era rules to modern internet-enabled services, creating significant barriers to U.S. digital services. One prominent example is the rise of "sender-pays" or "network usage fee" proposals, which force online content and application providers (CAPs) to pay internet service providers (ISPs) for the traffic that end users themselves request. Originally justified as a means of offsetting network costs, these proposals ignore both the economic realities of network operations, where traffic growth remains manageable and ISP costs largely stable, and the internet's foundational principle that users pay their own access provider for connectivity.[27] South Korea's long-standing sender-pays regime illustrates the harm such policies cause: they lead to poorer network performance, increased latency, higher bandwidth costs and reduced investment in local infrastructure, as CAPs relocate services abroad to avoid punitive charges.[28] Similar proposals are now under discussion in the EU, Australia, Brazil, and the Caribbean, with some governments using arbitrary traffic thresholds to target large U.S. providers. Such mandates effectively tax U.S. digital exports to subsidize domestic ISPs, distort competition, and disincentivize innovation and investment in network efficiency, ultimately raising costs for consumers and weakening the global internet ecosystem.

At the same time, governments are increasingly imposing legacy telecom-style regulatory frameworks on over-the-top (OTT) communications and cloud services, despite the fundamental differences between these services and traditional telecommunications providers. Proposals in markets such as India would subject OTT messaging apps, email services, and other internet-enabled platforms to the same regulatory obligations as network operators, even though OTT providers operate at the application layer and rely on, but do not manage, the underlying network infrastructure. This approach threatens to upend the open architecture of the internet by imposing licensing requirements, compliance obligations, and other regulatory burdens designed for monopolistic, infrastructure-based industries onto competitive, service-layer providers.

By blurring the distinction between networks and services and importing outdated regulatory models into the digital economy, these policies undermine the conditions that enabled the internet's growth and present a growing obstacle to U.S. services exports.

I. Potential Challenges to the Development of AI

AI is poised to transform global trade by lowering costs, boosting productivity, and significantly expanding U.S. digital services exports. The WTO predicts that AI could, if supported by the

[27] Abecassis, D., Kende, M., & Osman, S. (2022), *The impact of tech companies' network investment on the economics of broadband ISPs*. Analysys Mason. https://www.analysysmason.com/consulting/reports/internet-content-application-providers-infrastructure-investment-2022/.
[28] Wagener, T. (2023). *Myths Surrounding Network Usage Fees: South Korea.* CCIA. https://ccianet.org/wp-content/uploads/2023/11/CCIA_Myths-Surrounding-Network-Usage-Fees-South-Korea.pdf.

right policies, help expand trade by up to 37% and increase global GDP by 13% by 2040.[29] An emerging trend that warrants close attention is the potential proliferation of AI laws and regulations that would adversely affect investment in or the cross-border supply of AI-enabled services and technologies. Access to vast and diverse datasets, including publicly available information from the open web, is fundamental to developing accurate, secure, and effective AI systems. This access underpins AI innovation by allowing models to learn from billions of data points, identify relationships and patterns, incorporate diverse perspectives, and guard against bias.[30] However, this essential ecosystem is increasingly at risk from restrictive measures that could severely limit the ability to train AI models. Countries such as Brazil are already pursuing proposals that would impose impractical licensing requirements on the use of copyrighted works for AI training, while policy debates in Australia, Canada, Korea, and the UK are also raising fundamental questions about access to online content. Such measures, if enacted, could create significant trade barriers, stifle innovation, and disadvantage developers who operate in line with international norms. Consistent with longstanding U.S. copyright law, U.S. courts correctly continue to find the copying necessary for AI training to be protected by the fair use doctrine. As most other countries do not have this innovation-friendly doctrine, several trade partners are pursuing legislation to create explicit safe-harbors in copyright, including text and data mining exceptions. If the United States is to succeed in its ambition of promoting the export of AI-enabled products and services, championing fair use should be a priority.

As governments seek to advance regulations with the legitimate aim of promoting safety, they may be tempted to regulate poorly understood functions or features, slow competitive threats, and protect local businesses, either incumbents or new entrants. For U.S. firms, representing leading capabilities in foundational models, basic research, advanced computing, and end-use tools, the risk of discriminatory treatment is significant. Traditional threats to digital trade similarly affect AI, such as restrictions on the cross-border transfer of data, data localization requirements, and onerous transparency requirements that infringe on intellectual property rights and trade secrets. More specific threats to the cross-border supply of AI services include poorly distinguishing obligations between AI developers and deployers; forced disclosure of source code, algorithms, model weights and training data; imbalanced applications of copyright law; identification of risk and imposition of special obligations based on inaccurate risk proxies such as compute thresholds or business scale; and onerous transparency and labeling requirements that conflict with best practices.[31] The U.S. government should bolster its current efforts to build consensus on best practices for governing AI by ensuring that foreign governments do not impose measures that restrict U.S. firms' AI offerings and market access.

---

[29] World Trade Organization. (2025). *World Trade Report 2025: Making trade and AI work together for the benefit of all*. https://www.wto.org/english/news_e/news25_e/wtr_15sep25_e.htm.
[30] Sacks, D [@DavidSacks]. 2025, June 24. *Positive ruling for AI. There must be a fair use concept for training data or models would be crippled. China* [X Post]. X. https://x.com/DavidSacks/status/1937558998166954092.
[31] McHale, J. (2023). *Rules of the Road: Trade Principles for a Competitive Global AI Market*. https://ccianet.org/wpcontent/uploads/2023/11/CCIA_Trade-Principles-Competitive-Global-AI-Market.pdf.

J. Restrictions on Cross-Border Data Flows

The free flow of data across borders is a cornerstone of the global digital economy and essential to growth, innovation, and trade across all sectors. In 2023, digitally deliverable services dependent on cross-border data transfers generated nearly $4.25 trillion worldwide,[32] enabling businesses of all sizes to operate seamlessly across markets. Despite this, many governments continue to impose unclear privacy regimes, onerous transfer conditions, and restrictive export requirements that drive up costs, reduce efficiency, and undermine competitiveness for industries reliant on data flows. The absence of clear and interoperable mechanisms for data transfer, particularly in restrictive data governance regimes, further disadvantages the ability of foreign digital firms to operate effectively in these markets. Such rules not only distort competition but can also lower GDP, deter foreign investment, disrupt supply chains, and significantly reduce productivity and export potential, effects that are particularly damaging for local firms dependent on digital tools and services.

K. Taxation of Digital Products and Services

A growing number of jurisdictions have moved forward with unilateral digital services taxes (DSTs) that overwhelmingly target U.S. companies and distort global trade. While a handful of governments, including those in Canada, India, Pakistan, and New Zealand, have recently withdrawn enacted or proposed DSTs, many others continue to advance such measures. In the United Kingdom, France, Spain, and Italy alone, DSTs extracted more than $9 billion from 2020 to 2024, with the overwhelming share of that burden falling on U.S. firms.[33] These measures, often justified by the inaccurate claim that digital service suppliers do not pay sufficient tax, ignore the reality that U.S. firms are taxed in the United States on their global revenues.[34] In practice, DSTs do not address whether a company pays taxes, but, rather, where those taxes are paid; and absent a multilateral agreement, they will inevitably result in harmful double taxation. Many such proposals, including those advanced in the EU and elsewhere, are discriminatory by design, discouraging foreign investment and, in some cases, conflicting with countries' obligations under international tax treaties and trade agreements. Policymakers in Washington, across administrations and parties, have consistently condemned these measures,[35] and the United States should continue to respond forcefully, using all available trade tools, to prevent

---

[32] D'Andrea, B., et al. (2024, April 24). *Thirty years of trade growth and poverty reduction*. World Trade Organization. https://www.wto.org/english/blogs_e/data_blog_e/blog_dta_24apr24_e.htm.
[33] CCIA. (2025, July 8). *Status of Key Digital Services Taxes in July 2025*. https://ccianet.org/library/status-of-key-digital-services-taxes-in-july-2025/.
[34] Bauer, M. (2018). *Digital Companies and Their Fair Share of Taxes: Myths and Misconceptions*. ECIPE. https://ecipe.org/wp-content/uploads/2018/02/ECI_18_OccasionalPaper_Taxing_3_2018_LY08.pdf.
[35] See, e.g., Smith, A., et al. (2024, July 11). [Letter from members of the U.S. Congress to Ambassador Tai regarding Canada's digital services tax]. https://waysandmeans.house.gov/wp-content/uploads/2024/07/7.11.24-Canada-DST-Letter-to-Ambassador-Tai.pdf; Estes, R., et al. (2025, September 15). [Letter from members of the U.S. Congress to President Trump regarding the UK's digital services tax]. https://estes.house.gov/uploadedfiles/uk_dst_letter_to_president_trump_-_final.pdf.

their proliferation and to protect U.S. exporters from being singled out for discriminatory treatment in foreign markets.[36]

While distinct from DSTs, a parallel threat to digital trade comes from efforts by some governments to impose customs duties on electronic transmissions, reversing over two decades of trade-liberalizing practice. Since 1998, WTO members have repeatedly renewed a moratorium prohibiting such duties, a commitment that has underpinned the growth of the digital economy and is now reflected in dozens of bilateral and regional trade agreements. Imposing tariffs or reporting obligations on electronic transmissions would create significant compliance burdens, particularly for SMEs, because data points such as the origin, value, or destination of a transmission are often unknowable, especially for cloud-based services.[37] Although the WTO extended the moratorium through March 2026 and a subset of members committed to longer-term prohibitions under the Joint Statement Initiative,[38] key markets remain outside these commitments and continue to explore tariff measures. With the next Ministerial Conference approaching, the United States should prioritize securing a permanent extension of the moratorium and push back against attempts, by both governments and the World Customs Organization, to incorporate electronic transmissions into tariff schedules.

M. Threats to the Security of Devices and Services

Providers of digital devices and services have long enhanced platform security through technologies that protect communications and transactions. Strong encryption is now standard on smartphones and widely deployed end-to-end across communications services and browsers, safeguarding users' sensitive personal and financial data from malicious actors. Yet many governments, often at the urging of national security and law enforcement agencies, are pursuing or have enacted laws mandating access to encrypted communications. A key example is the UK's 2023 Online Safety Act, which empowers the government to compel digital firms to scan for illegal materials, undermining end-to-end encryption. Such mandates, even when not explicit, often require "technical assistance" or compliance with otherwise infeasible judicial orders. International hostility to encryption is growing.[39] Amendments to the UK's Investigatory Powers Act, for instance, require companies to notify the government before deploying updates that

---

[36] Stelly, R. (2020, July 14). *Comments of the Computer & Communications Industry Association Regarding Section 301 Investigations of Digital Services Taxes*. CCIA. https://ccianet.org/wp-content/uploads/2020/07/Comments-of-CCIA-USTR-2020-0022-Section-301-Digital-Services-Taxes-.pdf.

[37] Andrenelli, A., & Lopez Gonzalez, J. (2019). *Electronic transmissions and international trade – Shedding new light on the Moratorium Debate*. OECD. https://one.oecd.org/document/TAD/TC/WP(2019)19/FINAL/en/pdf; Lee-Makiyama, H. & Gopalakrishnan, B. N. (2019). *The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions*. ECIPE. https://ecipe.org/publications/moratorium/; Cory, N. (2019, March 13). Explainer: Understanding Digital Trade. *Real Clear Policy*. https://www.realclearpolicy.com/articles/2019/03/13/explainer_understanding_digital_trade_111113.html.

[38] WTO. (2024). *Joint Statement Initiative on Electronic Commerce*. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/87.pdf&Open=True.

[39] CCIA. (2019, October 3). *CCIA Dismayed by AG Opposition to Stronger Consumer Encryption Options*. http://www.ccianet.org/2019/10/ccia-dismayed-by-ag-opposition-to-stronger-consumer-encryption-options/.

could affect surveillance capabilities, potentially delaying or blocking critical security patches and hindering innovation.[40] These "exceptional access" regimes run counter to consensus security assessments, as they are often technically or economically unworkable.[41] Companies operating in such jurisdictions may be forced to alter global platforms, design region-specific products, or risk fines, shutdowns, or even criminal liability. Secrecy mandates further prevent companies from sharing information about government demands with employees or customers. Such requirements can deter market entry and, because technology is deployed globally, mandated vulnerabilities risk the security and privacy of users worldwide.

Beyond anti-encryption measures, some governments also require companies to configure app stores in ways that threaten user security and privacy, for example, mandating that phones sold domestically come with pre-installed, government-approved apps; or mandate providing consumers access to unverified apps offered by competing app stores. Similarly, mandatory interoperability requirements that some governments pursue in the name of competition promotion can hinder device makers' ability to protect users against privacy breaches or malicious actors.

III. COUNTRY-SPECIFIC CONCERNS

Argentina

Customs-Related Restrictions and Import Barriers for Goods

Argentina's Impuesto PAIS, a 30% surcharge on foreign currency purchases and imports of services, expired on December 23, 2024.[42] The decree had imposed 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 meant that a single import could result in an additional tax of up to 15% simply because its purchase and transport were funded through U.S. dollars, putting U.S. suppliers at a distinct disadvantage. Despite the Impuesto PAIS' expiration, the Customs Collection and Control Agency (ARCA) subsequently issued General Resolution No. 5617/24 on

[40] Schonfeld, S. (2024, February 26). [Letter from privacy experts to UK Home Secretary]. https://www.globalencryption.org/2024/02/experts-letter-on-investigatory-powers-act-amendment/; Internet Society & Access Now. (2024, March 7). *Investigatory Powers (Amendment) Bill: Written Evidence*. https://www.internetsociety.org/wp-content/uploads/2024/03/ISOC_ISOC-UK_Access-Now-submission-IPAB.pdf; Baker, J. & Salgado, R. (2024, January 19). *Surveillance-by-Design in Proposed Amendments to the U.K. Investigatory Powers Act*. Lawfare. https://www.lawfaremedia.org/article/surveillance-by-design-in-proposedamendments-to-the-u.k.-investigatory-powers-act.

[41] Abelson, H. et al. (2015). *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*. MIT. http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[42] ARCA. (n.d.). *Impuesto PAIS*. https://www.afip.gob.ar/impuesto-pais/.

December 19, 2024,[43] maintaining the linked 30% advance payment on income. For registered taxpayers, this amount functions as an advance tax credit recoverable in the next calendar year, but for non-registered foreign suppliers, reimbursement involves a burdensome and lengthy administrative procedure, prolonging the financial impact.

Argentina's customs clearance process is administered through a risk-based "channel system" managed by the General Customs Directorate (DGA) under ARCA. This system determines whether imports are subject to documentation checks (yellow channel) or physical inspection (red channel). In April 2024, the government implemented significant deregulation measures through Resolution S.I.C. N° 154/2024, Resolution S.I.C. N° 112/2024, and General Resolution N° 5582/2024,[44] eliminating the automatic "red channel" for a large percentage of imports, including goods subject to antidumping measures and certain reference price controls. Although this reform removed a major source of costly and unpredictable delays, the yellow channel remains in place and continues to create logistical and administrative obstacles for U.S. firms, albeit with shorter delays than those previously caused by mandatory red channel inspections.

In February 2025, Argentina enacted Resolution S.I.C. N° 16/2025 (Resolution of the Secretary of Industry and Commerce), establishing essential quality and safety requirements for electrical equipment.[45] This measure is part of a broader regulatory overhaul under Resolution S.I.C. N° 237/2024, which sets the general conformity assessment framework for certified products.[46] While the reform was presented as a modernization effort that permits the use of international certificates in lieu of local certification, provided the importer is formally authorized by the certificate holder, it simultaneously eliminated the simplified "internal use" exemption that previously allowed companies to import equipment by submitting a sworn statement. As a result, companies importing for their own use now face increased procedural and financial burdens, including securing the relevant international certificate, identifying the certificate holder, and obtaining formal authorization. These requirements significantly increase compliance obligations for U.S. and other foreign suppliers.

---

[43] *Agencia de recaudacion y control auduanero impuesto a las ganancias, impuesto sobre los bienes personales, regimen de percepcion* [Argentina], Resolución General 5617. (2024). https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-5617-2024-407430.
[44] *Resolución del Ministerio de Economía* [Argentina] Resolución 154/2024. (2024). https://www.boletinoficial.gob.ar/detalleAviso/primera/305469/20240408; *Ente Nacional Regulador del Gas, Transportadora del Gas sue S.A., Cuadros Tarifarios* [Argentina] Resolución 112/2024. (2024). https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-112-2024-397711; *Administracion Federal de Ingresos Publicos, Importacion, Valores Criterio de Caracter Precautorio* [Argentina] Resolución General 5582/2024. (2024). https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-5582-2024-405112.
[45] *Resolución del Ministerio de Economía* [Argentina] Resolución 16/2025. (2025). https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-16-2025-410052.
[46] *Resolución del Ministerio de Economía* [Argentina] Resolución 237/2024. (2024). https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-237-2024-403547/texto.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Argentina's public sector currently lacks a standardized framework for cloud service procurement, creating a significant market access barrier for foreign providers. Existing regulations lead to lengthy and inefficient procurement processes, discouraging public sector adoption of cloud solutions and imposing unnecessary administrative burdens on providers. This fragmented and cumbersome framework particularly affects U.S. technology companies seeking to offer cloud services to Argentine government entities. Establishing a comprehensive cloud procurement mechanism with flexible resource allocation and streamlined approval procedures would help address these challenges, facilitating market access while promoting more efficient and secure cloud service adoption in the public sector.

Restrictions on Cross-Border Data Flows

Argentina currently does not recognize the United States as an "adequate" jurisdiction for personal data transfers, creating a significant barrier to digital trade for U.S. companies. While data can flow freely to EU member states, EEA countries, and jurisdictions with EU adequacy decisions, transfers to the U.S. require additional contractual safeguards, such as standard contractual clauses, to comply with Argentina's data protection regime. This restriction stems from Argentina's close alignment with EU data protection standards, which contrasts with the U.S.'s sectoral approach and the absence of a comprehensive federal privacy law. As a result, U.S. companies face higher operational complexity, increased compliance costs, and delays in service implementation. Addressing this barrier would likely require amending Disposition E60/2016 AAIP[47] to recognize the U.S. as an adequate jurisdiction or accepting U.S. Data Privacy Framework (DPF)-certified companies as meeting adequacy requirements.

Taxation of Digital Products and Services

In 2018, ARCA ruled that online advertising services provided by non-residents did not generate Argentine-sourced income and were therefore not subject to taxation in Argentina. However, in 2020, AFIP changed its interpretation and unreasonably classified online advertising services as audiovisual content, subjecting cross-border advertising to a 17.5% withholding tax applicable to audiovisual royalties.[48] This change represented a significant expansion of the tax base, bringing certain digital services, previously regarded as non-taxable, within the scope of Argentine income tax. Notably, the 2020 ruling specifically targets online advertising with audiovisual elements, but its application has not been consistent across other digital services, similar to digital services taxes in other markets.

---

[47] *Disposición del Ministerio de Justicia y Derechos Humanos* [Argentina] Disposición E 60/2016. (2016). https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-60-2016-267922

[48] Santander. (n.d.). *Argentina: Tax System*. https://santandertrade.com/en/portal/establish-overseas/argentina/tax-system.

Australia

Asymmetric Platform Regulation

In December 2022, the Australian Competition and Consumer Commission (ACCC) launched a consultation on adopting a new regulatory framework for consumer protection and competition in digital platform services, drawing heavily on elements of the EU's Digital Markets Act.[49] The ACCC's proposals, many of which would require new legislation, included targeted obligations on practices such as self-preferencing, tying, exclusive defaults, impediments to switching and interoperability, data-related barriers, and unfair dealings with business users, alongside mandatory scanning for scams and harmful content. Industry expressed concern that these measures rested on poorly defined harms, risked hindering innovation, and could, if provable, be actionable under existing competition law.

In December 2023, the Australia Treasury formally endorsed key recommendations from the ACCC's interim report, including introducing *ex-ante* regulation of select digital services suppliers. These ideas were subsequently incorporated into a December 2024 Australian Treasury proposal to regulate large digital platforms with a "critical position in the Australian economy."[50] The regime would introduce *ex ante* obligations, applying only to platforms designated through thresholds such as revenue or user base, though the proposal also considered factors like market position and power. Designated platforms would face both "broad obligations" applicable across all services, covering issues such as self-preferencing, tying, barriers to switching and interoperability, unfair treatment of business users, and lack of transparency, as well as potential service-specific obligations. Compliance would be overseen by the ACCC, which would gain expanded powers for monitoring and data gathering, with significant financial penalties for breaches. The proposal also includes an exemption mechanism, allowing designated platforms to seek ACCC approval for conduct that might otherwise breach obligations, though the Treasury paper emphasizes that exemptions would be granted only under a high threshold and stricter conditions than under existing law. This approach reflects Australia's move toward proactive regulation of digital platforms, aligning in many respects with international trends such as the EU's Digital Markets Act.

[49] Australian Department of the Treasury. (2022). *Digital Platforms: Government consultation on ACCC's regulatory reform recommendations*. https://treasury.gov.au/sites/default/files/2022-12/c2022-341745-cp.pdf.
[50] Australian Department of the Treasury. (2024). *A New Digital Competition Regime*. https://treasury.gov.au/sites/default/files/2024-12/c2024-547447-pp.pdf.

In March 2025, the ACC issued the final report from its inquiry, retaining recommendations on *ex-ante* regulation.[51] At this point, the focus going forward is likely to be on legislative drafting to implement the recommendations.

The ACCC recommendations and the parallel Treasury proposal risk creating significant trade barriers for U.S. digital services providers by imposing broad, DMA-style obligations that disproportionately affect foreign firms. Similar frameworks in Europe have shown such rules to drive up compliance costs, deter cross-border investment, and raise consumer prices.[52] Although the Australian government has justified its proposed intervention in terms of bolstering economy-wide efficiency, estimates suggest the regime could reduce investment in digital services by up to 17.4%, lower GDP by up to A$21.1 billion, and disproportionately impact international suppliers.[53] By targeting specific firms through prescriptive obligations rather than adopting principle-based, evidence-driven enforcement, the proposal threatens to distort competition and undermine U.S. market access in Australia.

A November 2023 proposed rule Australia is considering would empower its central bank with overly broad authority to oversee digital payment providers like Apple Pay and Google Pay.[54] If implemented, the draft law would expand the definitions of "payment system" and "participant," and introduce "a new ministerial designation power that will allow particular payment services or platforms that present risks of national significance to be subject to additional oversight by appropriate regulators."

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In 2019, the Australian Government released the Hosting Strategy,[55] providing policy direction on how government data and digital infrastructure implements the Digital Transformation Strategy, focusing on certification of data center facilities, infrastructure, data storage and data transmission. In March 2021, the certification framework for the policy was released.[56] Certification requires hosting providers, data center operators, and cloud service providers to

---

[51] Australian Competition & Consumer Commission. (2025). *Digital Platform Services Inquiry final report – March 2025*. https://www.accc.gov.au/about-us/publications/serial-publications/digital-platform-services-inquiry-2020-25-reports/digital-platform-services-inquiry-final-report-march-2025

[52] Schramm, C. (2025). *Costs to U.S. Companies from EU Digital Services Regulation.* CCIA. https://ccianet.org/research/reports/costs-to-us-companies-from-eu-digital-services-regulation/.

[53] Taylor, W. & Feyler, E. (2025). *A New Digital Competition Regime: Insights into Economic Risks*. CCIA. https://ccianet.org/wp-content/uploads/2025/02/CCIA_New-Digital-Competition-Regime-Insights-into-Economic-Risks_report.pdf.

[54] Australian Department of the Treasury. (2023). *Reforms to the Payment Systems (Regulation) Act 1998 – Exposure draft legislation* [Consultation]. https://treasury.gov.au/consultations/c2023-452114.

[55] Australian Digital Transformation Agency. (2019). *Annual Report 2018-19.* https://www.dta.gov.au/sites/default/files/documents/2025-05/dta-annual-report-2018-19-revised-7-Nov-19.pdf.

[56] Australian Digital Transformation Agency. (2021). *Whole of Government Hosting Strategy: Hosting Certification Framework.* https://www.dta.gov.au/sites/default/files/documents/2025-05/dta-annual-report-2018-19-revised-7-Nov-19.pdf.

allow the government to specify ownership and control conditions. The framework has the effect of imposing data localization, data residency, and 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.[57]

Discriminatory Local Content Quotas and Audiovisual Service Mandates

The Australian government has long been under pressure to introduce legislation imposing local content quotas, mandatory spending, or "prominence" obligations on streaming services. In 2023, it released a report calling for "requirements for Australian screen content on streaming platforms to ensure continued access to local stories and content," with measures to be unveiled in the third quarter of 2023 and to commence no later than July 1, 2024.[58] These proposals would compel streaming providers to dedicate up to 20% of their annual drama expenditures in Australia, or 10–20% of their local revenues, towards narrowly defined "Australian programs." These obligations would fall disproportionately on U.S. streaming services, diverting investment away from U.S. and international productions. They are highly prescriptive, granting Screen Australia oversight authority and potentially extending to subgenres such as childrens programming and documentaries, creating significant compliance burdens and conflicts of interest.

Such measures would directly conflict with Australia's obligations under AUSFTA. Article 16.4 prohibits discrimination against digital products based on the nationality of authors, producers, or distributors, while Article 11.9 bars performance requirements that mandate specific levels of domestic content.[59] By obligating U.S. firms to allocate fixed portions of their budgets or revenues to Australian productions, the proposals effectively impose discriminatory local content mandates. Australia may only derogate from these commitments if domestic content is "not readily available," yet data show that Australian programming is already abundant and expanding.[60] Foreign investment has fueled record production levels, with more than US$1.2 billion from U.S. streaming providers supporting Australian drama in 2022–23, alongside a 60% year-over-year increase in Australian titles on major platforms. The supply of domestic content

---

[57] Australian Department of Home Affairs. (n.d.). *Safeguarding Australian Government data.* https://www.hostingcertification.gov.au/.
[58] Australian Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts. (2023). *Revive: Australia's Cultural Policy for the next five years.* https://www.arts.gov.au/sites/default/files/documents/national-culturalpolicy-8february2023.pdf.
[59] *Australia–United States Free Trade Agreement*, Art. 16.4 (2005). https://www.dfat.gov.au/trade/agreements/in-force/ausfta/official-text; *Australia–United States Free Trade Agreement*, Art. 11.9 (2005). https://www.dfat.gov.au/trade/agreements/in-force/ausfta/official-text.
[60] Screen Australia. (2021). *Drama Report 2021/22: Record $2.29 billion spent on drama production in Australia*. https://www.screenaustralia.gov.au/sa/media-centre/news/2022/11-10-drama-report-2021-22; Australian Communications and Media Authority. (n.d.). *Spending by Subscription Video On Demand Providers: 2021–22 Financial Year*. https://www.acma.gov.au/spending-subscription-video-demand-providers-2021-22-financial-year.

has nearly doubled since 2020, undercutting the rationale for new mandates.[61] While reports suggest the government has paused these proposals,[62] such legislation could still be revived at a later point. CCIA urges USTR to actively monitor these developments and engage with Australia to prevent discriminatory obligations that would breach AUSFTA if adopted.

Forced Revenue Transfers for Digital News

In February 2021, the Australian Government passed the News Media and Digital Platforms Mandatory Bargaining Code.[63] The Code requires designated platforms to negotiate with and pay Australian news publishers for online content.[64] If negotiations fail within three months, the process moves to compulsory mediation and, if still unresolved, "final offer" arbitration. The Code also mandates advance notice of algorithm changes likely to affect referral traffic. The Australian Treasury has broad discretion to determine which platforms are subject to the Code, considering both bargaining power imbalances and contributions to the sustainability of the news sector. To date, only two companies, both U.S.-based, have been targeted, raising concerns from procedural,[65] competition,[66] trade,[67] and intellectual property[68] perspectives. While no firm has yet been formally designated, Treasury's 2022 consultation made clear that Google and Meta remain the law's primary focus, with both avoiding designation only after striking commercial deals.[69] A Treasury report in November 2022 found that at least 30 such agreements were reached, though their contents remain confidential.[70] The report recommended expanded

---

[61] Screen Australia. (2021). *Drama Report 2021/22: Record $2.29 billion spent on drama production in Australia*. https://www.screenaustralia.gov.au/sa/media-centre/news/2022/11-10-drama-report-2021-22; Australian Communications and Media Authority. (n.d.). *Spending by Subscription Video On Demand Providers: 2021–22 Financial Year*. https://www.acma.gov.au/spending-subscription-video-demand-providers-2021-22-financial-year.
[62] Lowrey, T. & Long, C. (2025, November 5). Federal government quietly shelves plans for local content requirements. *ABC*. https://www.abc.net.au/news/2024-11-06/government-quietly-shelves-plans-for-local-content-requirements/104564654.
[63] *Australia Communications and Media Authority*. (n.d.). News media bargaining code. https://www.acma.gov.au/news-media-bargaining-code.
[64] Disruptive Competition Project. (2021, February 19). *The Dangers of Australia's Discriminatory Media Code*. https://www.project-disco.org/21st-century-trade/021921-the-dangers-of-australias-discriminatory-media-code/.
[65] Lopez-Galdos, M. (2020, August 6). *Australian Regulations Detrimental to the Digital Economy: Process (Part 1)*. Disruptive Competition Project. https://www.project-disco.org/competition/080620-australian-regulations-detrimental-to-the-digital-economy-process/.
[66] Lopez-Galdos, M. (2020, August 13). *Australian Regulations Detrimental to the Digital Economy: Process (Part 2)*. Disruptive Competition Project. https://www.project-disco.org/competition/081320-australian-regulations-detrimental-to-the-digital-economy-competition/.
[67] Stelly, R. (2020, September 4). *Australian Regulations Detrimental to the Digital Economy: Process (Part 3).* Disruptive Competition Project. https://www.project-disco.org/21st-century-trade/090420-australian-regulations-detrimental-to-the-digital-economy-trade-part-3/.
[68] Sternburg, A. (2020, October 9). *Australian Regulations Detrimental to the Digital Economy: Process (Part 4)*. Disruptive Competition Project. https://www.project-disco.org/intellectual-property/100920-australian-regulations-detrimental-to-the-digital-economy-intellectual-property-part-4/.
[69] Australian Department of the Treasury. (2022). *Review of the News Media and Digital Platforms Mandatory Bargaining Code Consultation Paper*. https://treasury.gov.au/sites/default/files/2022-04/c2022-264356_0.pdf.
[70] Australian Department of the Treasury. (2022). *News Media and Digital Platforms Mandatory Bargaining Code.* https://treasury.gov.au/sites/default/files/2022-11/p2022-343549.pdf.

investigatory powers, compulsory information sharing, and a full review in 2025. The government has since committed to implementing all recommendations, further strengthening the ACCC's oversight. Despite proponents' claims, the Code has failed to revitalize journalism. Studies show the sector has continued to shrink, with regional and rural outlets disproportionately closing, leaving small independent publishers less competitive and communities underserved. The divide between urban and regional news production has widened since the law's passage.[71] As initial agreements expire, concerns remain that Australian policymakers will exert political pressure to extract additional payments from U.S. firms as a condition of market access, particularly given the 2024 decision by one major platform to cease carrying domestic news.

On December 12, 2024, the government announced the News Bargaining Incentive, a form of tax aimed at reinforcing revenue-sharing with Australian news organizations.[72] The charge applies to platforms with annual Australian revenue above AUD 250 million that lack agreements and can be offset by payments made to local media. Since by its scoping this tax will fall on a limited number of foreign (predominantly U.S.) firms, it appears challengeable under trade commitments as being discriminatory.

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 that 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.[73] Criticism for the legislation was widespread, with particular concern about the rushed nature of the drafting and legislative process, precluding meaningful stakeholder consultation.[74] The legislation applies to a broad range of technology and internet services, including U.S.-based social media platforms, user-generated content, live streaming services, and hosting services. However, the law does not take into account the varying business models of the services in scope and their varying capabilities or roles in facilitating user-generated content.

---

[71] The Public Interest News Foundation. (2023, June 15). *A submission to the Public Bill Committee* [Submission to the government of the UK]. Government of the UK. https://bills.parliament.uk/publications/51757/documents/3633; CCIA. (2023). *The Harms of Forced Online News Payments: How Mandatory Payments from Digital Services to News Business Undermine Commerce and the Internet Ecosystem*. https://ccianet.org/wp-content/uploads/2023/12/CCIA-Harms-of-Forced-Online-News-Payments-Paper.pdf.

[72] Australian Department of the Treasury. (2024). *News Bargaining Incentive Fact Sheet*. https://ministers.treasury.gov.au/sites/ministers.treasury.gov.au/files/2024-12/news-bargaining-incentive-fact-sheet.docx

[73] *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019* [Australia] Bill No. 45. (2019). https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1201.

[74] Douek, E. (2019, April 10). *Australia's New Social Media Law Is a Mess.* Lawfare. https://www.lawfareblog.com/australias-new-social-media-law-mess.

The Online Safety Act which was passed in July 2021[75] gives the eSafety Commissioner the power to demand the removal of adult cyber abuse and other content that is deemed "harmful." This legislation also gave the eSafety Commissioner the power to compel 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, which the eSafety Commissioner exercised in April 2022.[76] The sectors are: social media services; internet search engine services; app distribution services; enterprise online hosting services; internet access services; manufacturers, suppliers, maintainers and installers of any equipment used to access the internet; relevant electronic services (covering e-mail, instant messaging, SMS, MMS, chat, and online gaming services); and designated internet services (covering all websites and end-user online hosting services).[77] While industry responded by developing eight different Codes of Practice (corresponding to the eight different sectors mentioned), the eSafety Commissioner rejected two of those covering relevant electronic services and designated internet services - and instead proceeded, in November 2023, to issue two industry standards for such services.[78] Industry is concerned about strict requirements to invest in systems to detect and remove harmful online content (and the associated need to build Australia-specific policies, products, and systems); the ill-defined concept of "harm" that will lead to lawful content being censored; and disproportionate penalties. These concerns have grown as the Commissioner has recently used these powers to compel the removal of certain lawful but controversial content, underscoring how broad and discretionary enforcement may create significant barriers for platforms, particularly foreign ones, by forcing rapid content moderation decisions under unclear standards.

The Online Safety Amendment (Social Media Minimum Age) Bill was passed by the Australian Government on November 28, 2024. It introduces a mandatory minimum age of 16 years old for accounts on certain social media platforms, and the minimum age cannot be overridden by parental controls. This legislation will come into effect by December 2025. The law and the implementation expectations signaled by the Australian Government to date appear to disproportionately target U.S. technology companies,[79] overlooking existing industry investments in age assurance solutions and imposing obligations that are misaligned with the current state of age assurance technologies. Restriction of access to online content based on age raises serious concerns for industry about freedom of expression and information. Such a

[75] *Online Safety Act 2021* [Australia] Bill No. 76. (2021). https://www.legislation.gov.au/C2021A00076/latest/text.
[76] Library of Congress. (2021, August 10). *Australia: Online Safety Bill Passed*. https://www.loc.gov/item/global-legal-monitor/2021-08-10/australia-online-safety-bill-passed/.
[77] *See* 135 of the *Online Safety Act 2021*. *Online Safety Act 2021* [Australia] Bill No. 76. (2021). https://www.legislation.gov.au/C2021A00076/latest/text.
[78] Australian eSafety Commissioner. (n.d.). *Register of industry codes and industry standards for online safety*. https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards#register-of-industry-standards.
[79] Australian eSafety Commissioner. (n.d.). *Social media age restrictions*. https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions.

framework risks applying disproportionate penalties to U.S. firms, while overbroad and blanket restrictions could stifle creativity and disproportionately limit valuable online experiences.

On July 12, 2024, the Chair of the Competition and Consumer Commission announced a proposed law requiring internet companies to proactively take down scams. The regulation would create a mandatory, enforceable set of requirements for companies to take reasonable steps to protect consumers and offer redress, with potential fines of up to A$50 million, three times the benefit gained by the scam, or 30% of turnover.[80] The obligation would require companies to proactively monitor their services, drastically increasing the costs of operation in the Australian market.

Failure to implement obligations under existing trade agreements serves as a barrier to trade.[81] AUSFTA contains an obligation to provide liability limitations for online 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 online 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.[82] 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.[83] These amendments specifically exclude U.S. digital services and platforms from the operation of the framework. The failure to include online services such as search engines and commercial content distribution services disadvantages U.S. digital services in Australia and serves as a deterrent for investment in the Australian market.

---

[80] Kaye, B. (2024, July 12). Australia to Bring Anti-Scam Law Targeting Internet Giants This Year, Regulator Says. *Reuters*. https://www.reuters.com/technology/australia-bring-anti-scam-law-targeting-internet-giants-this-year-regulator-says-2024-07-12/.

[81] CCIA. (2020, February 6). *A submission to the U.S. Trade Representative re 2020 Special 301 Review* [Submission to the U.S. Trade Representative]. https://www.ccianet.org/wp-content/uploads/2020/03/CCIA_2020-Special-301_Review_Comments.pdf.

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

[83] *Copyright Amendment (Disability Access and Other Measures) Bill 2017* [Australia] Act. No. 49. (2017). https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5832; Band, J. (2018, July 6). Australian Copyright Law Thumbs Nose at U.S. Trade Commitments. *Disruptive Competition Project*. http://www.project-disco.org/intellectual-property/070518-australian-copyright-law-thumbs-nose-at-u-s-trade-commitments/.

Potential Challenges to the Development of AI

The Australian Department of Industry, Science, and Resources (DISR) is pursuing a regulatory framework that would establish mandatory guardrails for high-risk AI systems, as first proposed on September 4, 2024.[84] Despite the framework's intended interoperability with other national regulations, it advances broad principles for AI governance that would impose substantial burdens on the private sector. In particular, industry remains concerned that it does not clearly define which AI systems are considered high risk according to a specific threshold of potential harm, instead defining all general-purpose AI systems as high risk. Given U.S. companies' leading edge in AI innovation, such a broad scope would mostly capture U.S. companies, imposing substantial disclosure obligations disproportionate to the risk their systems pose.

Taxation of Digital Products and Services

The Treasury Laws Amendment (GST Low Value Goods) Act 2017 took effect in 2018 and directs the Australian government to start collecting a goods and services tax (GST) on all goods including those purchased online from overseas, that previously only applied to goods over AU$1,000.[85] Companies with over AU$75,000 in sales to Australian customers are required to register and lodge returns with the Australian Tax Office (ATO). Australia's GST on low-value imported goods imposes a *de facto* market access barrier by requiring foreign companies above a sales threshold to register, collect, and remit Australian taxes, effectively outsourcing domestic tax administration to offshore firms. This obligation departs from international practice, where import duties and taxes are typically collected at the border, and creates disproportionate compliance costs for smaller exporters relative to domestic competitors.

The ATO has long been considering changes to what is deemed a "royalty" in a manner that if finalized, could implicate digital exporters.[86] In January 2024 the ATO released an updated proposed rule (TR 2024 D1) that would institute core changes to the treatment of software license distributors.[87] Based on this ruling, the delivery of software (both as a download or as a cloud-based service) could be subjected to Australian withholding tax as a royalty. This change to the 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

---

[84] Australian Department of Industry, Science, Energy and Resources. (2024). *Introducing Mandatory Guardrails for AI in High-Risk Settings: Proposals Paper*. https://consult.industry.gov.au/ai-mandatory-guardrails.
[85] *Treasury Laws Amendment (GST Low Value Goods) Act 2017* [Australia] Act No. 77, 2017. (2017). https://www.legislation.gov.au/C2017A00077/latest/text.
[86] *Draft Taxation Ruling, Income tax: royalties - character of receipts in respect of software* [Australia] TR 2021/D4. (2021). https://www.ato.gov.au/law/view/document?DocID=DTR/TR2021D4/NAT/ATO/00001.
[87] *Draft Taxation Ruling, Income tax: royalties - character of payments in respect of software and intellectual property rights* [Australia] TR 2024/D1. (2024). https://www.ato.gov.au/law/view/document?docid=DTR/TR2024D1/NAT/ATO/00001.

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.[88] The new approach would classify distributors and resellers as engaging in an ancillary "authorization" copyright inherent in software programs, regardless of whether the owner of the software copyright has approved any rights to modification, reproduction, or other actions to the distributor in question. This would effectively characterize transactions between software distributors and resellers as engaging in copyright rights exchanges rather than simply exchanging a copyrighted article or supplying a service.

In a related action, on August 19, 2025, the High Court issued a decision rejecting ATO's attempt to impose royalty withholding tax and diverted profits tax on payments for goods between independent parties.[89] The Court held that such payments could not be recharacterized as containing "embedded royalties" for intellectual property. This should inform TR 2024/D4 in failing 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. However, the High Court's *PepsiCo* decision has weakened the ATO's stance by rejecting overly broad recharacterizations of payments as royalties, suggesting parts of TR 2024/D1 may need to be revised before finalization. Notwithstanding this, the ATO continues to assert that its approach is consistent with Australia's Double Taxation Avoidance Agreements, including its treaty with the United States, leaving important uncertainty for affected companies.

Threats to Encryption and Security of Devices

The Australian Parliament passed the Telecommunications (Assistance and Access) Act in 2018, granting the country's national security and law enforcement agencies additional powers when dealing with encrypted communications and devices.[90] 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, which seek voluntary assistance from communications providers; and technical assistance notices (TANs) and technical capability notices. These tools call upon providers to do one or more specified acts which could include building new technical capabilities as required by the Attorney General. While the legislation specifically forbids a notice to provide a "systemic

[88] OECD. (2017). *Model Tax Convention on Income and on Capital: Condensed Version 2017.* https://www.oecd.org/ctp/treaties/model-tax-convention-on-income-and-on-capital-condensed-version-20745419.htm
[89] *Commissioner of Taxation v PepsiCo Inc* [2025] HCA 30.
[90] *Telecommunications (Assistance and Access) Bill 2018* [Australia] Act No. 148. (2018). https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195.

weakness or vulnerability" into an encrypted system, it provides authority to undermine encryption through other technical means with little oversight. 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, empowering the agency to "compel designated communications providers to give assistance where they already have the technical capability to do so."[91]

In April 2022, Australia passed the Critical Infrastructure Protection Bill 2022.[92] The legislation significantly expands the sectors considered critical infrastructure (including companies that provide "data storage or processing" services) and imposes additional positive security obligations for critical infrastructure assets (e.g. risk management programs and cyber incident reporting), enhanced cyber security obligations and, most concerningly, government assistance measures that 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.

Austria

Taxation of Digital Products and Services

On January 1, 2020, Austria enacted a 5% digital services tax on digital advertising services provided domestically.[93] The global revenue threshold for suppliers subject to the tax is €750 million, excluding a broad range of Austrian suppliers. "Online advertisement services" under the law are defined broadly to include advertisements placed on a digital interface, including banner advertising, search engine advertising, and other comparable services.[94] 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." The design and implementation of this measure raise serious concerns regarding its discriminatory intent and impact. Public statements by Austrian officials at the time of introduction made clear that the measure was aimed at foreign digital service providers, particularly large global platforms.[95] In 2023, the total amount paid under the tax reached €103

---

[91] Australian Department of Home Affairs. (2021). *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.
[92] *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* [Australia] Act No. 33. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6833.
[93] KPMG. (2019, October 29). *Austria: Legislation Introducing Digital Services Tax*. https://home.kpmg/us/en/home/insights/2019/10/tnf-austria-legislation-introducing-digital-services-tax.html.
[94] Federal Ministry Republic of Austria. (n.d.). *Digital Tax Act 2020*. https://www.bmf.gv.at/en/topics/taxation/digital-tax-act.html.
[95] Kurz, S.[@sebastiankurz]. (2019, April 3). *#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* [Social media post]. https://x.com/sebastiankurz/status/1113361541938778112; Austrian Parliament. (2019, September 20). *Nationalrat: Digitalsteuer auf Online Werbeumsätze beschlossen*. https://www.parlament.gv.at/aktuelles/pk/jahr_2019/pk0914.

million, with the overwhelming majority of revenues collected from foreign, especially U.S.-based, companies.[96] This approach risks distorting competition, discouraging foreign investment, and undermining the principles of non-discrimination in international trade.

Bangladesh

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In October 2025, the Cabinet of the Interim Government of Bangladesh adopted the Personal Data Protection Ordinance (PDPO) and the National Data Governance Ordinance (NDGO), following limited industry consultation on the former and none on the latter. The PDPO introduces criminal liability and extraterritorial provisions, as well as data localization requirements for certain categories of restricted data.[97] Classified data (classified as confidential and restricted, based on governmental discretion) must be stored within Bangladesh's jurisdiction. Cross-border transfers of internal and confidential data are permitted only with consent or under specific contractual or interest-based conditions, and solely to countries deemed to have adequate data protection technology and infrastructure. These localization mandates and transfer restrictions could significantly limit the ability of companies to rely on global cloud infrastructure and may, in practice, compel foreign providers to establish or expand local data centers, effectively functioning as a data localization requirement.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

The Bangladesh government has historically taken an aggressive stance against digital services platforms, particularly American companies. Throughout June and August 2024, the Bangladesh Telecommunication Regulatory Commission (BTRC) instructed international internet gateway operators to block access to major social media platforms and messaging services, including Facebook, WhatsApp, TikTok, and YouTube, amidst ongoing social unrest.[98] The Minister for Posts, Telecommunications & Information Technology cited companies' failure to comply with laws on combatting misinformation, without citing specific directives, to justify the blockages—and threatened imposing further regulatory measures, including data localization.[99] The full

[96] Austrian Ministry of Finance. (2024, January 15). *Brunner: Tax revenues from digital tax increased by 7.4 % year-on-year to EUR 103 million in 2023; Digital tax contributes to a fair tax landscape*. https://www.bmf.gv.at/en/press/press-releases/2024--New/January-2024/Brunner--Tax-revenues-from-digital-tax-increased-by-7.4---year-on-year-to-EUR-103-million-in-2023--Digital-tax-contributes-to-a-fair-tax-landscape.html.
[97] *Dhaka Tribune*. (2025, October 9). Government approves Personal Data Protection Ordinance, 2025. https://www.dhakatribune.com/bangladesh/393590/bangladesh-government-approves-personal-data.
[98] *The Daily Star*. (2024, July 27). Social Media Off-Limits Indefinitely. https://www.thedailystar.net/news/bangladesh/news/social-media-limits-indefinitely-3662216.
[99] The Business Post. (2024, July 17). *Palak Issues Final Warning, Blames Facebook for Misinfo.* https://businesspostbd.com/national/palak-issues-final-warning-blames-facebook-for-misinfo.

block was removed once former Prime Minister Sheikh Hasina was deposed and fled the country in August 2025.

The Information and Communication Technology Act of 2006 (the Act), amended in 2013, authorizes the government of Bangladesh to access any computer system for the purpose of obtaining any information or data, and to intercept information transmitted through any computer resource. Under the Act, Bangladesh may also prohibit the transmission of any data or voice call and censor online communications. The BTRC has ordered mobile operators to limit data transmissions for political reasons on several occasions ahead of politically sensitive events, including local and national elections.

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.[100] The Act 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.[101] These include such broad categories such as the publication of information online that undermines the nation, tarnishes the image of the state or hurts religious sentiment. The Act also empowers the government to remove and block content online.[102] Upon passage of the Act, 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."[103] The State Department, in its latest Investment Climate Statements, observed that "the CSA continues to criminalize freedom of expression, and cases have been filed under the new law to harass members of the media, civil society, and opposition groups."[104] While there were high hopes for the Interim Government to usher in transparency and proportionality, its legislative process has not been consultative. Earlier in 2025, the ICT Division issued the Cyber Security Ordinance (CSO), which replaced the restrictive and globally criticized CSA.[105] Though the CSO was an improvement over the CSA, there was little to no consultation with industry before it passed.

---

[100] Sengupta, D.M. (2023, September 20). Bangladesh Revised a Digital Security Law. Is it Really Less Severe? *Rest of World*. https://restofworld.org/2023/south-asia-newsletter-bangladesh-cyber-security-act/.
[101] Singh, S. (2023, August 22). [Letter from Amnesty International to the Bangladesh Government regarding the proposed "Cyber Security Act.] https://www.amnesty.org/en/documents/asa13/7125/2023/en/.
[102] *Dhaka Tribune*. (2023, September 13). Parliament Passes Cyber Security Bill 2023. https://www.dhakatribune.com/bangladesh/325228/parliament-passes-cyber-security-bill-2023.
[103] U.S. Embassy in Bangladesh. (2023, September 14). *U.S. Embassy Statement on the Passage of the Cyber Security Act.* https://bd.usembassy.gov/30390/.
[104] U.S. Department of State. (2024). *2024 Investment Climate Statements: Bangladesh*. https://www.state.gov/reports/2024-investment-climate-statements/bangladesh/.
[105] Amnesty International. (2024, August 8). *Bangladesh: Interim Government must restore freedom of expression in Bangladesh and repeal Cyber Security Act*. https://www.amnesty.org/en/latest/news/2024/08/bangladesh-interim-government-must-restore-freedom-of-expression-in-bangladesh-and-repeal-cyber-security-act/

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

The BTRC has been working since 2022 on an amendment to the Bangladesh Telecommunication Regulatory Act (BTRA) that would bring digital services platforms under its purview, ostensibly to protect end users and vulnerable groups; prevent fraud and threats to public order and sovereignty; and discourage piracy and obscenity.[106] The combination of takedown requirements based on vague standards, weakening of privacy protections, and the potential for abuse for political ends has motivated significant opposition by civil society.[107]

Belgium

Taxation of Digital Products and Services

In 2025, the government of Belgium announced plans to introduce a 3% "digitax" by 2027 at the latest, pending the outcome of ongoing European and international discussions.[108] If modeled on Belgium's 2019 proposal,[109] the tax would apply to companies with global revenue of at least €750 million and local revenue of at least €5 million, mirroring the scope of the European Commission's Digital Services Tax proposal and the extant regimes of several European countries. Under this framework, revenue from digital advertising services, intermediation and marketplace services, and data transmission would be subject to taxation, potentially creating a significant burden for large foreign digital service providers.

Bolivia

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Bolivia maintains restrictive data localization requirements for the public sector through its Electronic Government Plan and Open Software and Open Standards Implementation Plan (PISLEA 2025–2030), which was adopted in March 2025.[110] Under these regulations, public sector entities must store "non-public" government data within Bolivian territory, effectively preventing international cloud service providers from offering storage solutions to government institutions. While recent updates to PISLEA in mid-2025 introduced limited flexibility,

---

[106] Biyani, N., De Guzman, N. F., Maheshwari, N., & Mahmood, S. (2022). *Internet Impact Brief: Bangladesh: Regulation for Digital, Social Media and OTT Platforms, 2021*. Internet Society. https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-bangladesh-regulation-for-digital-social-media-and-ott-platforms-2021.

[107] Freedom House. (2024). *Freedom on the Net 2024: Bangladesh*. https://freedomhouse.org/country/bangladesh/freedom-net/2024.

[108] Asquith, R. (2025, February 4). *Belgium 3% DST by 2027*. VAT Calc. https://www.vatcalc.com/belgium/belgium-3-dst-by-2027/.

[109] Clifford Chance. (2020). *New Belgian Digital Services Tax Discussed in Commission*. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/06/new-belgian-digital-services-tax-discussed-in-commission.pdf.

[110] *Plan de Implementación de Software Libre y Estándares Abiertos (PISLEA)* [Bolivia] Decreto Supremo N° 5322. (2025). https://agetic.gob.bo/sites/default/files/2025-02/ANEXO-DS-5322.pdf.

allowing cloud services for "public" data and certain cloud-based operations for "non-public" data such as processing, the regulations continue to impose strict localization requirements on data storage. The absence of clear definitions for "public" and "non-public" data creates significant legal uncertainty for companies seeking to serve Bolivian government clients. To address these barriers, Bolivia should consider aligning with international data protection standards, permitting cross-border data flows, and adopting risk-based regulatory approaches rather than blanket localization mandates.

Institutions are required to submit detailed implementation projects without clear assessment guidelines, resulting in lengthy and unpredictable approval timelines. In addition, financial institutions must maintain both an on-premises data processing center and an alternate processing center, even if adopting cloud solutions, while ASFI also requires physical auditing access to cloud providers' facilities. These requirements are more restrictive than those of neighboring countries such as Argentina, Brazil, Chile, Colombia, Peru, and Paraguay, which only require notification rather than prior approval. To modernize its approach, Bolivia should replace the prior approval system with a notification mechanism, establish clear timelines and criteria for review, and harmonize its regulatory framework with regional best practices to enable more efficient and secure cloud adoption.

Brazil

Asymmetric Platform Regulation

In November 2022, Bill 2768 was introduced in Brazil's Congress,[111] borrowing from the European Union's Digital Markets Act. This bill would authorize the National Telecommunications Agency (ANATEL) to function as the primary regulator of "digital platforms." The bill also prescribes a regulatory framework for "digital platforms" that offer services to users in Brazil but with vague definitions that fail to clearly delineate who would be subject to regulation and what specific obligations would result. Instead, it provides ANATEL with broad discretionary authority to define terms and create rules, resulting in significant uncertainty, increased compliance costs, and the possibility of having to restructure business operations.[112]

On September 18, 2025, the Brazilian government formally submitted Bill 4.675/2025 (the "Digital Markets Bill") to the House of Representatives for legislative consideration.[113] The bill

[111] *Dispõe sobre a organização, o funcionamento e a operação das plataformas digitais que oferecem serviços ao público brasileiro e dá outras providências* [Brazil] PL 2768. (2022). https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2337417.
[112] CCIA. (2025, September 18). *CCIA's Comments on Brazil's New Digital Competition and Regulatory Bill*. https://ccianet.org/news/2025/09/ccias-comments-on-brazils-new-digital-competition-and-regulatory-bill/.
[113] *PL 4675/2025* [Brazil]. (2025). https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2562481.

would give the competition authority, CADE, new powers to designate digital platforms as "systematically relevant" based on qualitative criteria and revenue thresholds. Once designated, firms would face a set of ex-ante obligations including mandatory M&A notification, transparency and interoperability mandates, and restrictions on certain commercial practices. It closely mirrors elements of the EU DMA, the UK DMCCA, and Germany's GWB §19a, marking a major shift from Brazil's traditional effects-based antitrust model. However, the proposal's narrow designation criteria would disproportionately affect foreign firms, raising national treatment and market access concerns. It would also impose costly local office requirements and onerous obligations that could chill innovation and deter investment. Finally, the absence of an efficiency defense and potential fines of up to 20% of gross revenue create significant legal uncertainty and risk of overdeterrence

Even in the absence of ex ante regulation, CADE has in recent years been exceedingly aggressive in its prosecution of U.S. digital services companies under Brazil's existing competition regime, frequently using these proceedings to import remedies established in the ex-ante law of other jurisdictions.

Barriers to the Deployment and Operation of Network Infrastructure

Law No. 9.472, enacted in 1997, requires that telecommunications service providers be juridical persons, with headquarters and administration in the country, created to operate telecommunications services exclusively.[114] In addition, it establishes a preference for Brazilian satellites over foreign satellites used for the performance of telecommunications services, unless the foreign satellites demonstrably provide superior technical, operational, or commercial conditions. These two requirements disadvantage foreign satellite operators. The domestic incorporation requirement effectively excludes foreign firms from directly supplying services without establishing a costly and administratively burdensome local subsidiary. Such requirements act as a form of forced localization that can deter investment and limit the ability of global providers to operate efficiently. Meanwhile, the preferential treatment of Brazilian satellites over their foreign competitors entrenches domestic orbital filings and disadvantages foreign satellite operators, limiting their ability to compete fairly in the Brazilian market.

ANATEL has reversed its 2021 decision to allocate the full 1,200 MHz of the 6 GHz band for unlicensed use, ending a policy that had aligned with the U.S. FCC approach to support next-generation Wi-Fi technologies. This 6 GHz spectrum is critical for a wide range of devices, including routers, AR/VR headsets, smartphones, and other internet-connected equipment. Harmonization of this band in the Americas would be of significant benefit to consumers and device makers in both the U.S. and the EU. In January 2025, under Resolution No. 772,

[114] *Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995* [Brazil] Law Nº 9.472. (1997). https://www.planalto.gov.br/ccivil_03/leis/l9472.htm.

ANATEL reserved 700 MHz of the band for licensed mobile services, leaving only 500 MHz available for unlicensed use.[115] The reversal followed lobbying from Chinese interests as well as European fixed and mobile equipment manufacturers,[116] despite extensive technical studies conducted between 2021 and 2025 that support the full, unlicensed allocation of the 6 GHz band. These studies have enabled U.S. companies to make substantial R&D investments and long-term business plans in Brazil based on the license-exempt framework. The effort moved through a closed and expedited process that bypassed meaningful public consultation and disregarded prior technical analyses, undermining regulatory stability. This abrupt policy shift risks eroding investor confidence and could negatively impact U.S. technology companies whose strategies and product development relied on Brazil's 2021 6 GHz allocation plan.

In April 2025, Anatel adopted Act No. 4141, updating Brazil's radio frequency rules governing satellite operations.[117] The new measure introduces a two-sided restriction: while new satellite operators must take all necessary steps to avoid causing harmful interference to existing systems, they are simultaneously barred from demanding interference protection for their own services. This asymmetry effectively locks in the position of incumbents, who enjoy protection from interference, while weakening the ability of new entrants to guarantee service quality. For U.S. satellite broadband providers seeking to enter or expand in the Brazilian market, such conditions create a structural disadvantage. Without the ability to claim protection, new entrants can face heightened operational risks, greater costs to maintain service reliability, and potentially reduced incentives to deploy innovative satellite-based connectivity solutions.

Customs-Related Restrictions and Import Barriers for Goods

Brazil's "ex-tarifário" program is a mechanism under Brazilian customs law that provides for a temporary reduction or complete exemption from import duties on capital goods and information and communication technology goods. To qualify, these goods must meet specific criteria, primarily demonstrating a lack of equivalent national production within Brazil. In August 2023, the government introduced updated guidance for the ex-tarifário program,[118] significantly altering the application process, including a requirement for importers to submit an "investment project" related to the imported products. This investment project demands detailed disclosure of

---

[115] *Resolução Anatel nº 772* [Brazil]. (2025). https://informacoes.anatel.gov.br/legislacao/resolucoes/2025/2001-resolucao-772.

[116] Lipscombe, P. (2023, July 7). TIM Brasil and Huawei to test 6GHz 5G. *Data Center Dynamics*. https://www.datacenterdynamics.com/en/news/tim-brasil-and-huawei-to-test-6ghz-5g/; Ericsson. (n.d.). *Spectrum, a shared gem*. https://www.ericsson.com/en/reports-and-papers/microwave-outlook/articles/spectrum-a-shared-gem#:~:text=The%%2020WRC%20in%202023%20(WRC,the%20next%20WRC%20in%202027.

[117] Bakaus, T. A. (2025, May 5). *Brazilian Regulations Use of Orbit and Space Sustainability* [Presentation Slides]. ANATEL. https://owl.purdue.edu/owl/research_and_citation/apa_style/apa_formatting_and_style_guide/reference_list_electronic_sources.html.

[118] *Resolução Gecex No. 512* [Brazil]. (2023). https://www.in.gov.br/en/web/dou/-/resolucao-gecex-n-512-de-16-de-agosto-de-2023-503880256.

the equipment's function, its planned schedule and location of use, its necessity for operations, expected productivity gains, and any innovative technologies it may introduce. Furthermore, the 2023 reforms granted greater flexibility for Brazilian domestic firms to challenge tariff exception requests for imported goods. These increasingly complex reporting requirements for importers, coupled with enhanced opportunities for Brazilian firms to challenge requests, are likely responsible for a noticeable decline in the approval rate of tariff exemptions for imported capital and ICT goods since 2023.[119]

This policy increases the ability of Brazilian firms to challenge tariff exemption requests, creating a procedural advantage for domestic producers by allowing them to block imports by claiming "equivalent national production," even if their offerings are not directly comparable in terms of technology or quality. While not facially discriminatory, the uncertainty and arbitrary effect of this process institutes de facto protection for local industry and restricts market access for U.S. ICT and capital goods providers, especially in highly technical or niche sectors where domestic alternatives are not truly substitutable. In addition, the "investment project" requirement imposes significant administrative and compliance burdens on importers, many of whom are subsidiaries or customers of U.S. firms, including services suppliers. This raises the cost and complexity of doing business in Brazil for U.S. exporters, particularly for SMEs that may lack the resources to navigate the revised process.

In August 2025, Brazil's Ministry of Environment, through the National Environmental Council, launched a public consultation on a draft national Restriction of Hazardous Substances regulation for electrical and electronic equipment, raising concerns among U.S. industry about trade impacts and regulatory divergence. The proposed regulation departs significantly from international best practices and relevant IEC 63000 standards, potentially creating new compliance burdens and market access barriers for ICT imports. Compounding these concerns, Brazil did not notify the WTO TBT Committee of the proposed regulation, contrary to its obligations under the TBT Agreement, undermining transparency and stakeholder engagement. These regulatory developments are particularly concerning in light of Brazil's longstanding prohibition on the import of used and remanufactured goods, including ICT products, subject only to limited exceptions. Together, these policies risk restricting the flow of ICT products, increasing costs for businesses and consumers, and creating additional obstacles for U.S. exporters seeking to access the Brazilian market.

[119] Putnam-Ladley, L. (n.d.). *Spotlight on Brazil: More Tariff Remedies and Tariffs, Fewer Tariff Exceptions*. Descartes Customs Info. https://www.customsinfo.com/knowledge-center/spotlight-on-brazil-more-tariff-remedies-and-tariffs-fewer-tariff-exceptions.

Discriminatory Local Content Quotas and Audiovisual Services Mandates

In July 2025, Brazil's Video on Demand Bill (2331/2022) was approved by the House Culture Commission and is now awaiting approval from the broader House.[120] The bill introduces a new "Contribution for the Development of the National Cinema Industry" levy, set at 6% of gross revenue, on video platforms, including U.S. social media services hosting user-generated content, and assigns Brazil's film agency responsibility for overseeing compliance. The stated purpose of the tax is to fund national content production through cultural promotion funds; however, access to these funds would be limited to companies directly engaged in content production, excluding most digital platforms that act primarily as intermediaries between creators and users. The bill also contains new provisions requiring the prominent placement of Brazilian broadcasters on connected TV interfaces. Together, these measures would disproportionately burden U.S. platforms while favoring domestic broadcasters, granting them both competitive visibility advantages and the financial benefits of the tax revenues. By imposing additional and unequal tax and regulatory obligations on foreign services, the proposal risks functioning as a discriminatory digital trade barrier with significant implications for market access, investment, and the broader digital economy.

Government-Imposed Content Restrictions and Related Access Barriers

The Brazilian Advisory Rating System, Classificação Indicativa (ClassInd), is the government's mandatory content rating framework for classifying media and entertainment, including streaming services, electronic games, applications, public performances, films, and television programs.[121] In recent months, the Ministry of Justice has raised the age classification 13 for Google, Facebook, Threads, and Instagram to 16+ (while TikTok and Kwai remain at 14+), citing the presence of age-inappropriate content. However, the decision-making process for establishing age-appropriate content is opaque and non-standardized, making it difficult for platforms to address the Ministry's concerns. Authorities do not provide URLs or specific examples of allegedly harmful material, relying instead on an opaque and non-standardized process in which officials submit screenshots from individual searches as "proof" of age-inappropriate content. This approach fails to account for the existence of established content moderation systems, such as Community Standards or other review processes. This lack of clarity and transparency appears to have resulted in disparate treatment of U.S. digital platforms, many of which have already implemented robust measures and parental tools to enhance child and youth safety online, while foreign competitors benefit from more 14 favorable classifications. Brazilian authorities should ensure consistent, transparent, and non-

[120] *Projeto de Lei 2331/2022* [Brazil]. (2022). https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2432409.
[121] Brazilian Ministry of Justice and Public Security. (n.d.). *Classificação Indicativa*. https://www.gov.br/mj/pt-br/assuntos/seus-direitos/classificacao-1.

discriminatory application of ClassInd to foster a predictable regulatory environment that supports continued investment and innovation.

In June 2025, Brazil's Federal Supreme Court issued a ruling finding Article 19 of the Marco Civil da Internet,[122] the country's primary internet governance framework, unconstitutional. Article 19 had previously limited the liability of internet application providers, establishing that platforms could only be held responsible for user-generated content if they failed to remove it following a judicial order. This ruling introduced a new liability framework under which internet platforms may be held civilly liable for harm caused by illicit third-party content, regardless of whether judicial notice was given.

The June 2025 ruling introduces significant legal uncertainty and may unfairly disadvantage U.S. companies engaged in digital trade and electronic services. By removing the long-standing liability shield that conditioned platform responsibility on responsiveness to judicial orders, the ruling exposes internet application providers to heightened and potentially subjective standards of civil liability for third-party content, even in the absence of prior notification. Given the volume of content that providers host and/or transmit, it is widely recognized that effectively monitoring all content is infeasible, which leads to extraordinary liability. Notwithstanding this infeasibility, providers will still face strong incentives to engage in preemptive or overbroad content removal to mitigate legal risk, undermining freedom of expression while imposing disproportionate compliance burdens on foreign firms operating in Brazil, given their market share. This shift is particularly harmful to SMEs that rely on social media platforms and online marketplaces to access Brazilian consumers, a major customer base of U.S. firms.[123] These platforms offer low-cost, low-barrier entry points for SMEs lacking physical infrastructure or local business presence. However, with platforms now exposed to strict liability for third-party listings and communications, many may respond by tightening eligibility requirements, deactivating user-generated listings, or limiting access to foreign sellers altogether. Without the liability shield, the legal risk associated with hosting SME-generated content such as product descriptions, consumer reviews, and promotional materials shifts, incentivizing broad content takedowns or exclusion of smaller vendors. Moreover, the new legal framework requires providers to implement additional mechanisms, including due-process protocols, takedown systems, and annual transparency reporting, which impose additional operational and legal burdens, especially on non-domestic platforms that must navigate Brazil's evolving regulatory and judicial landscape remotely.

---

[122] Baker McKenzie. (2025, July 1). *Brazil: The Supreme Court (STF) establishes that Article 19 of the Brazilian Internet Legal Framework is partially unconstitutional, creating a new regime of civil liability*. https://insightplus.bakermckenzie.com/bm/intellectual-property/brazil-the-supreme-court-stf-establishes-that-article-19-of-the-brazilian-internet-legal-framework-is-partially-unconstitutional-creating-a-new-regime-of-civil-liability.

[123] Statista. (2025). *Most popular social media platforms in Brazil as of 3rd quarter 2024, by usage reach*. https://www.statista.com/statistics/1307747/social-networks-penetration-brazil/.

Brazil's Regulation for Conformity Assessment and Approval of Telecommunications Products establishes mandatory national certification requirements for telecommunications equipment prior to sale in the Brazilian market. On August 1, ANATEL adopted a revised conformity assessment framework,[124] citing the recent Supreme Federal Court decision on intermediary liability as the basis for expanding joint liability to online marketplaces and virtually any digital platform involved in the commercialization of telecommunications products, including platforms that merely advertise or facilitate product listings without participating in the sale or logistics chain.

This extremely broad interpretation could capture a wide range of digital services not traditionally viewed as part of the sales chain. Under the new rule, marketplaces and other digital commerce platforms must ensure that all telecommunications products they offer are certified and compliant with applicable standards. Obligations include verifying compliance, displaying certification codes, and preventing the sale of non-certified products. Failure to comply can result in penalties of up to R$50 million. U.S.-based marketplaces operating in Brazil now face heightened legal exposure for third-party sellers' compliance failures, including the obligation to verify ANATEL certification codes and ensure product conformity, tasks traditionally outside the platform's operational scope and technically difficult to implement at scale. By holding intermediaries, including platforms with no direct role in the sale, handling, or distribution of goods, jointly liable for the conformity of third-party products, Brazil's regime imposes disproportionate compliance burdens on digital commerce platforms. These provisions create significant legal uncertainty and risk, chilling participation in Brazil's online market, increasing compliance costs for international platforms, and creating barriers to entry for foreign firms seeking to operate in the Brazilian e-commerce ecosystem. Therefore, this framework raises serious concerns regarding proportionality, operational feasibility, and alignment with global digital trade principles, as it may not only restrict market access but also deter cross-border digital trade and innovation.

In September 2025, Brazil enacted landmark legislation establishing the Digital Child and Adolescent Statute,[125] creating a comprehensive legal framework to strengthen online safeguards for minors and imposing far-reaching obligations on digital platforms and services. Key requirements include robust age-verification mechanisms, effective parental control tools, and strict rules governing the processing of personal data and advertising directed at children and adolescents. Critically, the law mandates that any service likely to be accessed by minors must be designed with their best interests as the primary consideration, ensuring high levels of privacy

[124] *Resolução Anatel nº 780* [Brazil]. (2025). https://informacoes.anatel.gov.br/legislacao/resolucoes/2025/2054-resolucao-anatel-780.
[125] Baker McKenzie. (2025, September 22). *Brazil: Digital ECA (Brazil's Child and Adolescent Statute) - A new framework for online protection of children and adolescents*. https://insightplus.bakermckenzie.com/bm/data-technology/brazil-digital-eca-brazils-child-and-adolescent-statute-a-new-framework-for-online-protection-of-children-and-adolescents_2.

and safety by default. The government has moved quickly to accelerate implementation. A presidential decree shortened the compliance period from the original one year to just six months, and another decree designated the National Data Protection Authority (ANPD) as the primary enforcement authority for the statute. This expanded role will require the ANPD to ensure that data processing and content moderation practices fully align with the statute's heightened protections for minors. Given these developments, USTR should urge the reversal of the decree reducing the compliance period to allow a more realistic implementation timeline and closely monitor ANPD's enforcement activities and future regulatory guidance under the new framework.

Brazil is also advancing two major legislative proposals that could reshape the copyright framework for digital services and create new compliance and financial burdens for U.S. technology companies. The first, Bill 4968/24, introduced in the Senate in December 2024,[126] seeks to establish a new right to remuneration for copyright and related rights holders for content used by online platforms. Notably, the bill would require payment even in cases of unauthorized third-party uploads or where existing contractual agreements already allow use of the works, introducing substantial financial and operational risks for user-generated content platforms. In parallel, the Chamber of Deputies is advancing Bill 2370/19,[127] which mirrors many of the Senate bill's core provisions. This proposal would introduce new remuneration rights for journalistic and artistic content. It would also establish uncapped liability and "must-carry" obligations, effectively preventing platforms from removing content to avoid payment. Together, these initiatives could impose significant new costs, legal exposure, and content management burdens on digital platforms. USTR should closely monitor these legislative discussions and assess their potential impact on U.S. business interests.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

ANATEL in 2023 launched a public consultation regarding the regulation of "Value Added Services" (*e.g.*, internet services), including exploring the viability and appropriateness of network usage fees in Brazil.[128] The consultation sought input on whether there is a need for specific regulations targeted at large CAPs offering services over broadband networks, including

[126] *Projeto de Lei 4968* [Brazil]. (2022). https://legis.senado.leg.br/sdleg-getter/documento?dm=9879382&ts=1740076601466&disposition=inline.
[127] *Projeto de Lei 2370* [Brazil]. (2019). https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1734276&filename=PL%202370/2019.
[128] ANATEL. (2023, March 30). *Anatel abre tomada de subsídios sobre regulamentação de deveres dos usuários*. https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-abre-tomada-de-subsidios-sobre-regulamentacao-de-deveres-dos-usuarios; CCIA. (2023). *CCIA Submission to ANATEL*. https://ccianet.org/wp-content/uploads/2023/07/2023-CCIA-Submission-to-ANATEL-English.pdf.

new remuneration obligations.[129] A proposal to impose network usage fees on "large" companies would by definition discriminate against U.S. internet services, given their popularity in Brazil.

ANATEL issued a second consultation focused on network usage fees that concluded in May 2024[130] in which the agency reiterated many of the misguided arguments suggesting that remuneration schemes between online services providers and internet service providers are necessary and beneficial to the broader connectivity ecosystem.[131] The former Minister of Communications has publicly supported network usage fees and argued that ANATEL has the authority to impose them.[132] One ANATEL Commissioner has publicly expressed that he supports network usage fees,[133] and the ANATEL Chair has suggested that the agency will put forward network sustainability regulations in the coming years.[134]

On September 7, 2024, Sen. Angelo Coronel introduced Bill of Law 2804/2024,[135] which includes giving ANATEL authority to oversee a wide range of internet services and requires digital services suppliers to contribute 5% of their gross operating revenue in Brazil to the Universal Fund for Telecoms Services. The legislation avoids specific prescriptive mandates, but it does grant ANATEL with broad discretionary authority to set the definitions and draft rules. As such, the bill would empower ANATEL to require U.S. services providers to contribute to the telecommunications and transmissions infrastructure of Brazilian companies, some of which compete against these U.S. firms in the realm of content and streaming, even though the U.S. internet services do not have any direct access to or control over the infrastructure relevant to the Fund. As drafted, this law could violate the principle of competitive neutrality under the WTO's rules governing universal service, as Brazilian suppliers would receive preferential treatment at the expense of foreign suppliers that are unable to access the Fund (including through

[129] ANATEL. (2023). *Visualização da Tomada de Subsídios No. 13*. https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=2&ConsultaId=10120.
[130] ANATEL. (2024). *Visualização da Tomada de Subsídios No. 26*. https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=2&ConsultaId=20202.
[131] CCIA. (2024). *CCIA Submission to ANATEL on Connectivity Investment. https://ccianet.org/library/ccia-submission-to-anatel-on-connectivity-investment-english-version/.*
[132] Vasconcelos, E. (2023, October 3). Fair share deve criar ambiente justo e simétrico, defende ministro. *Tele.Sintese. https://www.telesintese.com.br/fair-share-deve-criar-ambiente-justo-e-simetrico-defende-ministro/.*
[133] Freire, A. & Campos, R. (2023, September 14). *Fair Share and Net Neutrality: What Is the Relationship?* Tele Time (Sept 14, 2023), https://teletime.com.br/14/09/2023/fair-share-e-neutralidade-de-rede-qual-a-relacao/; Alexandre Freire & Ricardo Campos, *Net neutrality and the new competitive dynamics of digital markets*, Tele Time (Mar. 10, 2023), https://teletime.com.br/04/10/2023/a-neutralidade-de-rede-e-as-novas-dinamicas-concorrenciais-dos-mercados-digitais.
[134] *Anatel Will Not Mention Cost-sharing With Big Techs Says President*, Valor (Sept. 12, 2023), https://valor.globo.com/empresas/noticia/2023/09/12/anatel-nao-vai-se-omitir-sobre-compartilhamento-de-custo-com-big-techs-diz-presidente.ghtml; Miriam Aquino, *Can big techs be blocked for abusive use of networks?* Tele.Sintese (Oct. 3, 2023), https://www.telesintese.com.br/big-techs-podem-ser-bloqueadas-por-uso-abusivo-das-redes/.
[135] Bill of Law 2804/2024 (Sept. 7, 2024), https://legis.senado.leg.br/sdleg-getter/documento?dm=9697364&ts=1726059294378&rendition_principal=S&disposition=inline.

affiliates).[136] CCIA urges USTR to remain vigilant as Brazil continues to pursue network usage fees and misguided universal service mandates. Industry appreciates USTR's consistent work pushing back on similar efforts in South Korea and the European Union, and urges similar engagement with Brazil.

On August 1st, 2025, ANATEL approved Resolution No. 780/2025, which revised the Regulation on Conformity Assessment and Homologation of Telecommunications Products.[137] The new regulation imposes numerous requirements on data centers including: (1) mandatory conformity assessment and homologation as a prerequisite for installation or contracting by telecommunications service providers; (2) operational resilience to ensure continuity of service during failures or disasters; (3) physical security measures to prevent unauthorized access and mitigate internal and external threats; (4) robust cybersecurity protections against intrusions and attacks; and (5) energy efficiency and environmental sustainability measures, applying best practices and technologies to reduce consumption. ANATEL's technical staff must issue a new operational procedure within 240 days detailing the conformity assessment process, including deadlines for compliance. Existing data centers will have a three-year transition period to meet the new requirements. These new requirements, introduced directly by ANATEL's Board of Directors during deliberations, were neither subject to public consultation nor supported by a regulatory impact assessment, as ordinarily required under ANATEL's own procedures. Moreover, the rule's vague and expansive language could be interpreted to cover a far broader range of data center operators than just telecom service providers, enabling ANATEL to assert authority over large segments of the digital infrastructure ecosystem. While objectives such as operational resilience, physical security, cybersecurity, and sustainability are important, requirements developed for transmission networks are not directly applicable to data centers, and extending them in a blanket fashion creates significant regulatory uncertainty as to their applicability. Given substantial U.S. investments in Brazilian data centers, such measures risk operating as a burdensome trade practice that undermines market access for U.S. firms and impedes cross-border digital services.

In addition, ANATEL is in the process of broadening its regulatory oversight, seeking to extend its authority beyond traditional legacy telecommunications. In 2025, ANATEL launched consultations to bring AI systems and data centers under its authority,[138] both of which would subject these services to new legal obligations and any relevant guidelines issued by the agency. The inclusion of AI systems is especially unusual, since such "value-added-services" have

[136] WTO, *Negotiating Group on Basic Telecommunications* (Apr. 26, 1996), https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm#top.
[137] *Resolução Anatel nº 780* [Brazil]. (2025). https://informacoes.anatel.gov.br/legislacao/resolucoes/2025/2054-resolucao-anatel-780.
[138] *CONSULTA PÚBLICA Nº 31* [Brazil]. (2025). https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=2&ConsultaId=20333; *CONSULTA PÚBLICA Nº 32* [Brazil]. (2025). https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=2&ConsultaId=20334.

traditionally been exempt from ANATEL's regulatory purview, whose focus to date has been limited to transmission systems.

Potential Challenges to the Development of AI

On May 12, 2023, Bill No. 2338 was introduced in the Brazilian Senate to establish a regulatory framework for AI technologies.[139] The bill outlines requirements for the operation of AI systems in Brazil, including mandatory risk assessments and risk-based classification of AI applications, and poses numerous concerns. First, it fails to distinguish between the responsibilities of AI developers and deployers, adding further ambiguity to its scope. Second, it introduces expansive copyright provisions that would require developers to compensate Brazilian content owners for any data used to train AI models, even though AI models extract and replicate unprotectable facts and patterns rather than protected expression. Foundational AI models need massive, diverse datasets, and excluding individual pieces of data does not materially affect model performance, making licensing not only unfeasible but also unnecessary, especially given the effectiveness of existing opt-out protocols such as robots.txt. Third, it designates the ANPD as the primary AI regulator, tasked with coordinating sectoral regulators and issuing rules for "unregulated sectors" which might include social media, since content recommendation systems are increasingly driven by AI. This creates uncertainty due to overlaps between the LGPD and the proposed AI framework. In 2024, the ANPD launched AI-related investigations against U.S. and foreign tech firms, sometimes issuing preemptive blocking orders, reflecting a restrictive, EU-inspired approach that risks stifling innovation. The ANPD is expected to issue secondary rules on AI and data protection in late 2025, and, if the AI Bill is enacted, will expand its rulemaking to AI regulation more broadly. Given the scale and global nature of U.S.-developed AI systems, these vague and far-reaching obligations could disproportionately impact U.S. firms operating in or serving the Brazilian market.

Restrictions on Cross-Border Data Flows

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.[140] 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.[141] Further, the LGPD does not permit cross-border data transfers based on the controller's legitimate interests, but rather lists ten specific instances in

---

[139] *Bill No. 2338* [Brazil]. (2023). https://legis.senado.leg.br/sdleggetter/documento?dm=9347622&ts=1683827933990&disposition=inline&_gl=1*gdi95o*_ga*ODMxNzgxMDUzLjE2ODAxMDM2NTc.*_ga_CW3ZH25XMK*MTY4NDI1MDY2OS4xLjAuMTY4NDI1MDY2OS4wLjAuMA.

[140] *General Personal Data Protection Act* [Brazil]. (2018). https://lgpd-brazil.info/.

[141] Locker, E., & Navetta, D. (2018, September 18). Brazil's new data protection law: The LGPD. *Cooley Policy & Legislation.* https://cdp.cooley.com/brazils-new-data-protection-law-the-lgpd.

which cross-border data transfer under the LGPD is permitted.[142] 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 with overseeing standard contractual clauses, before any data is authorized to be transferred abroad.[143]

On August 23, 2024 the ANPD published the International Transfer of Personal Data Regulation.[144] The regulation implements a framework to identify jurisdictions deemed to have adequate privacy protections for the transfer of data, with the ANPD requiring "equivalence in the level of personal data protection"—a regime similar or comparable to the LGPD, while not needing to be identical.[145] The regulation allows for the use of standard contractual clauses (SCCs) in four categories: general information, mandatory clauses, security measures, and additional clauses and annexes. The ANPD can certify foreign SCCs as adequate but the ANPD board must approve and publish SCCs and their applicability to Brazil's SCCs before they enter effect. To date, many aspects of this framework remain incomplete. However, the regulation explicitly states that the international collection of personal data (such as personal data from a subject carried out directly by a foreign processing agent) does not constitute an international data transfer.

In October 2025, Brazil's Ministry of Development, Industry, Commerce and Services began developing a national policy and legal framework for the "data economy," aimed at regulating the use and flow of non-personal data. The proposal, modeled on the EU's Data Act, seeks to establish rules for non-personal data sharing in B2G and B2B contexts, complementing the personal data framework under Brazil's LGPD. A public consultation is expected by the end of 2025 to shape the framework, focusing on issues such as data portability, the creation of sectoral data spaces (e.g., Open Finance), and mechanisms to encourage data access and re-use. While the initiative is presented as a step toward regulatory alignment with the EU, the legislation could disproportionately impact large U.S. technology companies, particularly if thresholds based on market share, revenue, or user base are set to target global players while exempting domestic firms. Provisions on mandatory data sharing raise particular alarm, as they could result in forced transfers of proprietary information and act as non-tariff trade barriers, undermining foreign competitiveness and signaling potential protectionist applications of the framework.

As Brazil implements these regulations, USTR should monitor to make sure the rules align with international norms that facilitate the free and fair flow of data that underpins U.S. digital

[142] Brook, C. (2019, June 10). Breaking down LGPD, Brazil's new data protection law. *Data Insider.* https://www.digitalguardian.com/blog/breaking-down-lgpd-brazils-new-data-protection-law.
[143] Greenberg Traurig. (2020, August 28). Brazil's data protection law will be effective after all, but enforcement provisions delayed until August 2021. *Greenberg Traurig.* https://www.gtlaw.com/en/insights/2020/8/brazils-data-protection-law-effective-enforcement-provisions-delayed-august-2021.
[144] Brazil Data Protection Agency. (2024, August 23). *International transfer of personal data regulation.* https://www.gov.br/anpd/pt-br/assuntos/noticias/resolucao-normatiza-transferencia-internacional-de-dados.
[145] Bousso, F., & Kasputis, M. B. (2024, September 4). Brazil's new regulation on international data transfers. *IAPP.* https://iapp.org/news/a/brazil-s-new-regulation-on-international-data-transfers.

services exports and should urge Brazil to deem privacy protections available in the United States as adequate under Brazilian law.

Taxation of Digital Products and Services

On September 5, 2024 Sen. Flavio Azevedo issued a request to the Minister of Finance to initiate more aggressive taxation of big technology companies.[146] On October 3, 2024, Brazil's Ministry of Finance issued Provisional Measure No. 1,262/24,[147] a 15% minimum tax on multinationals operating in Brazil. Brazil described this as a Social Contribution on Net Profit, ostensibly in line with the OECD's Pillar II scheme. It will require implementing legislation, and deserves careful monitoring for consistency with OECD principles and WTO non-discrimination obligations. Despite reporting that the government has abandoned such plans,[148] CCIA asks USTR to remain watchful of Brazil's actions on this matter, as the government appears intent on seeking new revenue streams for its coffers by disproportionately taxing foreign corporations.[149] Sen. Azevedo asked the Minister of Finance to determine if there was a basis for imposing new taxes solely on digital platforms--mirroring DSTs imposed elsewhere.

Brazil's financial transaction tax, or Imposto sobre Operações Financeiras (IOF), is a federal tax applied to a broad range of financial transactions.[150] On May 23, 2025, the government enacted Decree No. 12,466 modifying the IOF, including by raising the rate on foreign exchange operations from .38% to 3.5%. Foreign exchange operations affected include transactions using credit and debit cards abroad, purchases of foreign currencies, foreign repaid cards, cross-border remittances, and traveler's checks. This policy shift is particularly notable given that Brazil had previously committed as part of its OECD accession plan to fully eliminate the IOF on foreign exchange operations. The revised IOF regime imposes a significant new barrier to cross-border digital trade and electronic payment services. By raising the IOF rate on foreign exchange operations to 3.5%, Brazil has substantially increased the cost of international financial transactions, directly affecting U.S. firms engaged in cross-border delivery of digital services, SaaS, e-commerce, and electronic payments by making it more expensive for Brazilian consumers and businesses to engage in transactions involving U.S.-based providers. Since foreign firms inevitably have to engage in foreign exchange transactions, this additional burden

---

[146] *Letter to the Minister of Finance from the Office of Sen. Flavio Azevedo* [Federative Republic of Brazil]. (2024, September 5). https://legis.senado.leg.br/sdleg-getter/documento?dm=9800288&ts=1725570407029&disposition=inline.

[147] *Provisional Measure No. 1,262* [Brazil]. (2024). https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.262-de-3-de-outubro-de-2024-588158201.

[148] Ayres, M. & Caram, B. (2025, March 26). Brazil holds off big tech tax amid Trump tariff talks, say sources. *Reuters*. https://www.reuters.com/technology/brazil-holds-off-big-tech-tax-amid-trump-tariff-talks-say-sources-2025-03-26/.

[149] Reuters. (2024, September 2). Brazil's government considers taxing Big Techs if revenue falls short. *Reuters.* https://www.reuters.com/world/americas/brazils-government-considers-taxing-big-techs-if-revenue-falls-short-2024-09-02/.

[150] *LEI No 5.143* [Brazil]. https://www.planalto.gov.br/ccivil_03/LEIS/L5143.htm#art1.

puts cross-border suppliers at a significant competitive disadvantage as compared to domestic suppliers–i.e., a form of discrimination. This regime functions as a financial restriction on trade in services, and one that appears inconsistent with trade rules designed to prevent such outcomes. While Brazil has not undertaken GATS commitments in certain relevant sectors (e.g., audiovisual or video services), the principle underlying GATS Article XI (Payments and Transfers) is directly implicated. GATS Article XI prohibits restrictions on international transfers and payments for current transactions where commitments exist, and although not legally binding in uncommitted sectors, the IOF reform exemplifies the kind of barrier the multilateral framework was intended to prevent.

CIDE Royalties (Law 10,168/2000), currently levied at a 10% rate on payments, credits, use, or remittances made by a Brazilian source for royalties, licenses, and technical services provided by non-residents,[151] significantly increases the cost of U.S. companies operating in Brazil, especially those conducting cross-border technology transfers. A case challenging the validity of the CIDE Royalties is currently pending before Brazil's Supreme Court, on the grounds that the tax's stated purpose, supporting technological development in Brazil, is not reflected in the actual allocation of the collected revenue. Notably, the tax is also listed in the Reciprocation Law (Law 15,122/2025, Art. 10) as a potential retaliatory measure the Brazilian government may apply against companies from countries that adopt unilateral measures against Brazil.[152] When combined with other levies such as the IOF, the result is often a doubling of taxes on the same revenue stream. This overlapping and cumulative taxation structure creates an excessively burdensome fiscal environment, undermines tax equity and neutrality, and places the digital economy at a competitive disadvantage compared to other industries.

On August 1, 2024, new taxation rules for e-commerce imports entered into force. The rules place a 20% tax on purchases up to $50, and a 60% tax on items valued between $50.01 and $3,000.[153] Since this tax, applicable only to imports, is higher than comparable domestic taxes, it could be inconsistent with Brazil's GATT obligations. USTR is urged to engage with Brazil to determine its GATT consistency.

Other Barriers to Digital Trade

In October 2025, Brazil's Central Bank came under increased scrutiny for its dual role as both regulator and market participant through its operation of Pix, the government-run instant payment system.[154] This mix of roles creates a significant competitive disadvantage for foreign

[151] *LEI No 10.168* [Brazil]. (2000). https://www.planalto.gov.br/ccivil_03/leis/L10168.htm.
[152] *LEI Nº 15.122* [Brazil]. (2025). https://www.in.gov.br/en/web/dou/-/lei-n-15.122-de-11-de-abril-de-2025-623734149.
[153] Ministry of Finance. (2024, June 28). *Federal revenue implements new rules for imports via e-commerce.* https://www.gov.br/fazenda/pt-br/assuntos/noticias/2024/junho/receita-federal-implementa-novas-regras-para-as-importacoes-por-e-commerce.
[154] Trachtenberg, D. (2025). *Section 301 Investigation into Brazil's Acts, Policies, and Practices*. Congressional Research Service. https://www.congress.gov/crs-product/IN12613.

fintech providers. Private payment providers are subject to technical standards, cybersecurity protocols, and supervisory fees that do not apply to Pix, giving the state-run system an undue market advantage. In addition, the Brazilian government mandates the integration of Pix into retail payment networks, further entrenching Pix's dominant market position and constraining opportunities for commercial growth for U.S. providers of digital payment and digital wallet services. This bias is compounded by the lack of regulatory and operational separation between Pix and the Central Bank, which allows the state to shape the market in ways that undermine fair competition.

Further reinforcing these concerns, a bill (2141/2025) was introduced in October 2025 in Brazil's lower house that would require all device manufacturers and operating system providers to grant access to Near Field Communication (NFC) technology for Pix transactions to any financial institution authorized by the Central Bank.[155] This measure not only creates technical and cybersecurity risks, but also undermines intellectual property and investment protections by depriving companies of the ability to receive fair, reasonable, and non-discriminatory (FRAND) remuneration for their technology and platforms. These developments risk distorting Brazil's payments ecosystem, limiting innovation, and creating barriers to market access for U.S. fintech and technology companies.

Cambodia

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Cambodia's 2022-2035 Digital Policy Agenda[156] contains a number of proposed regulations relating to privacy[157] and cybersecurity[158] that would require data localization. While the policy aims to accelerate digital transformation and promote cloud adoption in the public sector, its mandates on data localization, particularly for confidential data, and strict data sovereignty provisions, though intended to protect national interests, introduce significant operational complexities and limitations. The policy requires that confidential data, including categories such as government-classified information, personally identifiable information, and financial data, be stored or processed exclusively within in-country infrastructure operated by an MPTC-accredited cloud service provider or the government cloud. By restricting the storage of data connected to domestic infrastructure, the policy effectively prevents ministries and institutions from leveraging the scale, flexibility, and cost efficiencies of global public cloud providers.

---

[155] *Projeto de Lei 2141/2025* [Brazil]. (2025). https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2504778.
[156] Cambodian Ministry of Post and Telecommunications. (2022). *Cambodia Digital Government Policy*. https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf.
[157] Chng, D. G. (2025, July 26). *Draft Law on Personal Data Protection*. DGC Briefings. https://dgcbriefings.substack.com/p/cambodia-draft-law-on-personal-data.
[158] Access Now. (2023). *Legal Analysis: Cambodia Draft Law on Cybersecurity*. https://www.accessnow.org/wp-content/uploads/2023/10/Legal-Analysis-Cambodia-Cybersecurity-Draft-Law-Final-29-Sept.pdf.

Government-Imposed Content Restrictions and Related Access Barriers

Reports of censorship and mandated internet filtering and blocking continue to persist in Cambodia.[159] Independent outlets have been blocked, often coinciding with politically sensitive moments, such as the July 2023 general elections, when critical news sources were taken offline while pro-government media remained accessible. Beyond news sites, the government has also used threats of legal action and forced public apologies to silence critical voices in digital spaces.

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.[160] As noted by the State Department's most recent investment analysis from April 2024, "the MOC and MEF issued notification number 837 requiring all companies operating in Cambodia to use a national second-level domain name (.com.kh) as well as an email address with the national second-level domain name when filing annual declarations of commercial enterprises."[161] While the specifics of the implementation remain unclear, there is potential that this could be abused to block online content and keep out certain foreign digital services, akin to China's "Great Firewall.[162]

Cambodia's Interior Ministry is developing a draft Cybercrime bill that could hold intermediaries liable for third party content.[163] The bill also contemplates new data localization mandates. 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.[164] Although not yet finalized, reports indicate that the government is targeting completion of the bill by the end of 2025.[165] The latest draft was not public but reportedly included provisions prohibiting defamation, using "insulting, derogatory or rude language," and sharing "false information" that

---

[159] Freedom House. (2024). *Freedom on the Net 2024: Cambodia*. https://freedomhouse.org/country/cambodia/freedom-net/2024.
[160] Thul, P. K. (2021, February 18). Cambodia's new China-style internet gateway decried as repression tool. *Reuters*. https://www.reuters.com/article/us-cambodia-internet/cambodias-new-china-style-internet-gateway-decried-as-repression-tool-idUSKBN2AI140.
[161] U.S. Department of State. (2024). *2024 Investment Climate Statement: Cambodia*. https://www.state.gov/reports/2024-investment-climate-statements/cambodia/.
[162] Human Rights Watch. (2021, February 18). *Cambodia: Internet Censorship, Control Expanded*. https://www.hrw.org/news/2021/02/18/cambodia-internet-censorship-control-expanded; Wan, A. & Mok, C. (2022, February 18). *Internet Impact Brief: Cambodia National Internet Gateway*. Internet Society. https://www.internetsociety.org/resources/2022/internet-impact-brief-cambodia-national-internet-gateway/.
[163] Sun, N. (2020, October 11). Activists: Cambodia's Draft Cybercrime Law Imperils Free Expression, Privacy. *VOA*. https://www.voanews.com/a/east-asia-pacific_activists-cambodias-draft-cybercrime-law-imperils-free-expression-privacy/6196959.html.
[164] Kelliher, F. (2023, March 10). Leaked Law Proposal Would Give Cambodia Expanded Powers to Censor Critics. *Rest of World*. https://restofworld.org/2023/cybersecurity-law-draft-cambodia-elections/.
[165] Sikol, K. (2025, February 9). PM Urges to Push Draft Cybersecurity Law. *KiriPost*. https://kiripost.com/stories/pm-urges-to-push-draft-cybersecurity-law.

could harm Cambodia's public order and "traditional culture."[166] These terms are ill-defined and the punishments for violations include fines and imprisonment. The law would also permit the government to gather and record internet traffic data of individuals suspected of committing crimes and would criminalize online material that "depicts any act or activity … intended to stimulate sexual desire."

Restrictions on Cross Border Data Flows

Cambodia released a draft Law on Personal Data Protection (LPDP) on July 23, 2025,[167] modeled in part on the EU's GDPR. The draft introduces rules governing data processing, establishes data subject rights such as access and erasure, requires the appointment of a Data Protection Officer for certain organizations, and provides for administrative fines in cases of non-compliance. It applies to both domestic and foreign entities processing the personal data of individuals in Cambodia, with a proposed two-year implementation period following enactment. Several provisions in the LPDP deviate from international best practices, creating an unpredictable and burdensome compliance environment that could pose significant barriers for U.S. service providers seeking to operate in the Cambodian market. The law would impose administrative fines of up to 10 percent of annual turnover, far exceeding global norms and not clearly tied to the turnover related to the specific violation, creating significant financial risk. It also includes rigid compliance timelines, such as requiring "immediate" action upon consent withdrawal and mandating notification of data breaches within 72 hours of merely becoming aware of an incident, timelines that are often impractical in complex operational settings. In addition, the right to erasure is drafted broadly, without a balancing test to protect freedom of expression and without precluding private rights of action, which could lead to inconsistent enforcement and excessive litigation. Finally, the high age of consent—set at 16—diverges from the widely accepted international standard of 13 and could limit teenagers' access to online services.

Canada

Asymmetric Platform Regulation

On November 24, 2022, the Canadian Government opened a consultation seeking feedback on its initiative to update the Canadian Competition Act.[168] The consultation specifically requests public comment on data and digital markets, asking whether "sector-specific mechanisms"

---

[166] Sikol, K. (2025, February 9). PM Urges to Push Draft Cybersecurity Law. *KiriPost*. https://kiripost.com/stories/pm-urges-to-push-draft-cybersecurity-law.
[167] *Draft Law on Personal Data Protection* [Cambodia]. (2022). https://data.opendevelopmentcambodia.net/laws_record/draft-law-on-personal-data-protection.
[168] Innovation, Science and Economic Development Canada. (n.d.). *Consultation on the future of competition policy in Canada*. 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/.

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.[169] 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." While the Competition Act has undergone several amendments recently, asymmetric regulation targeting digital service suppliers has not yet been proposed.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

On August 22, 2025, Shared Services Canada (SSC) initiated a consultation under its Canadian Sovereign Cloud Services initiative to inform the development of a sovereign procurement stream for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).[170] The framework would mandate that all government data be processed, transmitted, and stored exclusively in Canada, and that providers, including their ultimate parent companies, not be subject to foreign laws that could permit external government access, essentially, any foreign-domiciled firm. SSC has invoked the National Security Exception as a means of exempting this procurement from Canada's obligations under WTO and other trade agreements that preclude discriminatory treatment of foreign suppliers. Canada's proposed requirements raise significant concerns. Conditioning participation on ownership structures and jurisdictional control, rather than on technical capacity or security standards, effectively excludes U.S. cloud providers from competing on fair terms.[171] CCIA urges USTR to engage proactively with the Government of Canada to ensure that this initiative does not evolve into a discriminatory barrier to trade and to safeguard the ability of U.S. cloud and digital service providers to compete fairly in the Canadian market.

Discriminatory Local Content Quotas and Audiovisual Mandates

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

[169] Innovation, Science and Economic Development Canada. (2022). *The Future of Competition Policy in Canada*. https://ised-isde.canada.ca/site/strategic-policy-sector/sites/default/files/attachments/2022/The-Future-of-Competition-Policy-eng_0.pdf.
[170] Shared Services Canada. (2025, August 13). *Request for Information – Sovereign Public Cloud Capability*. https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/cb-416-17296820.
[171] CCIA. (2025, September 29). *Canada's Sovereign Cloud Initiative*. https://ccianet.org/library/canadas-sovereign-cloud-initiative/.

and creators.[172] 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."

The CRTC's implementing framework makes clear that all video and audio streaming services with more than C$25 million in annual subscription and advertising revenue are in scope of the Canadian content obligation. In its June 2024 policy document, the CRTC exempted Canadian-affiliated streaming players tied to domestic broadcasters, but imposed obligations on all other providers, video and audio alike.[173] Revenues from user-generated content, audiobooks, podcasts, and video game services are excluded, but subscription, advertising, and transactional video-on-demand revenues are included. The obligation currently stands at 5% of Canadian gross subscription and advertising revenue, though the CRTC has indicated it intends to raise this requirement to 20% or even 30% of revenues over time.[174]

These measures will fall overwhelmingly on U.S. suppliers. Excluding user-generated content, Canada's streaming video market was valued at US$5.73 billion at the end of 2025, with U.S. providers estimated to hold the majority of market share.[175] At an initial 5% contribution rate, U.S. streaming services will be compelled to fund approximately US$2.19 billion between 2025 and 2030. Should the rate increase to 20% as the CRTC has signaled, the cumulative burden could rise to US$6.95 billion, with no sunset to these measures.[176] These obligations are discriminatory, onerous, and inconsistent with USMCA Articles 19.4 (non-discriminatory treatment of digital products), 15.3.1 (cross-border trade in services), and 14.10.1(b) (performance requirements).[177]

The CRTC has compounded uncertainty by imposing contribution obligations before updating the definition of Canadian content. Existing broadcasting definitions, which require IP ownership by Canadian entities, effectively disincentivize foreign investment in production. If extended to

---

[172] *An Act to amend the Broadcasting Act and to make related and consequential amendments to other Acts* [Canada] Bill C-11. (2021). https://www.parl.ca/DocumentViewer/en/44-1/bill/C-11/royal-assent.
[173] Canadian Radio-television and Telecommunications Commission. (2024, June 4). *Broadcasting Regulatory Policy CRTC 2024-121.* https://crtc.gc.ca/eng/archive/2024/2024-121.htm.
[174] Canadian Radio-television and Telecommunications Commission. (2024, June 4). *Broadcasting Regulatory Policy CRTC 2024-121.* https://crtc.gc.ca/eng/archive/2024/2024-121.htm.
[175] Gaines, B. (2025, October 3). *Streaming Service Market Share (2025): Revenue Data & Trends*. Evoca TV. https://evoca.tv/streaming-service-market-share; *BNN Bloomberg*. (2025, March 24). 'TV is becoming niche': Streaming grows in Canada despite rising prices, report says. https://www.bnnbloomberg.ca/business/technology/2025/03/24/tv-is-becoming-niche-streaming-grows-in-canada-despite-rising-prices-report-says/.
[176] CCIA. (2025). *Canada's Requirement to Force U.S. Companies to Fund Local Music and Video Content Could Cost the U.S. Industry $7 Billion by 2030*. https://ccianet.org/wp-content/uploads/2025/09/Cost-of-Canadas-Online-Streaming-Act.pdf.
[177] CCIA. (2024, June 14). *CCIA Comments on Canada's Obligatory Base Contribution for Streaming Suppliers.* https://ccianet.org/library/ccia-comments-on-canadas-obligatory-base-contribution-for-streaming-suppliers/.

online services, as envisaged in the Act, these requirements could significantly reduce foreign participation in Canada's creative sector and limit consumer choice by shrinking content libraries. The CRTC only began rulemaking on a new definition of Canadian content in January 2025, creating uncertainty as to whether current investments by streaming providers might already qualify.[178]

In parallel, the Act directs the CRTC to ensure the "discoverability" of Canadian programming, raising the prospect of interference in content curation and recommendation systems. Such obligations would undermine recommendation engines that expose consumers to a broad range of content, harming both creators and audiences. While drafters of the Act and Canadian Heritage's directive sought to exclude user-generated content,[179] the CRTC has ignored this guidance. It ruled in September 2023 that it was "neither necessary nor appropriate" to exempt social media platforms from registration, obligating them to register as broadcasters and pay regulatory fees despite not being within scope.[180] This approach risks intrusive regulation of user-generated content, creating uncertainty for foreign suppliers and content creators alike.

Representatives from Canada's creative sector, academia, public interest groups, and the streaming industry have opposed the Act, citing its discriminatory impact and inconsistency with USMCA obligations.[181] CCIA urges USTR to actively oppose implementation of these measures and not to avoid its statutory obligation under USMCA's implementing legislation to evaluate discriminatory measures pursued under the cultural industries exception and consider a proportionate response. A pause in implementation, and ultimately rescission of the Online Streaming Act, is warranted to prevent lasting harm to U.S. suppliers, Canadian consumers, and the broader digital economy.

---

[178] Canadian Radio-television and Telecommunications Commission. (n.d.). *Regulatory Plan to Modernize Canada's Broadcasting Framework*. https://crtc.gc.ca/eng/industr/modern/plan.htm.
[179] Canadian Heritage. (2023, June 28). *Government of Canada Outlines Proposed Directions for the Online Streaming Act to Set the Stage for Equitable, Flexible and Adaptable Regulation*. https://www.canada.ca/en/canadian-heritage/news/2023/06/government-of-canada-outlines-proposed-directions-for-the-online-streaming-act-to-set-the-stage-for-equitable-flexible-and-adaptable-regulation.html.
[180] Canadian Radio-television and Telecommunications Commission. (2023, September 29). *Broadcasting Regulatory Policy CRTC 2023-329 and Broadcasting Order CRTC 2023-330.* https://crtc.gc.ca/eng/archive/2023/2023-329.htm.
[181] YouTube Creators [@youtubecreators]. (2022, June 6). *Canada's Bill C-11: What it could mean for Creators and discoverability on YouTube* [Video]. YouTube. https://www.youtube.com/watch?v=pKEGnAo4Eqg; Geist, M. [@michaelallengeist]. (2022, June 21). *Michael Geist opening statement on Bill C-11* [Video]. YouTube. https://www.youtube.com/watch?v=TovmyFfZqIU; Bhullar, R. (2022, September 28). *What's wrong with Bill C-11? An FAQ*. OpenMedia. https://openmedia.org/article/item/whats-wrong-with-bill-c-11-an-faq; Patell, J. (2022, June 22). *An Update from YouTube Canada on the Online Streaming Act*. Google. https://blog.google/intl/en-ca/company-news/outreach-initiatives/an-update-from-youtube-canada-on-the-online-streaming-act/.

Forced Revenue Transfers for Digital News

In April 2022, Canadian Heritage introduced Bill C-18, the Online News Act,[182] which would empower the Canadian Radio-television and Telecommunications Commission ("CRTC") to compel large "digital news intermediaries" to pay groups of news publishers for *any* reproduction of *any* piece of news content on their services, including headlines, quotes, and links. The legislation received Royal Assent and became law on June 22, 2023, with substantive obligations coming into effect on December 19, 2024.

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. Notwithstanding facially neutral criteria, Bill C-18 targets specific U.S. companies, as is evident from statements made by Canadian lawmakers. 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.[183] 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—was estimated to 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.[184] The estimates perpetuate concerns that the law would forcibly transfer revenue from U.S. digital services firms to shore up Canada's already highly concentrated media sector. Canadian Heritage's draft implementing regulations [185] 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.[186]

The implementing 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

---

[182] *An Act respecting online communications platforms that make news content available to persons in Canada* [Canada] Bill C-18. (2022). https://www.parl.ca/DocumentViewer/en/44-1/bill/C-18/first-reading.
[183] Canadian House of Commons. (2022, May 13). *Debate of the House of Commons, 44th Parliament, 1st Session* [Parliamentary Debate Transcript]. https://www.ourcommons.ca/DocumentViewer/en/44-1/house/sitting-71/hansard#11685803.
[184] Tossou, R. K. (2022). *Cost Estimate for Bill C-18: Online News Act. Office of the Parliamentary Budget Officer*. https://www.pbo-dpb.ca/en/publications/RP-2223-017-M--cost-estimate-bill-c-18-online-news-act--estimation-couts-lies-projet-loi-c-18-loi-nouvelles-ligne.
[185] *Regulations Respecting the Application of the Online News Act, the Duty to Notify and the Request for Exemptions* [Canada] Part 1, Vol. 157, No. 35. (2023). https://gazette.gc.ca/rp-pr/p1/2023/2023-09-02/html/reg1-eng.html.
[186] Deschamps, T. (2023, September 1). Online News Act could see Google, Meta Pay Combined $230 Million to Canadian Media. *CTV News.* https://www.ctvnews.ca/canada/online-news-act-could-see-google-meta-pay-combined-234-million-to-canadian-media-1.6544576.

exemption from the law. This requirement reflects how the purported goal of the legislation has instead devolved into an arbitrary, extractive tax. The government expected that the targeted two companies would pay a combined total of at least C$234 million annually to news businesses to be able to continue operating in the market with news links and sharing on their platforms.

The long-term viability of this law is now in question. One of the U.S. companies subjected to the law obtained a five-year exemption from the law in October 2024, after agreeing to pay C$100 million annually to Canadian news organizations;[187] and the second U.S. company ceased hosting links to news content in Canada. Even if not fully tested, the law remains an incipient threat to U.S. companies and is the government's leverage to extract fees. The law has already resulted in harms to the internet landscape and consumers in Canada. As detailed by the Internet Society: "Canada's 2023 passage of the Online News Act shows that these laws not only fail to help the sustainability of the news industry but also disrupt people's access to the open Internet, threaten security and safety, and reinforce the dominance of large platforms."[188] Absent repeal, this law still conflicts with several of Canada's international trade obligations, so USTR should remain vigilant of action against these two U.S. companies and any others they may seek to scope into the law. Other U.S. companies that link to news articles (e.g. Microsoft's Bing) could still come under consideration by the CRTC or Canadian Heritage. The fact that the popular Chinese social media service TikTok is not subject to this law, despite a clear role in news distribution[189] raises clear MFN issues under both USMCA and the GATS. 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 WTO's absorption of the Berne Convention and the right to quotation in the Agreement on Trade-Related Aspects of Intellectual Property Rights.[190]

In August 2025, Prime Minister Mark Carney acknowledged the shortcomings of the Online News Act, suggesting that the government may seek to amend or repeal the law in light of its disruptive impact on the dissemination of news and information online. While reaffirming support for local journalism, he noted that the government would "look for all avenues" to ensure

---

[187] Canadian Radio-television and Telecommunications Commission. (2024, October 28). *CRTC approves Google's application and paves way for annual $100 million contribution to Canadian news organizations*. https://www.canada.ca/en/radio-television-telecommunications/news/2024/10/crtc-approves-googles-application-and-paves-way-for-annual-100-million-contribution-to-canadian-news-organizations.html.

[188] Internet Society. (2024). *Case Study: Canada's Online News Act Hurt Journalism, Competition, and the Internet*. https://www.internetsociety.org/resources/doc/2024/case-study-canadas-online-news-act-hurt-journalism-competition-and-the-internet/.

[189] Krichel, S. (2023, October 11). TikTok's Awkward Dance with Canadian Journalism. *The Tyee*. https://thetyee.ca/News/2023/10/11/TikTok-Awkward-Dance-Canadian-Journalism/.

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

its wide and timely distribution.[191] This admission underscores how the law has failed to achieve its stated objectives and instead imposed harmful consequences on digital services, Canadian consumers, and the open internet. CCIA will continue to monitor developments closely and urges USTR to maintain pressure on Canada to withdraw or substantially revise the measure in order to bring it into compliance with international trade obligations.

Government Imposed Restrictions on Internet Content and Related Access Barriers

In 2021, Canada announced a framework to "address harmful content online," proposing 24-hour takedown requirements, monitoring, filtering, and site-blocking,[192] raising concerns about censorship, overbroad definitions of "harmful" content, and limited stakeholder input. On February 26, 2025, the government introduced the *Online Harms Act*, Canada's first federal content moderation regime, which defines harmful content such as hate speech, incitement to violence, and cyberbullying, and imposes strict obligations on social media platforms, including 24-hour deadlines for removal of flagged child exploitation and non-consensual intimate content.[193] The bill would establish a powerful Digital Safety Commission empowered to issue codes of conduct, impose fines of up to 6% of global revenue, conduct inspections, and potentially require company funding, while raising concerns about encryption through possible scanning mandates that could extend to services like file transfers and cloud storage. In parallel, the Conservative Party has advanced an alternative bill (C-412, *Protection of Minors in the Digital Age Act*), which would impose "duty of care" obligations, mandate parental controls, authorize private rights of action for "serious harm" (broadly defined), and prohibit certain interface or algorithmic designs deemed to impair user autonomy,[194] creating risks of over-enforcement, frivolous lawsuits, and constraints on content moderation. While the proposals failed to advance and expired on the Order Paper, the new Liberal government announced its intention in June 2025 to revive the effort and expand it to address developments in AI.[195]

Additionally, the Office of the Privacy Commissioner of Canada (OPC) recently concluded its exploratory consultation on age assurance, which ran from June to September 2024, and is now

[191] Nardi, C. (2025, August 5). Carney suggests he's considering rescinding Online News Act. *National Post*. https://nationalpost.com/news/politics/carney-suggests-hes-considering-rescinding-online-news-act.
[192] Canadian Heritage. (n.d.). *Have your say: The Government's proposed approach to address harmful content online*. https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html.
[193] *Proposed Bill to address Online Harms* [Canada] Bill C-63. https://www.canada.ca/en/canadian-heritage/services/online-harms.html.
[194] *An Act to enact the Protection of Minors in the Digital Age Act and to amend the Criminal Code* [Canada] Bill C-412. (2024). https://www.parl.ca/legisinfo/en/bill/44-1/c-412; Garner, M. R. (2024, September 16). *Bill C-412: Keeping kids safe online, keeping civil liberties intact*. Substack. https://michellerempelgarner.substack.com/p/bill-c-412-keeping-kids-safe-online.
[195] Bronskill, J. (2025, June 29). Liberals taking 'fresh' look at online harms bill, says Justice Minister Sean Fraser. *CBC*. https://www.cbc.ca/news/politics/liberals-taking-fresh-look-at-online-harms-bill-says-justice-minister-sean-fraser-1.7573791.

proceeding to draft formal guidance for online service providers.[196] While the consultation is officially complete, this process is advancing in concert with pending federal legislation, specifically Bill S-209,[197] which seeks to mandate age verification for access to certain online content and is currently being considered in committee in the Senate. The Privacy Commissioner has endorsed this Bill, signaling a coordinated regulatory and legislative push toward mandatory, high-friction age assurance systems. For U.S. industry, this trajectory raises significant concerns that constitute a potential non-tariff barrier to trade, including: substantial operational costs and technical burdens of implementing Canada-specific systems, which disproportionately impact small and medium-sized enterprises; the creation of legal and financial liability from collecting and storing highly sensitive datasets that link verified identities to private online behavior; and regulatory uncertainty driven by a lack of clear technical standards, data protection safeguards.

Potential Challenges to the Development of AI

Bill C-27, introduced in 2022 and focused on privacy 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.[198] That bill has now lapsed but AI elements are expected to be re-introduced. Artificial intelligence systems in that version were 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. The proposal also includes monetary penalties of up to 3% of global revenues and introduced a criminal enforcement provision for non-compliance, which represented a unique addition to AI regulatory proposals.

---

[196] Office of the Privacy Commissioner of Canada. (n.d.). *Consultation on age assurance.* https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-age/

[197] *An Act to restrict young persons' online access to pornographic material* [Canada] Bill S-209. (2025). https://www.parl.ca/legisinfo/en/bill/45-1/s-209.

[198] *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts* [Canada] Bill C-27. (2022). https://www.parl.ca/legisinfo/en/bill/44-1/c-27.

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. 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. While the bill lapsed with the conclusion of the 2025 federal elections, Canada's new Minister of AI and Digital Innovation has indicated an intention to reintroduce it.[199]

An October 2023 letter from then Minister of Innovation, Science and Industry, François-Philippe Champagne, stating that the government seeks to include AI used in the "moderation of content 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.[200]

Separately, on July 7, 2024 the Competition Bureau concluded its open consultation[201] on its discussion paper on AI and competition.[202] The paper is part of the Bureau's broader inquiry on how competition is developing in AI markets, the potential for regulation to protect and promote competition in AI markets, and potential measures to address competitive harms arising from AI. Industry recommends monitoring this process to ensure that any oversight on competition and AI is balanced, flexible, and applies to all actors equally on a nationality-neutral basis. Generally, however, the market for Generative AI includes many participants, and there are no indications that access to AI inputs has impeded market development or created competitive harms. Existing competition rules in Canada are sufficient to address any future problems, such as the potential for algorithmic collusion.[203]

---

[199] Bronskill, J. (2025, June 29). Liberals taking 'fresh' look at online harms bill, says Justice Minister Sean Fraser. *CBC*. https://www.cbc.ca/news/politics/liberals-taking-fresh-look-at-online-harms-bill-says-justice-minister-sean-fraser-1.7573791.

[200] Champagne, F.P. (2023, October 3). [Letter from Honourable François-Philippe Champagne to Mr. Joël Lightbound, MP]. https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12600809/12600809/MinisterOfInnovationScienceAndIndustry-2023-10-03-e.pdf.

[201] Competition Bureau Canada. (n.d.). *Feedback Form – Artificial Intelligence and Competition: Discussion Paper.* https://competition-bureau.canada.ca/feedback-form-artificial-intelligence-and-competition-discussion-paper.

[202] Competition Bureau Canada. (2024). *Artificial intelligence and competition*. https://competition-bureau.canada.ca/sites/default/files/documents/AICompetition-Discussion-Paper-240320-ver3-e.pdf.

[203] CCIA. (2024, July 1). *CCIA Comments Canada AI & Competition Consultation*. https://ccianet.org/library/ccia-comments-canada-ai-competition-consultation/.

Restrictions on Cross-Border Data Flows

The Government of Quebec passed privacy legislation in September 2021 that, amongst other things, risk making data transfers extraordinarily difficult.[204] The law entered into effect on September 22, 2022, with various provisions entering into effect in phases over three years and the majority of the law entering into force September 22, 2023.[205] 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.[206]

Additionally, the Canadian federal government is signaling its intention to introduce new privacy legislation, drawing heavily from the principles of the now-defunct Bill C-27, which stalled in January 2025.[207] Based on the legacy of C-27, there a number of concerns with this approach. First, it would introduce ambiguous or overly strict rules on the use of publicly available information for AI training. Furthermore, it includes renewed focus on "digital sovereignty" that may lead to new requirements for cross-border data flows and data localization. Such provisions increase compliance costs and legal uncertainty for U.S. companies, hinder the highly integrated U.S.-Canada digital market, and impede innovation in critical areas like the development of artificial intelligence. USTR should proactively engage the Canadian government to advocate for a legislative framework that is interoperable with global standards and promotes a fair and open digital marketplace.

Taxation of Digital Products and Services

On June 29, 2025, the Canadian Department of Finance announced the planned rescission of the country's DST ahead of the first collection date.[208] The DST, adopted on June 20, 2024, would have imposed a 3% tax on revenues from online marketplace services, online advertising, social media, and user data.[209] As designed, it would predominantly affect U.S. firms while sparing

---

[204] Tehrani, M., Oates, C., Kappler, J. & Matziorinis, P. (2020, June 19). *Quebec to introduce the most punitive privacy laws in Canada - with fines of up to $25 million*. Lexology. https://www.lexology.com/library/detail.aspx?g=a42e22b1-ec2d-4a79-a9d3-74519ef6a3e8; Holland, J. (2021, November 12). Québec's Updated Privacy Law Complicates Cross-Border Data Flows. *Bloomberg Law*. https://news.bloomberglaw.com/privacy-and-data-security/quebecs-updated-privacy-law-complicates-cross-border-data-flows.

[205] Bernier, C. (2023, January 13). *2023 Canada Private-sector Privacy Law Reform: Keeping Track of Moving Parts*. IAPP. https://iapp.org/news/a/2023-canada-private-sector-privacy-law-reform-keeping-track-of-moving-parts/; Brisbois, L. (2022, February 16). *Canada Reforms Its Data Privacy Laws Through Enactment of Quebec Bill 64.* Digital Insights. https://lewisbrisbois.com/blog/category/data-privacy-cyber-security/canada-reforms-its-data-privacy-laws-through-enactment-of-quebec-bill-64.

[206] U.S. International Trade Commission. (2021). *The Year in Trade 2021 – Operation of the Trade Agreements Program*. https://www.usitc.gov/publications/332/pub5349.pdf.

[207] Walsh, M. & Guilman, A. (2025, September 26). *Federal privacy reform: Where we left off and what's next*. Gowling LG. https://gowlingwlg.com/en/insights-resources/articles/2025/federal-privacy-reform.

[208] Department of Finance Canada. (2025, June 29). *Canada rescinds digital services tax to advance broader trade negotiations with the United States*. https://www.canada.ca/en/department-finance/news/2025/06/canada-rescinds-digital-services-tax-to-advance-broader-trade-negotiations-with-the-united-states.html.

[209] *Digital Services Tax Act* [Canada] S.C. 2924, c. 15, s. 96. (2024). https://laws-lois.justice.gc.ca/PDF/D-1.65.pdf.

Canadian rivals in equivalent offline industries, and, through its retroactive application to January 2022, the measure was projected to cost U.S. companies an estimated US$3 billion in 2025 alone.[210] Although collection has been paused, industry reports indicate that payments made in anticipation of the tax have not yet been reimbursed, and the government has not introduced legislation to formally repeal the measure, leaving open the possibility of its revival. USTR is therefore urged to press the Canadian government to ensure timely reimbursement and to codify the DST's rescission in law.

Threats to the Security of Devices and Services

In September 2025, the Canadian government introduced Bill C-2, a border security and data access proposal that would significantly expand the government's powers to obtain and intercept digital information.[211] If enacted, the bill would: (1) authorize law enforcement and intelligence agencies to make warrantless "information demands" compelling service providers to hand over non-content information; (2) establish production orders for subscriber information; (3) enable cross-border data sharing by authorizing the enforcement of foreign decisions to compel the production of subscriber information or transmission data held by Canadian entities under the MLAT Act; and (4) introduce a new Authorized Access to Information Act, requiring electronic service providers to facilitate access to and interception of information by authorized persons. Bill C-2 would grant the Canadian government broad authority to access private information without a warrant and require service providers to implement technical capabilities to access encrypted communications and sensitive data. These measures raise significant concerns that providers could be forced to create or enable backdoor access to messaging and cloud services, posing serious risks to user privacy, data security, and trust in digital services.

Chile

Customs-Related Restrictions and Import Barriers for Goods

Under the U.S.-Chile Free Trade Agreement,[212] Chile committed to expedited customs procedures for express shipments and to allow shipment operators "to submit a single manifest covering all goods contained in a shipment transported by the express shipment service, through, if possible, electronic means." This commitment has yet to be fully implemented, and imports can be significantly delayed at the border due to the current customs systems' inability to process data from a variety of carriers.

---

[210] CCIA. (2024, May 1). *Impacts of Canada's Proposed Digital Service Tax on the United States*. https://ccianet.org/research/reports/impacts-canada-proposed-digital-service-tax-united-states/.
[211] *An Act respecting certain measures relating to the security of the border between Canada and the United States and respecting other related security measures* [Canada] Bill C-2. (2025). https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c2_2.html.
[212] *United States–Chile Free Trade Agreement*, June 6, 2003. https://ustr.gov/trade-agreements/free-trade-agreements/chile-fta/final-text.

Additionally, under the FTA, Chile agreed to "their desire to maintain the level of open market access existing on the date this Agreement is signed." The Chilean government had in place a trade facilitation mechanism for shipments under US$41, excluding such shipments from being subjected to VAT and customs duties. However, on September 25, 2024, Chile passed a bill that eliminates the VAT exemption on shipments under US$41, which removes the open market access policies for express delivery shipments that were previously available and are guaranteed under the FTA. USTR should press Chile to reconsider an action inconsistent with the spirit, if not the letter, of the FTA.

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*[213], requires that "significant" or "strategic" data of financial institutions be held in Chile. Under Chapter 20-7, use of cloud services 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 subject to local data center obligations, since most do not meet CMF standards with respect to risk management. This has become an obstacle for data hosting services in Chile, as it requires financial institutions to use local infrastructure offerings.

Similar requirements are outlined in Circular No. 2, which focuses on 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.

Restrictions on Cross Border Data Flows

Chile's recently approved Personal Data Protection Law,[214] inspired by the EU's General Data Protection Regulation, is scheduled to enter into force in December 2026. The law's implementation will depend heavily on the issuance of numerous secondary regulations by a newly established Data Protection Agency, which will only become operational at the same time the law takes effect. This sequencing creates considerable legal and operational uncertainty for U.S. companies. Critical mechanisms for enabling international data transfers, such as standard contractual clauses, binding corporate rules, and adequacy determinations, have not yet been developed. In the absence of this regulatory framework, businesses cannot meaningfully prepare

[213] Chilean Commission for Financial Markets. (2014, July 10). *Recopilación Actualizada de Normas Bancos.* https://www.cmfchile.cl/portal/principal/613/articles-28982_doc_pdf.
[214] *Ley que Regula La Protección y el Tratamiento de Los Datos Personales y Crea La Agencia de Protección de Datos Personales* [Chile] Law no. 21719. (2024). https://www.bcn.cl/leychile/navegar?idNorma=1209272.

for compliance, raising the risk of disruptions to transatlantic data flows that are essential to the digital economy. It is therefore crucial that USTR urge Chile to finalize and publish all key secondary regulations well in advance of the law's entry into force or, alternatively, extend the transition period to allow companies sufficient time to adapt.

Other Barriers to Digital Trade

Chile's government recently approved the Cybersecurity Framework Law, which entered into force on March 1, 2025 and is modeled after the EU's Network and Information Security Directive 2.[215] While the objective of strengthening cybersecurity is commendable, the law's implementation could create significant trade barriers if implementation is not carefully designed. For instance, requiring a Clave Única, Chile's state-issued digital ID, for registration or compliance would effectively exclude foreign companies whose implementation and cybersecurity teams are located abroad.

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, has adversely affected foreign businesses that are increasingly hesitant to enter the Chinese market. 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.[216]

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

China seeks to further restrain foreign cloud service operators, in concert with its national plan to promote the Chinese cloud computing industry. As CCIA has noted in previous submissions, U.S. cloud service providers are worldwide leaders and strong U.S. exporters, supporting tens of thousands of high-paying American jobs and making a strong contribution toward a positive balance of trade.[217] While U.S. CSPs have been at the forefront of the movement to the cloud in

---

[215] *Ley Marco de Ciberseguridad* [Chile] Law no. 21663. (2024). https://www.bcn.cl/leychile/navegar?idNorma=1202434).

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

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

virtually every country in the world, China has blocked them. Although the legal basis for the blocking foreign entry remains unclear (and is likely inconsistent with China's WTO commitment with respect to computer services), by imposing a licensing requirement and simply declining to license foreign applicants effectively closes the market. It restricts foreign firms to operating on a franchise model—licensing technology and know-how to a Chinese operator, in exchange for a fee or share of revenue.

All telecommunications businesses in China are subject to cumbersome licensing requirements. Foreign companies' participation in value-added telecommunication 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."[218]

Moreover, China imposes sector-specific restrictions on the use of public cloud services in sensitive industries such as financial services and smart vehicles, effectively prohibiting foreign CSPs from serving these sectors. Many international financial institutions and vehicle manufacturers cannot leverage global public cloud infrastructure to support their operations, undermining operational resilience, cybersecurity risk management, and standardization of internal controls. This fragmented and protectionist regulatory environment, combined with licensing barriers and sectoral prohibitions, not only prevents fair competition but also acts as a significant non-tariff trade barrier, restricting market access for U.S. CSPs and distorting global cloud service markets. Despite broader reform commitments under the August 2023 "Opinions on Further Optimizing the Foreign Investment Environment and Increasing Efforts to Attract Foreign Investment,"[219] meaningful progress in this sector has stalled.

Government Imposed Restrictions on Internet Content and Related Access Barriers

China has recently introduced a series of measures that significantly tighten state control over online expression and impose extensive new compliance burdens on online services. Together,

[218] Ross, L. & Zhou, K. (2023, August 15). *China Issues Policy to Further Boost Foreign Investment*. WilmerHale. https://www.wilmerhale.com/insights/client-alerts/20230815-china-issues-policy-to-further-boost-foreign-investment.
[219] State Council of China. (2023). *Opinions of the State Council on Further Optimizing the Foreign Investment Environment and Increasing the Attraction of Foreign Investment*. https://swj.xlgl.gov.cn/swj/zwgk/zcfg/202311151840472238/202311151840207925 4.pdf.

these initiatives illustrate a model of digital governance centered on pervasive state oversight, mandatory identity tracking, and broad content control.

- 2022 Provisions on Internet Post Comments: Updated rules require platforms to verify user identities, pre-screen and monitor comments and replies in real time, and report "illegal" or "negative" information directly to authorities. Providers must also hire and train professional moderation teams proportional to the size of their services. These obligations extend even to replies and livestream chats, effectively eliminating anonymous or unmonitored discourse.[220]
- 2022 Social Media Monitoring Rules: Complementary regulations further require platforms to review all comments before posting, monitor ongoing user activity in real time, track engagement such as "likes," and collect detailed identity information. This extends state visibility beyond posted content to user behavior itself, reinforcing a climate of self-censorship.[221]
- 2023 Cyberbullying Guidelines: Draft guidance would criminalize a wide range of online speech, including "rumor-spreading" or posts that "demean" others, and compel platforms to proactively detect and remove such content. Providers would also be required to preserve evidence for investigations, facing financial penalties or content suspensions if they fail to comply.[222]
- Real-Name Requirements for Influencers: Major platforms now mandate that users with large followings publicly display their real names. While identity verification was already required, this public disclosure intensifies privacy and safety risks, leading some creators to shut down their accounts.[223]
- 2024 National Network Identity Proposal: A draft measure would create a unified national digital ID, usable across multiple platforms. While nominally voluntary, the scheme could consolidate state tracking of online activity and add to already stringent data-handling obligations.[224]
- 2024 Regulations on Online Violence: Newly effective rules require providers to remove politically sensitive or otherwise prohibited material, and to ensure that online

---

[220] Cyberspace Administration of China. (2022). *Notice from the Cyberspace Administration of China on Soliciting Public Opinions on the "Regulations on the Administration of Internet Comment Services (Draft for Comments)*." https://www.cac.gov.cn/2022-06/17/c_1657089000974111.htm.
[221] Cyberspace Administration of China. (2022). *Provisions on the Administration of Internet Comment Services*. http://www.cac.gov.cn/2022-11/16/c_1670253725725039.htm; He, L. (2022, November 30). China to Punish Internet Users for 'Liking' Posts in Crackdown After Zero-Covid Protests. *CNN.* https://www.cnn.com/2022/11/30/media/china-new-internet-rule-punish-liking-posts-intl-hnk/index.html.
[222] *Bloomberg News*. (2023, July 7). China Warns its Tech Giants to Rein in Cyberbullying. https://www.bloomberg.com/news/articles/2023-07-07/china-warns-its-tech-giants-to-rein-in-cyberbullying.
[223] Chenglong, J. (2021, October 31). Social Media Influencers Required to Display Full Real Names on Accounts. *China Daily. https://www.chinadaily.com.cn/a/202310/31/WS6541068aa31090682a5ebbb9.html.*
[224] Cyberspace Administration of China. (2024, July 26). *Announcement of the Cyberspace Administration of China on the Public Solicitation of Comments on the Draft Measures for the Administration of National Network Identity Authentication Public Services.* https://www.cac.gov.cn/2024-07/26/c_1723675813897965.htm.

information "adheres to the correct political direction." The vague and expansive scope of these provisions grants authorities wide discretion to suppress speech.[225]

Taken together, these measures illustrate an increasingly sophisticated system of online control, one that fuses pervasive surveillance, mandatory identity verification, and proactive content policing into a single regulatory framework. As other governments look to China's approach as a model, these developments risk accelerating a global shift toward more restrictive, state-centric approaches to online speech and undermining international norms of free expression and open digital communication.

Potential Challenges to the Development of AI

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.[226] 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 consultation process was striking: the CAC issued its draft policy on April 11, 2023, and provided less than 30 days for comment.[227] The subsequent measures went into effect on August 15, 2023.

The Ministry of Industry and Information Technology of China issued draft Guidelines for Standardizing the Artificial Intelligence Industry for public comments on January 17, 2024.[228]

---

[225] Cyberspace Admin. of China. (2024, June 14). *Provisions on the Governance of Online Violence Information*. https://www.cac.gov.cn/2024-06/14/c_1720043894161555.htm.
[226] Cyberspace Admin. of China. (2023, July 13). *Interim Measures for the Administration of Generative Artificial Intelligence Services.* http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm.
[227] Huang S., et al. (2023, April 12). *Translation: Measures for the Management of Generative Artificial Intelligence Services (Draft for Comment) – April 2023*. Digichina. https://digichina.stanford.edu/work/translation-measures-for-the-management-of-generative-artificial-intelligence-services-draft-for-comment-april-2023.
[228] Ministry of Industry and Information Technology of China. (2024, January 17). *Guidelines for the Construction of a National Comprehensive Standardization System for the Artificial Intelligence Industry (Draft for Comments).* https://gxj.nanjing.gov.cn/hdjl/dczj/202401/P020240123509596442724.pdf.

This draft seeks to "take advantage of early opportunities in the development of the AI industry" and outlines a set of goals for the AI sector by 2026. It aims to establish more than 50 national and industry-wide standards and participate in the creation of more than 20 international standards for AI. CCIA urges the U.S. government to monitor closely, as the government may seek to use this proceeding to adopt China-specific standards for AI that differ from consensus international standards leverage these alternatives globally to usurp the footprint of competing foreign companies.

On May 23, 2024 the National Information Security Standardization Technical Committee released the draft Cybersecurity Technology – Basic Security Requirements for Generative AI Service regulation.[229] The regulation would require providers to implement security measures around training data, carry out security assessments, and limit harmful outputs to 5%.[230] The mandatory sharing of information to comply with the training data and security requirements with the Chinese government raises concerns due to the country's history of misappropriating U.S. technology and IP.

Restrictions on Cross-Border Data Flows

China remains a very difficult market for internet services to operate in due to a number of localization and protectionist measures.[231] The United States International Trade Commission has estimated that billions of dollars are being lost in the market as a result.[232] 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. Based on industry monitoring, as of August 2024, none of the top 10 globally most-visited sites (eight of which are American) were visible in China.[233] China's blocking mechanism, colloquially known as the Great Firewall,

[229] Center for Security and Emerging Technology. (2024, April 4). *Translation: Basic Safety Requirements for Generative Artificial Intelligence Services*. https://cset.georgetown.edu/publication/china-safety-requirements-for-generative-ai-final/.
[230] Chinese National Information Security Standardization Technical Committee. (2024, May 17). *Basic Requirements for Network Security Technology Generative Artificial Intelligence Service Security.* https://www.tc260.org.cn/file/2024-05-17/9e2853d0-99a0-49c2-9df7-ccaada842ac5.pdf.
[231] CCIA. (2023). *Comments of The Computer & Communications Industry Association Regarding Foreign Trade Barriers to U.S. Exports For 2023 Reporting*. https://ccianet.org/wp-content/uploads/2022/10/CCIA-Comments-2023-National-Trade-Estimate-Reporting.pdf.
[232] 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.
[233] Similar Web. (n.d.). *Top Websites Ranking*. https://www.similarweb.com/top-websites/; Website Test Behind the Great Firewall of China. (n.d.). *WebSite Pulse*.

is fundamentally protectionist and anticompetitive, and contrary to China's WTO commitments and separate commitments to the United States.[234]

Stringent restrictions on the cross-border transfer of data, both personal and non-personal, are implemented through three overlapping laws: the 2019 Cybersecurity Law, the 2021 Data Security Law, and the 2021 Personal Information Protection Law. [235]

- The Decision on Strengthening Online Information Protection, effective from December 28, 2012 (Decision);
- The Draft Regulation of Network Data Security Management, published for consultation on November 14, 2021;
- The Measures for the Security Assessment of Outbound Data Transfers, effective from September 1, 2022;
- The Measures for the Standard Contract for the Outbound Transfer of Personal Information, effective from 1 June 2023;
- The Regulations on Facilitating and Regulating the Cross–border Data Transfers, effective from 22 March 2024; and
- The Network Data Security Management Regulation (Network Data Regulation) , effective from 1 January 2025.

By requiring categorization of data into vague levels of sensitivity (some of which subject to outright export bans or pre-authorization), mandatory assessment of internal data-handling procedures and those of foreign recipients, reporting requirements and periodic audits by regulators, Chinese regulators have made transfers of data so burdensome and subject to incalculable liability that both domestic and foreign firms seek to minimize the action. As a result, services offered by foreign firms dependent on such exports (e.g., foreign cloud-based services) inevitably suffer.

Threats to the Security of Devices and Services

China's Cryptography Law went into effect on January 1, 2020,[236] 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 is deemed a state secret. Commercial encryption refers to technology

[234] 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.
[235] Webster, G. & Creemers, R. (2020, May 28). *A Chinese Scholar Outlines Stakes for New 'Personal Information' and 'Data Security' Laws (Translation).* New America. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-scholar-outlines-stakes-new-personal-information-and-data-security-laws-translation/.
[236] PwC. (2020, January 13). *New Chinese Cryptography Law in Force*. https://legal.pwc.de/de/news/fachbeitraege/new-chinese-cryptography-law-in-force-as-of-1-january-2020.

used to protect information that is deemed to not be state secrets. In April 2023, the government amended the Commercial Cryptography Administrative Regulations,[237] 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* mandatory 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.

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.

Other Barriers to Digital Trade

China's regulatory framework for critical information infrastructure has expanded in scope and restrictiveness, creating significant compliance burdens and market access barriers for foreign firms. The CII Security Protection Regulation, effective September 1, 2021, mandates enhanced security protection obligations for operators designated as CII. The regulation promotes the procurement of "secure and trustworthy" network products and services, a standard that can be used to favor domestic suppliers and disadvantage foreign technology providers. Companies identified as CII operators face heightened obligations under China's security legislation, including mandatory security certification, assessment, and cybersecurity review. Relatedly, the concept of "important data," introduced in Article 37 of the Cybersecurity Law in 2017,[238] has been expanded through successive guidelines directing data processors on classification and identification obligations. These measures significantly increase the compliance burden on firms that handle important data. In practice, vague definitions and opaque designation criteria for both CII and important data, combined with their expanding application by sectoral regulators, create legal uncertainty, higher operational costs, and de facto entry barriers for foreign companies seeking to serve Chinese customers or operate in sensitive industries.

---

[237] China Justice Observer. (2023, July 17). *China to Regulate Commercial Cryptography.* https://www.chinajusticeobserver.com/a/china-to-regulate-commercial-cryptography.
[238] *Cybersecurity Law (draft)* [China]. (2015). https://web.archive.org/web/20161029174914/http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm

China's cybersecurity review regime further compounds these barriers. The Cybersecurity Review Measures (CSRM), revised January 4, 2022,[239] require CII operators procuring network products and services, and online platform operators engaged in data activities that may affect national security, to proactively undergo a cybersecurity review. This process is highly opaque and involves broad, discretionary assessments of factors such as supply chain reliability, product security, openness, and geopolitical risks. In early 2023, for example, the Cyberspace Administration of China launched and failed Micron in a cybersecurity review,[240] effectively barring CII operators from purchasing its products. This case illustrates how vague criteria and broad administrative discretion can be used to discriminate against foreign technology providers. By conditioning market access on an unpredictable and non-transparent review process, China's cybersecurity review regime functions as a non-tariff trade barrier that deters investment and constrains foreign participation in key digital and infrastructure markets.

Colombia

Customs-Related Restrictions and Import Barriers for Goods

Colombia committed under the USCTPA to modernizing its customs procedures through the implementation of automation and electronic systems,[241] and to implementing expedited customs procedures for express shipments, including fully integrating express shipments into Colombia's Single Window.[242] As part of these commitments, the submission and processing of information required for the release of an express shipment prior to its arrival should be a central element of any expedited procedures, as should the use of a single electronic manifest whenever feasible. However, industry remains concerned that the Colombian government has yet to implement these commitments in practice, as the use of physical documents remains mandatory.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Colombia has established a significant trade barrier in its $218 million public sector cloud services market through the deliberate expiration of its Cloud Computing Framework Agreement (CCFA) on August 31, 2025,[243] and the subsequent preferential treatment of state-owned enterprises. The indefinite suspension of the CCFA, coupled with Presidential Directive No. 06

---

[239] Webster, G. & Creemers, R. (2022, January 10). *Translation: Cybersecurity Review Measures (Revised) – Effective Feb. 15, 2022.* DigiChina. https://digichina.stanford.edu/work/translation-cybersecurity-review-measures-revised-effective-feb-15-2022/.

[240] *Reuters*. (2023, May 22). China fails Micron's products in security review, bars some purchases. https://www.reuters.com/technology/chinas-regulator-says-finds-serious-security-issues-us-micron-technologys-2023-05-21/.

[241] 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."

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

[243] *Forbes*. (2025, September 3). Gobierno colombiano se enfrenta a incertidumbre en sus servicios digitales tras el fin del acuerdo marco de nube pública. https://forbes.co/2025/09/03/tecnologia/nube-publica-colombia.

of August 13, 2025,[244] which promotes Internexa, a state-controlled company, as the primary technology procurement vehicle, has created an environment of legal uncertainty, market distortion, and direct discrimination against U.S. cloud providers. The Colombia Compra Eficiente (CCE) has failed to formalize an extension or replacement for AMP IV, leaving procurement for new public cloud services effectively paralyzed. CCE's shifting approach to AMP V, including unclear segmentation between "Nube Pública Hiperescala" and "Nube Pública Abierta" and its recent moves to eliminate local segments temporarily, further undermines transparency and fair competition. At the same time, the government has proposed the "Compra Pública para la Innovación,"[245] which would create alternative procurement channels allowing direct contracting with specific providers, bypassing the mandatory framework agreements. These actions, combined with procedural irregularities and a lack of stable procurement rules, threaten existing systems operated by U.S. providers, and appear to violate US-Colombia FTA provisions on non-discriminatory treatment and transparent procurement, and raise security risks by increasing reliance on non-U.S. technology providers. The constant uncertainty surrounding Colombia's procurement process creates a highly unpredictable, non-transparent, and discriminatory environment, discouraging long-term investment and undermining market access for foreign firms.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

Colombia's proposed "Internet Solidarity" bill, introduced in August 2025,[246] would create a significant new trade barrier through excessive regulation of digital services, despite the Communications Regulation Commission's (CRC) earlier determination against implementing "Fair Share" contributions.[247] The proposal would establish a new "Digital Intermediary Service Providers" category that subjects U.S. cloud providers to burdensome registration obligations, mandatory cooperation with authorities, and new content moderation responsibilities. The bill's broad scope and six-month implementation timeline for accompanying regulations create serious operational uncertainty for U.S. technology companies. Of particular concern is the combination of expanded CRC authority to compel provider information and the designation of internet access as a fundamental right, which could enable the future imposition of network fees or similar financial obligations. Such measures would create cost asymmetries disadvantaging U.S. service providers, restrict market entry, and increase compliance costs in the Colombian market.

---

[244] *Directiva Presidencial 06 de 2025* [Colombia]. (2025). https://normograma.com/documentospdf/icfes2024/compilacion/docs/directiva_presidencia_0006_2025.htm

[245] Colombia Compra Eficiente. (2022). *Manual para entender la Compra Pública para la Innovación*. https://www.funcionpublica.gov.co/eva/admon/files/empresas/ZW1wcmVzYV83Ng==/imagenes/1125/manual_de_compra_publica_para_la_innovacion.pdf

[246] Colombian Ministry of Information and Communication Technologies. (2025). *Projecto de Ley Internet Solidario*. https://www.mintic.gov.co/portal/715/articles-405037_recurso_1.pdf.

[247] *Finance Colombia*. (2025, October 8). Colombia's CRC Study Finds No Basis for Charging OTT Platforms for Network Use. https://www.financecolombia.com/colombias-crc-study-finds-no-basis-for-charging-ott-platforms-for-network-use/.

The CRC has been actively exploring the issue of mandatory OTT contributions for securing infrastructure.[248] Domestic internet service providers are supportive of this effort, and back proposals to amend the current ICT Universal Service Fund, FUTIC. Following a series of consultations, the CRC published its final report in September 2025, "The Role of OTT Services in the Communications Sector in Colombia - 2024,"[249] which concluded not with an immediate proposal for network fees, but with a more foundational and strategic set of recommendations for the Colombian Congress, which represents a significant and concerning development for the digital sector: The CRC proposes a roadmap to intervention, with the most critical and immediate objective being to obtain legal powers to directly and compulsorily request a wide range of information, including traffic, investment, and infrastructure data, from OTTs. This power is framed as necessary for "analysis" but is, in reality, the foundational step to establish jurisdiction and build a regulator-driven case for future mandates. Building on this, the CRC's proposal includes several other alarming proposals, such as: initiating a "regulatory project" to intervene in the commercial and technical relationship between telcos and OTTs, which is an explicit vehicle to create a state-arbitrated system for "remunerated agreements" (or network fees); exploring mandatory financial contributions from OTTs to the FUTIC, which would effectively create a discriminatory second tax on the digital sector, in addition to the SEP tax; and expanding its mandate into content regulation, by seeking to set standards and enforce compliance on platforms' content moderation and parental control mechanisms. This pursuit of expanded oversight over OTTs, which are primarily U.S. companies, would cause significant financial harm and reduce their competitiveness. USTR should evaluate whether the pursuit of these new regulatory powers, and any subsequent measures, are consistent with Colombia's trade commitments, including the US-Colombia FTA.

Government-Imposed Content Restrictions and Related Access Barriers

Colombia has failed to comply with its obligations under the 2006 U.S.-Colombia Free Trade Agreement to provide protections for Internet service providers.[250] Revision to the legislation in 2018 that sought to implement the U.S.-Colombia FTA copyright chapter includes no language on online intermediaries.[251] 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

[248] Colombia Communications Regulation Commission. (2024, September 3). *Implications of the interaction between telecommunications operators and OTT Providers*. https://www.crcom.gov.co/sites/default/files/webcrc/documents/2024-09/Janeth-hernandez-taller-crc-2024.pdf.
[249] Colombia Communications Regulation Commission. (2025). *Estudio sobre el rol de los servicios «Over the Top» OTT en Colombia – 2024*. https://www.crcom.gov.co/es/proyectos-regulatorios/9000-38-2-22.
[250] *United States–Colombia Trade Promotion Agreement*, U.S.–Colom., Nov. 22, 2006, art. 16.11, para. 29. https://ustr.gov/trade-agreements/free-trade-agreements/colombia-fta/final-text
[251] Herrera, J. R. (2018, September 5). *The recent and relevant copyright bill in Colombia (Law 1915-2018)*. Kluwer Copyright Blog. http://copyrightblog.kluweriplaw.com/2018/09/05/recent-relevant-copyright-billcolombia-law-1915-2018/.

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.

Potential Challenges to the Development of AI

A new AI bill introduced in 2025 (N° 043) introduced by the government and currently under consideration in Congress would impose a restrictive "permission-first" regime for AI by mandating that "express consent" be obtained from rightsholders, and promoting government-fostered licensing schemes for the use of content in AI training.[252] This approach explicitly rejects the establishment of a broad and workable text-and-data mining exception and would instead codify a system that is technically and economically unworkable at the scale of the public internet. If passed, this legislation would not only fail to modernize Colombia's copyright framework to meet its international obligations but would actively create new, insurmountable barriers to AI development and deployment, further solidifying the legal uncertainty for all online services operating in the country.

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.[253] 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. This SEP provision contradicts the OECD two-pillar framework process and the MLC, which Colombia signed and agreed to.

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, including cross-border sale of goods and digital advertising. This 10% rate is high compared to other enacted DSTs and similar measures. A non-resident can, if it registers in Colombia, avail itself of an alternative, a 3% tax on the gross income earned through selling goods and/or providing digital services. Crucially,

---

[252] *Proyecto de Ley de Inteligencia Artificial en Colombia* [Colombia] No. 043 (2025). https://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2025%20-%202026/PL%20043-25%20-%20REGULACION%20INTELIGENCIA%20ARTIFICIAL.pdf.
[253] *Law 2277 of 2022 Tax Reform* [Colombia]. (2022). https://assets.kpmg.com/content/dam/kpmg/us/pdf/2022/12/tnf-colombia-dec19-2022.pdf.

this optional declarative gross-basis tax for non-residents is not transferable to customers. The SEP rule entered into force on January 1, 2024, marking what appears to be the first DST-like tax imposed in the Latin American region. Columbia recognizes that the measure may be inconsistent with the OECD framework and indicates that it will be adjusted if and when the OECD framework comes into force. This rule is currently being applied to US technology companies operating within the country, and since the OECD process remains uncertain, is likely to incur significant burdens on U.S. firms for the foreseeable future.

These measures are inconsistent with global tax norms, which favor taxing income at the permanent establishment associated with income generation, as well as the evolving principles being developed at the OECD to address global tax fairness. 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 Colombian government has implemented this measure, and urges USTR and Treasury to engage with the Colombian government to remove or alter this measure.

Imposing a gross-basis tax on non-residents of Colombia on income derived from cross-border sales impedes U.S. sales into the Colombian market. In addition, since the U.S. does not have a tax treaty with Colombia, implementation of this measure will likely 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 could implicate Colombia's obligations under both the WTO and the United States-Colombia Trade Promotion Agreement which prohibits discriminatory treatment of U.S. suppliers, including with respect to taxation measures.[254]

The Financial Law for the 2026 Budget submitted to Congress by the Government on September 1, 2025 includes a provision (Article 12) that would increase the optional, declarative gross-basis tax for non-residents opting for this mechanism, from the current 3% rate to 5% on the totality of gross income derived from the sale of goods and/or provision of digital services.[255] Moreover,

[254] 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.

[255] *Por medio de la cual se expiden normas para el financiamiento del Presupuesto General de la Nación orientadas al restablecimiento del equilibrio de las finanzas públicas, la sostenibilidad fiscal, y se dictan otras disposiciones* [Colombia]. (2025). https://img.lalr.co/cms/2025/09/01114632/PROYECTO-DE-LEY-DE-FINANCIAMIENTO-2025-PUB_1_09_2025.pdf.

the bill also includes a provision that eliminates the VAT exclusion that a prior 2018 reform had established for cloud computing services, a measure reflecting the government's inclination to discourage cloud services in favor of on-premise solutions.

Croatia

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Industry reports that Croatia has imposed significant barriers in its public procurement market through a combination of technical standards, procedural requirements, and structural preferences that effectively favor EU-based suppliers and disadvantage foreign firms. Croatia's Public Procurement Act, which entered into force in December 2016 (superseding a 2011 law) and implements the latest EU procurement directives, requires that all tender documentation be submitted in the Croatian language, creating substantial logistical and financial burdens on foreign bidders, who must translate complex legal and technical materials at significant cost. In addition, tenders for cloud services, infrastructure, and technology projects often mandate compliance with EU-specific technical standards, including CE marking and data residency requirements, effectively aligning procurement with EU certification regimes. This increases compliance costs and forces U.S. firms to modify their operations to meet standards designed for EU suppliers, thereby creating asymmetrical market access conditions.

These challenges are compounded by Croatia's centralized IT governance structure, which creates a de facto preference for state-owned infrastructure. Since 2005, APIS IT (the Information Systems and Information Technologies Support Agency), a state-owned entity jointly controlled by the Government and the City of Zagreb, has served as the primary IT gatekeeper for public sector systems, and this role was further entrenched with the launch of the Shared Services Centre (CDU), Croatia's official Government Cloud, in November 2019, aimed at consolidating infrastructure for roughly 300 state institutions. As APIS IT operates around 90% of critical public sector systems, the state is strongly incentivized to continue using its own infrastructure rather than procuring external commercial cloud services, effectively closing the market to foreign cloud providers. This combination of language mandates, EU-centric technical requirements, and centralized infrastructure control constitutes a significant non-tariff trade barrier that restricts market entry, increases compliance and operational costs for foreign bidders, slows procurement timelines, and discourages U.S. investment in Croatia's public sector digital services market, despite its WTO GPA commitments intended to bar such de facto discrimination.

Taxation of Digital Products and Services

In June 2022, the government of Croatia announced plans to pursue a digital services tax, based on the similar Austrian DST model that USTR opposed that same year.[256] CCIA urges USTR to encourage Croatia to suspend this plan rather than pursue discriminatory taxes on U.S. suppliers. This proposal has yet to be finalized.

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.[257] 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. [258] 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."[259] The definitions behind false information and public safety are extremely vague and left in the hands of the government authorities.[260]

This phenomenon has continued, at the expense of companies operating in the country, consumers reliant on the services, and the free press/civil society. Internet freedom in Cuba remains highly restricted, with the government blocking independent news sites, threatening digital journalists with criminal penalties, and conducting invasive cyberattacks. At least one internet disruption in March 2024 followed protests in Santiago de Cuba, while independent journalists, activists, and civil society were routinely subjected to targeted restrictions on connectivity.[261] Independent monitoring continues to document extensive restrictions: in 2023,

---

[256] Bloomberg Tax. (2022, July 7). *Croatia Parliament considers bill on digital services taxation*. https://news.bloombergtax.com/daily-tax-report/croatia-parliament-considers-bill-on-digital-services-taxation?context=article-related.
[257] Newman, L. H. (2021, July 13). Cuba's social media blackout reflects an alarming new normal. *WIRED*. https://www.wired.com/story/cuba-social-media-blackout/
[258] Marsh, S., & Culliford, E. (2021, July 13). Faced with rare protests, Cuba curbs social media access, watchdog says. *Reuters*. https://www.reuters.com/world/americas/cuba-curbs-access-facebook-messaging-apps-amid-protests-internet-watchdog-2021-07-13/.
[259] *Gaceta Oficial No. 92 Ordinaria* [Cuba]. (2021). https://www.gacetaoficial.gob.cu/sites/default/files/goc-2021-o92.pdf; *NBC News*. (2021, August 18). Cuba spells out social media laws, forbidding content that attacks the state. https://www.nbcnews.com/news/latino/cuba-spells-social-media-laws-forbidding-content-attacks-state-rcna1703
[260] Committee to Protect Journalists. (2021, August 19). *Cuba passes regulations criminalizing online content, further restricting internet access*. https://cpj.org/2021/08/cuba-passes-regulations-criminalizing-online-content-further-restricting-internet-access/.
[261] Freedom House. (2024). *Cuba: Freedom on the Net 2024 country report*. https://freedomhouse.org/country/cuba/freedom-net/2024.

the Cuban Institute for Freedom of Expression and Press recorded 210 instances of internet restrictions for reporters, including shutdowns, blocking of social media services, and hacking of journalists' and news outlets' accounts[262]

Cyprus

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Industry reports that U.S. cloud service providers experience significant barriers in Cyprus due to strict data sovereignty rules. These obstacles are particularly prominent for suppliers seeking to offer services to the public sector or certain industries with stronger oversight such as healthcare and financial services. These rules mandate that cloud providers store and process sensitive data, such as personal health records or financial transactions, locally in Cyprus or the EU. The mandates effectively mean that U.S. cloud providers must either build and deploy local data centers or partner with local centers to service the Cyprus market for covered entities.

Additionally, Cyprus's public procurement framework often specifies data residency requirements for government contracts, which disadvantages U.S. providers in the competition for tenders. To the extent such measures extend to the private market, USTR should investigate whether they are consistent with Cyprus' comprehensive GATS commitments ensuring the cross-border supply of computer services.

Czech Republic

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Industry reports that Czech law requires cloud providers to register under a Cloud Computing Catalog. This mandate is onerous for U.S. companies and creates preferences for local competitors. With a new Cybersecurity Law being adopted, companies expect that users will experience additional administrative burdens when using U.S. cloud services.

The Czech government's National Cyber and Information Security Agency (NÚKIB) is in the process of implementing the 2022 EU NIS 2 Directive through its Cybersecurity Act, which was signed into law in June 2025 and will come into effect in November 2025.[263] Industry reports that the original version of the legislation proposed classifying data from public administration information systems at the critical risk scale (level 4), which would restrict data processors to

[262] Graham Keeley, *Cuba Cuts Internet, Surveils Calls of Journalists, Report Finds*, VOA News (Feb. 23, 2024), https://www.voanews.com/a/cuba-cuts-internet-surveils-calls-of-journalists-report-finds-/7499415.html.
[263] Ščerba, T. & Metelka, J. (2023, August 16). *New Czech cybersecurity regulation: What you need to know*. DLA Piper. https://www.dlapiper.com/en/insights/publications/2023/08/new-czech-cybersecurity-regulation-what-you-need-to-know.

storing data of this category in servers located in the Czech Republic.[264] Such a blanket restriction is disproportionate, inconsistent with a risk-based approach, and would pose a burden to U.S. and foreign cloud services suppliers seeking to offer such services in the country. Czech mobile operators have criticized the law as well, arguing it would be among the strictest interpretations of the law in Europe and undermine their business by granting NUKIB with excessive power, while the costs of implementation have been questioned by the Czech Union of Towns and Municipalities.[265]

Government-Imposed Content Restrictions and Related Access Barriers

The Czech Republic's implementation of the EU Copyright Directive (EUCD) went into effect in January 2023.[266] The Czech approach 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. The results have been demonstrably harmful.[267] 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.[268] The CJEU has previously ruled that Article 17 as drafted provides sufficient

[264] U.S. Department of State. (2024). *2024 Investment Climate Statements: Czechia*. https://www.state.gov/reports/2024-investment-climate-statements/czechia.
[265] Zachová, A., & Pásztor, D. (2023, March 14). Criticism mounts over Czech implementation of EU cyber security. *Euractiv*. https://www.euractiv.com/section/politics/news/criticism-mounts-over-czech-implementation-of-eu-cyber-security/.
[266] Bird & Bird. (n.d.). *Czechia.* https://www.twobirds.com/en/trending-topics/copyright-directive/copyright-directive-countries/czech-republic.
[267] Connal, S. (2022, December 12). *Updates to Google's services in Czechia in light of the Czech transposition of the European Copyright Directive*. Google. https://developers.google.com/search/blog/2022/12/google-services-in-czechia
[268] Connal, S. (2022, December 12). *Updates to Google's services in Czechia in light of the Czech transposition of the European Copyright Directive*. Google. https://developers.google.com/search/blog/2022/12/google-services-in-czechia

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.

Taxation of Digital Products and Services

In 2019, the government proposed a DST of 7% on revenues from companies with an annual global turnover of more than €750 million and a turnover of more than CZK100 million.[269] Although there have been no decisions on implementing this plan, CCIA urges USTR to encourage the Czech Republic to formally abandon what would be a discriminatory tax on U.S. suppliers.

Ecuador

Potential Challenges to the Development of Artificial Intelligence

In September 2025, Ecuador's Data Protection Authority (SPDP) introduced a draft bill, "General Regulations for the Guarantee of the Right to Personal Data Protection in the Use of AI,"[270] representing a significant potential trade barrier that threatens U.S. companies' market access and operational capabilities. The draft creates multiple compliance challenges through jurisdictional overreach, as it conflicts with the Digital Transformation Law (LOTDA),[271] which designates the Ministry of Telecommunications and Information Society as the country's AI governance authority. The proposal imposes significant operational burdens on foreign technology providers through mandatory human supervision requirements, complex traceability standards, and expansive audit rights, going well beyond common international regulatory approaches. Of particular concern are the blanket prohibitions on key AI applications, including real-time biometric identification systems and synthetic content generation, which effectively bar U.S. firms from deploying innovative technologies in Ecuador. These restrictions, combined with excessive compliance costs and overlapping institutional mandates, would disproportionately burden U.S. businesses, especially startups and SMEs. The draft regulation imposes unnecessary and trade-distortive obstacles, creating legal uncertainty and compliance risks that undermine U.S. companies' ability to compete effectively in Ecuador's digital economy.

[269] Smith, J. (2019, September 5). *Czech finance ministry proposes 7 percent DST*. TaxNotes. https://www.taxnotes.com/featured-news/czech-finance-ministry-proposes-7-percent-dst/2019/09/05/29x7d.
[270] *Reglamento Inteligencia Artificial* [Ecuador] Resolution SPSP-XXX-XXX-XXX. (2025). https://www.scribd.com/document/915659366/pr-REGLAMENTO-INTELIGENCIA-ARTIFICIAL-0825-postdaj.
[271] *Ley Orgánica para la transformación digital y audiovisual* [Ecuador]. (2023). https://lexadvisorecuador.com/2023/02/09/ley-organica-para-la-transformacion-digital-y-audiovisual-ecuador/.

Egypt

Customs-Related Restrictions and Import Barriers for Goods

Egypt's import regime is marked by inconsistent application and a lack of transparency in customs processes, creating significant barriers for businesses, particularly smaller e-commerce firms and those engaging in cross-border trade. For instance, customs valuation practices often deviate from WTO-compliant methodologies, with declared values on commercial invoices, even those sealed by the Chamber of Commerce in the country of origin, frequently disregarded.[272] Discrepancies in HS codes can lead to goods being reclassified under higher tariff categories, and specific practices, such as a 50% value uplift on spare parts under service contracts, further inflate costs. Such inconsistencies, coupled with fines equal to the levied tariffs and the additional costs associated with protesting valuations, undermine predictability and efficiency in the import process.

In addition, businesses wishing to import goods into Egypt face stringent registration requirements, including the need to set up a permanent establishment (PE) in the country.[273] The Simplified Vendor Registration System obligates non-resident firms to register with the Egyptian Tax Authority, while PE rules define a PE as any fixed place of business or service operation lasting over 90 days in a 12-month period. These requirements, which also include navigating complex tax obligations and avoiding inadvertent PE triggers, place a significant administrative and financial burden on smaller e-commerce businesses. For many, the lack of resources and expertise to comply with these regulations restricts their ability to enter and compete in the Egyptian market. Together, these challenges create an unpredictable trade environment and limit opportunities for smaller businesses to benefit from Egypt's growing digital and regional shipping potential.

Government-Imposed Content Restrictions and Related Access Barriers

The Supreme Council for Media Regulation (SCMR), established under Law No. 180 of 2016,[274] serves as the central regulatory body for Egypt's media sector. Its responsibilities include issuing licenses for television, radio, newspapers, and online platforms, as well as monitoring media content to ensure it aligns with Egyptian cultural values. The SCMR has the authority to impose fines and refer cases to the Public Prosecutor's Office for potential legal violations. Compliance

[272] *Inconsistent customs valuation of imports in different ports*, European Commission Access2Markets (updated Apr 29, 2025), https://trade.ec.europa.eu/access-to-markets/nl/barriers/details?isSps=false&barrier_id=14222
[273] *Doing Business in Egypt 2024, A Tax and Legal Guide*, PwC (2024), https://www.pwc.com/m1/en/tax/documents/doing-business-guides/dbie.pdf
[274] *Law No. 180 of 2018 on Press, Media and the Supreme Council for Media Regulation* [Egypt]. (2018). https://www.wipo.int/wipolex/en/legislation/details/19960.

with its requirements has introduced notable operational and financial burdens for both domestic and international companies.

In 2018, Egypt enacted a law requiring all social media users with more than 5,000 followers to obtain a license from the SCMR.[275] Additionally, in May 2020, Decree no. 26 established a detailed licensing regime for media and press outlets, including online platforms.[276] This regulation requires platforms to remove harmful content within 24 hours and obligates international companies to establish a local representative office to provide legal liability and act as point of contact for content related matters. Licensing fees for international platforms are set at EGP 3 million (US$63,000), and there are no safe harbor protections for foreign companies, increasing compliance complexity.

In June 2024, the SCMR reiterated its licensing requirements, issuing notifications to all digital and satellite platforms operating in Egypt to comply with relevant regulations under Law No. 180 of 2018, Prime Ministerial Decree No. 418 of 2020, and SCMR Decision No. 29 of 2020.[277] Platforms were given a 90-day grace period to regularize their status, with potential consequences for non-compliance, including financial penalties, service blocking, or license revocation. The enforcement of these requirements is supported by the National Telecommunications Regulatory Authority (NTRA) and the Central Bank of Egypt, which can restrict payments and access to non-compliant platforms. Notwithstanding these formal requirements, many digital platforms operate on an unlicensed basis but also face constant enforcement risks.

While the SCMR has primarily focused on over-the-top platforms such as regional streaming services, international platforms face additional requirements to meet compliance standards. Social media platforms, although not the current primary focus, also fall under the same regulations. Decree No. 92 of 2020 introduced an accreditation model for social media platforms, offering a less demanding alternative to licensing.[278] Accreditation requires companies to submit organizational documentation and platform details, but does not impose the operational or content-management obligations tied to full licensing. Importantly, the accreditation process does not specify penalties for companies that choose not to apply, and there is room for dialogue with the SCMR and NTRA in cases where platforms face challenges during compliance discussions. However, the accreditation model is not widely emphasized by the SCMR, and platforms are often guided toward pursuing full licensing. This can introduce additional

[275] Article 19. (2019). *Law on the Organisation of Press, Media, and the Supreme Council of Media.* https://www.article19.org/wp-content/uploads/2019/03/Egypt-Law-analysis-Final-Nov-2018.pdf
[276] Hashish, M. (2020, June 6). *Egypt's new press and media regulation era*. Soliman, Hashish & Partners. https://www.shandpartners.com/egypts-new-press-and-media-regulation-era/.
[277] Al Tamimi & Co. (2024, June 24). *Regulating Websites and Platforms in Egypt: Compliance Requirements*. https://www.tamimi.com/news/regulating-websites-and-platforms-in-egypt-compliance-requirements/
[278] *Decree No. 92* [Egypt]. (2020). https://issuu.com/decree_no_92_of_2020/docs/_.

operational and financial requirements, particularly for international entities navigating Egypt's regulatory environment.

On another note, in 2025, Egypt witnessed actions taken by security agencies, including the arrests of certain content creators, which have drawn significant public attention.[279] These measures were led by security agencies and were primarily focused on addressing national security concerns rather than targeting specific platforms or their operators. For example, scrutiny of certain platforms increased following a controversial incident involving false allegations against public figures, prompting swift action by the Ministry of Interior. These efforts aim to mitigate the spread of harmful or unethical content that may pose risks to societal stability, aligning with the broader goal of maintaining public order and safeguarding community values.

Restrictions on Cross-Border Data Flows

Egypt's Personal Data Protection Law (PDPL) No. 151/2020,[280] which entered into force in October 2020, imposes one of the most restrictive cross-border data transfer regimes globally: it combines "adequacy" - based set of restrictions with a mandatory licensing and permit system administered by the Personal Data Protection Centre (PDPC). Under Article 14, the transfer of personal data outside of Egypt is generally prohibited unless two stringent conditions are met: (1) the destination country must provide a level of protection equivalent to Egypt's PDPL, and (2) the data controller or processor must obtain a specific cross-border transfer license from the PDPC. Unlike the EU's adequacy framework, Egypt does not maintain a list of approved jurisdictions, leaving adequacy determinations to the discretion of the PDPC and adding a layer of uncertainty for businesses. The licensing process itself is burdensome, requiring extensive documentation, proof of financial and technical capabilities, and adherence to prescribed security requirements. Although Article 15 provides limited exceptions, such as transfers necessary for preserving life or health, legal claims, contract fulfillment, or compliance with international treaties, these still require explicit consent from the data subject and do not meaningfully reduce the administrative burden for most transfers. Violations of these rules carry severe penalties, including imprisonment and fines ranging from EGP 300,000 to EGP 5,000,000 (approximately US$9,700-US$161,000), as well as administrative sanctions like license suspension or revocation. This framework creates a high-friction environment for international data flows, imposing legal uncertainty and significant compliance costs on companies handling the personal data of Egyptian residents. The lack of transparency in adequacy determinations, the absence of mutual recognition mechanisms, and the mandatory licensing requirement effectively act as a

[279] Human Rights Watch. (2025, September 10). *Egypt: Mass crackdown targets online content creators*. https://www.hrw.org/news/2025/09/10/egypt-mass-crackdown-targets-online-content-creators.
[280] *Issuance of the Personal Data Protection Law* [Egypt] Law No. 151. (2020). https://eg.andersen.com/wp-content/uploads/2025/06/Law-No.-151-OF-2020.pdf

trade barrier, making Egypt one of the most restrictive jurisdictions for cross-border data transfers.

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."[281] Measures include industrial and competition policy, platform regulation and increased platform liability, regulation of AI 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. There are signs that European policymakers are beginning to recognize the negative impact of some of these policies, with the widely-regarded economist and statesman Mario Draghi linking Europe's failure to embrace digitally-friendly policies to one of its most pressing weaknesses, its lagging innovation and the inevitable consequence, dragging productivity.[282]

Asymmetric Platform Regulation

The Digital Markets Act (DMA) was adopted by the European Parliament and the Council of the EU on September 14, 2022.[283] The measure entered into force on November 1, 2022, and became applicable on May 2, 2023. Under these 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 that primarily capture U.S. technology companies, reflecting the intent certain of key policymakers.[284] Similarly, the list of "core platform services" excludes competing European rivals whose business models do not fit the narrow definition of a platform, thus shielding major European firms in media, communications, retailing, and advertising from the highly prescriptive and burdensome obligations that flow from designation

[281] Breton, T. (2023, September 5). *Tech and geopolitics: Building European resilience in the digital age* [LinkedIn post]. LinkedIn. https://www.linkedin.com/pulse/tech-geopolitics-building-european-resilience-digital-thierry-breton/; Fulton III, S. (2019, November 5). *After Brexit, will 5G survive the age of the European empire?* ZDNet. https://www.zdnet.com/article/after-brexit-will-5g-survive-the-age-of-the-european-empire/.
[282] European Commission. (2024). *The future of European competitiveness – A competitiveness strategy for Europe* [Part A]. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The+future+of+European+competitiveness+_+A+competitiveness+strategy+for+Europe.pdf.
[283] *Digital Markets* Act [European Union] Reg. 2022/1925. (2022). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC.
[284] Espinoza, Javier. (2021, May 13). EU Should Focus on Top 5 Tech Companies, Says Leading MEP. *Financial Times*. https://www.ft.com/content/49f3d7f2-30d5-4336-87ad-eea0ee0ecc7b.

under this measure. Although it originally considered designating up to 25 companies[285] as so-called "gatekeepers" under the DMA (a number that would have likely swept in European operators), in September 2023, the European Commission ultimately only designated six companies, and 22 of their services, as subject to the new rules. Five out of those six companies (the sixth is Chinese) and 21 of the 22 services are American.[286] That list remains unchanged.

From March 7, 2024, companies designated as gatekeepers have been prohibited from engaging in a range of business practices often considered pro-competitive (*e.g.,* maintaining products and services that benefit from integrative efficiencies) when offering designated "core platform services." Furthermore, the Commission has been vested with authority over approval for future digital innovations, product integrations, and engineering designs of U.S. companies ("specification proceedings"). 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 European rivals. Even where not resulting in immediate benefits to rivals, the creation of a forum where competitors effectively direct regulatory oversight and intervention provides them a powerful tool in handicapping successful U.S. firms, raising their costs and in several cases delaying the introduction of new products. CCIA has estimated that annual compliance costs for the five U.S. companies subject to these rules average US$200 million annually, or a total of up to US$1 billion, and individual firms have had to dedicate hundreds of thousands of engineering hours to redesign products to meet these rules.[287] These extraordinary costs contrast dramatically with the EU's own initial cost-benefit analysis, which estimated a per-gatekeeper cost of €1.4 million ($1.64 million)--*i.e.*, less than one-hundredth of reported actual costs.[288]

In this sense, the DMA represents a dramatic shift in competition enforcement, resulting in greater potential infringement on fundamental IP 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.

The European Commission is due to review the effectiveness of the DMA since its applicability: the executive body will have to report to the European Parliament and European Council and potentially suggest amendments to the legislation. To gather stakeholder feedback, the European

[285] European Commission. (2020). *Impact Assessment of the Digital Markets Act*. https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act.
[286] European Commission. (n.d.). *Gatekeepers*. https://digital-markets-act-cases.ec.europa.eu/gatekeepers.
[287] CCIA. (2025). *Costs to U.S. Companies from EU Digital Regulation*. https://ccianet.org/wp-content/uploads/2025/03/CCIA_EU-Digital-Regulation-Factsheet_reportfinal.pdf.
[288] European Commission. (2020). *Impact Assessment of the Digital Markets Act*. https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act.

Commission has opened a public consultation[289] and a call for evidence[290] on the DMA review. Industry has responded to these consultations[291] and continues engagement with the relevant directorates of the European Commission (Competition and Connect), but also with the European Parliament and Council, presenting the latest evidence gathered on the DMA on the significant negative impact that the legislation is having on U.S. businesses,[292] European businesses,[293] and consumers.[294] CCIA urges the U.S. government to engage likewise, and advance concrete proposals for mitigating the significant impediment to effective market access that the DMA represents.

On June 28, 2023, the European Commission proposed a framework to extend open banking rules beyond payments to other financial services, enabling customers to share their financial data with third-party providers, with explicit consent, to foster innovation, increase competition, and support more tailored financial products.[295] The proposal obliges financial institutions to provide access to customer data — including investments, insurance, and mortgages — under strict data protection rules such as GDPR, while setting out clear rights and obligations for both data holders and users. During the legislative process, however, both the Council and the European Parliament have introduced provisions excluding gatekeeper-designated companies from accessing such financial data, even where consumers explicitly consent.[296] This constitutes a categorical exclusion based on designation rather than conduct, without clear rationale, justification, or the possibility of appeal or proportionality assessment. With interinstitutional negotiations advancing, it now appears increasingly likely that the final text will exclude U.S. gatekeeper-designated companies.

---

[289] European Commission. (2024, March 6). *Consultation on the first review of the Digital Markets Act.* https://digital-markets-act.ec.europa.eu/consultation-first-review-digital-markets-act_en.
[290] European Commission. (2024, March 6). *Review of the Digital Markets Act.* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14831-Review-of-the-Digital-Markets-Act_en.
[291] CCIA. (2024, June 12). *CCIA Europe response to DMA review questionnaire.* https://ccianet.org/library/ccia-europe-response-to-dma-review-questionnaire/.
[292] Computer & Communications Industry Association. (2025, July). *Costs to U.S. companies from EU digital services regulation.* CCIA Research Center. https://ccianet.org/research/reports/costs-to-us-companies-from-eu-digital-services-regulation/.
[293] Cennamo, C., Kretschmer, T., Constantiou, I., & Garcés, E. (2025). *Economic impact of the Digital Markets Act on European businesses and the European economy.* DMC Forum. https://www.dmcforum.net/publications/economic-impact-of-the-digital-markets-act-on-european-businesses-and-the-european-economy/.
[294] Nextrade. (2025). *Impact of the Digital Markets Act (DMA) on consumers across the European Union.* https://www.nextradegroupllc.com/impact-of-the-dma-on-eu-consumers.
[295] *Regulation on harmonised rules on fair access and use of data (Data Act)* [European Union] Reg. 2023/2854. (2023). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302854&qid=1726842542116; *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for Financial Data Access and amending Regulations* (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554 [European Union] COM/2023/360. (2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0360.
[296] Flinders, Karl. (2025, September 23). *EU to shut door on Big Tech in financial data sharing*. Computer Weekly. https://www.computerweekly.com/news/366631407/EU-to-shut-door-on-Big-Tech-in-financial-data-sharing.

Barriers to the Deployment and Operation of Network Infrastructure

The European Commission published a draft EU Space Act (EUSA) in June 2025.[297] The proposed regulation would create an asymmetric regulatory regime where non-European satellite providers are subject to a cumbersome registration process via a "Compliance Board" within the EU Agency for the Space Programme (EUSPA). This regime creates a significant conflict of interest, as EUSPA will operates EU constellations that will compete directly with U.S. operators. By contrast, European operators will be able to register through their Member State. The combination of procedural hurdles for foreign firms combined with the risks to fairness and impartiality poses potential barriers to U.S. firms' market access. In addition, the definitions and requirements EUSA imposes on "giga-constellations," which applies to constellations with over 1,000 satellites, appear arbitrary and discriminatory. The current definition would only capture two U.S.-based constellations while excluding competing EU suppliers that are unlikely to surpass this limit. As a result, this measure imposes disproportionate regulatory burdens on U.S. firms and risks restricting their access to the EU market. The EU Space Act may also restrict certain communications services to EU-headquartered satellite operators.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

As part of the EU-wide push for "technological sovereignty," the EU continues to advance industrial policy proposals that could disadvantage U.S. cloud providers in key segments of the EU market. Potential new measures aim to 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 been developing the EU Cybersecurity Certification Scheme for Cloud Services (EUCS), initially building upon protectionist cybersecurity certification standards seen in France.[298] While earlier drafts of the EUCS included explicit eligibility requirements that discriminated against non-EU companies, the latest draft no longer contains such requirements. However, the adoption of EUCS has faced delays due to political uncertainty around such discriminatory bans. There are growing concerns that discriminatory requirements could be reintroduced in the EUCS through the reopening of the Cybersecurity Act. The German and French governments have announced in recent months their aim for an "ambitious revision" of the Cybersecurity Act to ensure a truly "sovereign cloud" – which can be assumed to mean EU based cloud providers only following SecNumCloud

---

[297] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the safety, resilience and sustainability of space activities in the Union* [European Union] COM/2025/335. (2025). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0335.

[298] European Union Agency for Cybersecurity. (2022, June 6). *Cybersecurity certification: Breaking new ground.* https://www.enisa.europa.eu/news/enisa-news/cybersecurity-certification-breaking-new-ground; AmCham EU. (n.d.). *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.

guidelines.[299] This would directly discriminate against U.S. providers, requiring companies that wish to be certified under the Cybersecurity scheme to be European.

In addition to EUCS, the European Commission has put forward the Cloud and AI development Act (CAIDA). CAIDA could lead to the creation of a European-only cloud infrastructure ecosystem aimed at serving public services and critical use cases. As 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 cloud service, this would likely refer to the European-only cloud ecosystem under CAIDA. The Dutch government has in recent months advocated for a common definition of cloud sovereignty to be included in the EU's Cloud and AI Development Act.[300] The European Commission also emphasized that it hopes to leverage the Cloud and AI Development Act to strengthen EU digital sovereignty.[301] Such development could lead to a general band on U.S. cloud providers based on an oversimplified definition of sovereign cloud meaning European based. In doing so, American based cloud providers are de facto discriminated against.

In 2023, the European Commission 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."[302] Many of those ICT products are currently supplied by U.S. companies,[303] 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 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 European Commission has been

---

[299] Hartmann, T. (2025, September 15). Against US digital 'predators,' France digital minister calls for a European 'pack hunt.' *Euractiv.* https://www.euractiv.com/news/against-us-digital-predators-france-digital-minister-calls-for-a-european-pack-hunt/; Gkritsi, E., Haeck, P., & Pollet, M. (2025, September 15). A quiet presence. *Politico Pro Morning Technology.* https://pro.politico.eu/news/a-quiet-presence.

[300] Haeck, P. (2025, September 15). EU must help governments to break with US cloud providers, says Netherlands. *Politico Pro.* https://pro.politico.eu/news/201811EU.

[301] Pollet, M., Haeck, P., & Gkritsi, E. (n.d.). Quantum takes center stage in Brussels. *Politico Pro Morning Technology.* https://pro.politico.eu/news/quantum-takes-center-stage-in-brussels.

[302] European Commission. (2023, October 3). *Commission recommends carrying out risk assessments on four critical technology areas: Advanced semiconductors, artificial intelligence, quantum, biotechnologies* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4735.

[303] 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 at European Commission. (2023, October). *Recommendation on critical technology areas for the EU's economic security, for further risk assessment with member states.* https://defence-industry-space.ec.europa.eu/system/files/2023-10/C_2023_6689_1_EN_annexe_acte_autonome_part1_v9.pdf.

working with national governments to complete the first round of risk assessments since the fall of 2023. Based on those assessments, the European Commission will reportedly announce new measures to mitigate economic dependencies.

The European Commission and the European Parliament have recently announced introducing European preference in public procurement for "strategic sectors" and technologies.[304] The intended goal is to "bolster resilience, security, competitiveness and strategic autonomy" by discrimination against non-European providers. In doing so, this would directly exclude American companies from being eligible for certain public procurement opportunities, including cloud computing based on the range of exclusions the European Commission decides to implement.

Forced Revenue Transfers for Digital News

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.[305] The EMFA was published in the Official Journal of the European Union on April 17, 2024.[306] In particular, the EMFA introduces a special treatment of media content on very large online platforms.[307] While the adopted text claims that this special treatment should not contradict the horizontal rules established in the Digital Services Act, the implementation will be challenging as the EMFA create additional complexity in interaction with other digital regulations.[308] The U.S. government should pursue engagement with European partners to ensure that the EMFA's implementation does not supersede or revise parallel legislation whose implementation is ongoing and 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

---

[304] *European Parliament resolution on public procurement* [European Union] 2024/2103(INI). (2025). https://www.europarl.europa.eu/doceo/document/TA-10-2025-0174_EN.html; von der Leyen, U. (2024). *Europe's choice: Political guidelines for the next European Commission, 2024–2029.* European Commission. https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en; *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: A competitiveness compass for the EU* [European Union] COM(2025) 30 final. (2025). https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en.

[305] European Commission. (2022, September 16). *European Media Freedom Act: Commission proposes rules to protect media pluralism and independence in the EU* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5504.

[306] *Regulation (EU) 2024/1083 of the European Parliament and of the Council establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act)* [European Union]. (2024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401083.

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

[308] CCIA. (2023, December 15). *EU Media Freedom Act: Dangerous precedent set by mandatory carrying of media content for 24 hours* [Press release]. https://ccianet.org/news/2023/12/eu-media-freedom-act-dangerous-precedent-set-by-mandatory-carrying-of-media-content-for-24-hours/.

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.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

The Commission proposed a "Digital Services Act" (DSA) in December 2020, which further departs from transatlantic norms on liability for online services.[309] The DSA 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.[310] The DSA entered into application for designated "very large online platforms" and "very large online search engines" on August 28, 2023, and for all services on February 17, 2024. These new rules 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 & takedown systems for hosting services, '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, risk assessments, yearly audits,[311] obligations to disclose the main parameters used in their recommendation systems, data access, and requirements to appoint a compliance officer. Fines can reach up to 6% of annual turnover. In certain cases, policymakers have proposed audits as a mechanism to analyze adherence to content regulation. However, such audits are often overly burdensome and fail to advance the overall content safety objective. Audits present undue operational and financial burdens, risks to proprietary information and user privacy, and where published, risks of exploitation by bad actors. On April 24, 2023, the European Commission designated the first very large online platforms and search engines. Out of the 20 services designated, the majority are U.S. firms.[312] The DSA's scoping based on size rather than risk levels results in greater burdens being placed on a few key firms, mostly U.S.-based, while high risk services with smaller user bases face far fewer obligations and less oversight.

The DSA was weaponized 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

[309] CCIA. (2020, April 9). *CCIA's submission to the EU DSA consultation.* https://www.ccianet.org/library-items/ccias-submission-to-the-eu-dsa-consultation/.
[310] *Regulation (EU) 2022/2065 of the European Parliament and of the Council on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act)* [European Union]. (2022). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:277:FULL&from=EN.
[311] CCIA. (2023, June 2). *Feedback on the Digital Services Act's draft delegated regulation, rules on the performance of audits.* https://ccianet.org/library/ccia-europe-draft-feedback-dsa-delegated-regulation-on-audits/.
[312] European Commission. (2024, October 11). *Supervision of the designated very large online platforms and search engines under DSA.* https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.

personalized targeted advertising undermines the horizontal normative purpose of the DSA proposal and harms European companies along with U.S. firms.

Throughout implementation, the European Commission continues to use the DSA to further regulate online services beyond the scope of the legislation.[313] As the Commission was building a database for online platforms to document their terms of service, information beyond what was required by the DSA was solicited from online service suppliers.[314]

In 2025, the Commission also worked on guidelines on protection of minors under the DSA, which were published in July 2025.[315] CCIA contributed to the work of the Commission in this respect and provided comments to the draft.[316] While they help clarify how to apply certain rules to guarantee online safety of minors, industry has expressed concern about fragmentation of rules at Member State level when it comes to potential bans on social media or requirements related to age verification.[317]

Online marketplaces, including a large number of U.S. companies, are required to compile a significant amount of information on traders before allowing them to use the marketplace to reach consumers. Given the high fines set out in the DSA, the verification burden this results in is high. As a result, marketplaces have an incentive to take down traders who are difficult to verify, meaning fewer products available online, and some categories of products considered too risky, simply 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.[318] The GPSR was published in the Official Journal of the European Union on May 23, 2023.[319] This regulation updates the existing Product Safety Directive to respond to new challenges related to online purchases including via marketplaces.[320] Building on the DSA, the

[313] Adjutor, M. (2022, October 20). The Digital Services Act's moment of truth: Implementation. *Disruptive Competition Project.* https://www.project-disco.org/european-union/102022-the-digital-services-acts-moment-of-truth-implementation/.
[314] CCIA. (2023, August 29). *Letter on transparency database for content moderation decisions.* https://ccianet.org/library/ccia-letter-on-transparency-database-for-content-moderation-decisions/.
[315] European Commission. (2024). *Commission publishes guidelines on the protection of minors.* https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors.
[316] CCIA. (2024). *CCIA Europe's feedback: Guidelines on protection of minors online under the DSA.* https://ccianet.org/library/ccia-europes-feedback-guidelines-on-protection-of-minors-online-under-the-dsa/.
[317] CCIA. (2024). *CCIA Europe letter on draft guidelines on minor protection pursuant to Article 28 of the DSA.* https://ccianet.org/library/ccia-europe-letter-on-draft-guidelines-on-minor-protection-pursuant-to-article-28-of-the-dsa/.
[318] European Commission. (n.d.). *The general product safety directive.* https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/consumer-product-safety_en.
[319] *Regulation (EU) 2023/988 of the European Parliament and of the Council on general product safety and amending Regulation (EU) No 1025/2012 and repealing Council Directive 87/357/EEC and Directive 2001/95/EC* [European Union]. (2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R0988.
[320] *Directive 2001/95/EC of the European Parliament and of the Council on general product safety* [European Union]. (2001). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32001L0095.

GPSR imposes further restrictions on online marketplaces by creating a stay down obligation forcing marketplaces to remove products identical to ones previously flagged by authorities.[321]

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.[322] The rules would 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 services 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 measures that could require providers to break end-to-end encryption and could result in an oppressive surveillance system.[323] The European Commission opened a public consultation through September 5, 2022, which CCIA responded to.[324] This proposal is still undergoing legislative scrutiny with Member States currently trying to find a common position in the Council. CCIA is actively involved in the negotiations, highlighting the need to reach an adequate balance between the protection of minors and safeguarding privacy rights for all users and opposing any proposal that could undermine encryption, including but not limited to end-to-end encryption.[325] Due to the delays in the adoption of this proposal and the looming expiration of the Interim regime allowing providers of interpersonal communications services to proactively scan their content to detect and report child sexual abuse material, the European Commission published a proposal in

---

[321] CCIA. (2022, November 29). *Product safety: Deal on new EU rules adds complexity for thousands of online marketplaces in Europe* [Press release]. https://ccianet.org/news/2022/11/product-safety-deal-on-new-eu-rules-adds-complexity-for-thousands-of-online-marketplaces-in-europe/.

[322] European Commission. (2022, May 11). *Fighting child sexual abuse: Commission proposes rules to protect children* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2976; *Proposal for a Regulation laying down rules to prevent and combat child sexual abuse (COM(2022) 209 final)* [European Union]. (2022). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472.

[323] James Vincent, *New EU rules would require chat apps to scan private messages for child abuse. The Verge.* (2022, May 11). https://www.theverge.com/2022/5/11/23066683/eu-child-abuse-grooming-scanning-messaging-apps-break-encryption-fears; EDRI. (2022, June 8). *Letter to European Commission.* https://edri.org/wp-content/uploads/2022/06/European-Commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law.pdf; *Open letter by academics and researchers on CSA Regulation.* (n.d.). https://docs.google.com/document/d/13Aeex72MtFBjKhExRTooVMWN9TC-pbH-5LEaAbMF91Y/edit; *Joint industry call for protecting encryption and limiting detection orders in the CSA Regulation.* (2023, September 6). https://ccianet.org/wp-content/uploads/2023/09/CSAM-Joint-call-for-safeguarding-encryption-and-limiting-detection-orders.pdf.

[324] CCIA. (2022, September). *CCIA position paper: The proposed EU regulation to prevent and combat child sexual abuse.* https://www.ccianet.org/wp-content/uploads/2022/09/CSAM-CCIA-Position-Paper-9-September-2022.pdf.

[325] *Protecting kids while respecting Europeans' rights: How to navigate the safety-privacy conundrum. Disruptive Competition Project.* (2024, June 11). https://project-disco.org/european-union/protecting-kids-while-respecting-europeans-rights-how-to-navigate-the-safety-privacy-conundrum/.

November 2023 to extend the temporary derogation from certain provisions of the e-Privacy Directive for the purpose of combating child sexual abuse. The European Commission opened a public consultation which CCIA responded to.[326] Given the time pressure brought by the expiration of the regime and a significant push from all stakeholders, including CCIA,[327] this proposal was quickly approved and published in the Official Journal of the European Union on April 29, 2024, and is applicable until April 3, 2026.[328] The upcoming expiration of this temporary framework, paired with the unwillingness by legislators to extend once again provisions that were only meant to be temporary raises questions for industry as to the possibility to reach an agreement that is lasting while still respecting the balance between online safety of minors and the right to privacy for all users.

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.[329] The new Regulation was published in the Official Journal of the European Union on March 13, 2024.[330] It requires any political advertisement to be clearly labelled and introduces new rules on political targeting and amplification techniques which go further than the restrictions on personalized targeted advertising already foreseen in the DSA. 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. As a result of these provisions, the entry into force of this legislative regime resulted in several U.S. companies withdrawing their political advertising services from the European market.

On May 17, 2019, the EU Copyright Directive was published in the Official Journal of the European Union, introducing major legal changes that significantly diverge from global IP norms and U.S. law.[331] Articles 15 (press publisher rights) and 17 (a de facto filtering obligation) impose unprecedented obligations on online service providers, with serious implications for U.S. companies' market access. Under Article 17, absent licensing from all relevant rightsholders, online services are directly liable for user uploads unless they make "best efforts" to obtain

---

[326] CCIA. (2024, February 8). *Feedback on proposal to combat online child sexual abuse – amending temporary derogation from certain provisions of Directive 2002/58/EC. European Commission.* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14053-Combating-online-child-sexual-abuse-amending-temporary-derogation-from-certain-provisions-of-Directive-2002-58-EC/F3454142_en.
[327] CCIA. (2024, January 23). *Fighting child sexual abuse: Looming legal vacuum requires urgent action, but long-term CSA regulation should remain priority* [Press release]. https://ccianet.org/news/2024/01/fighting-child-abuse-looming-legal-vacuum-requires-urgent-action-but-long-term-csa-regulation-should-remain-priority/.
[328] *Regulation (EU) 2024/1307 of the European Parliament and of the Council* [European Union]. (2024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401307.
[329] European Commission. (2021, November 25). *European democracy: Commission sets out new laws on political advertising, electoral rights and party funding* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6118.
[330] *Regulation (EU) 2024/900 of the European Parliament and of the Council on the transparency and targeting of political advertising* [European Union]. (2024). https://eur-lex.europa.eu/eli/reg/2024/900/oj/eng.
[331] *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* [European Union]. (2019). *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:130:FULL&from=EN.

licenses, "ensure the unavailability" of works identified by rightsholders, remove content expeditiously upon notice, and "prevent their future uploads," effectively creating an EU-wide "notice and staydown" obligation. The vague "best efforts" standard invites inconsistent interpretation and potential abuse across Member States. Although the CJEU's April 2022 ruling confirmed that the directive should not lead to a general monitoring obligation,[332] it did not prohibit upload filters outright, leaving legal uncertainty in place. This structure makes full compliance practically impossible, as no service can license every work, especially when rightsholders can refuse to license altogether, undermining the viability of user-generated content services in Europe.[333] CCIA has long argued that mitigation measures are needed to make Article 17 workable, including requiring notification of infringing uses, not just works, and adopting standardized rights information to facilitate compliance. Article 15 compounds these issues by creating a press publishers' right, obligating search engines, aggregators, and platforms to license snippets of news content—contrary to U.S. law and commercial practice. The narrow "short excerpts" exemption offers little legal certainty, and some Member States have introduced mandatory revenue-sharing with journalists, though evidence shows it has had negligible impact on journalist income. The Directive also fails to harmonize exceptions and limitations, omitting key concepts like freedom of panorama entirely and adopting a narrow text and data mining exception limited to "research organizations," excluding startups and individual researchers. National implementation has further fragmented the legal landscape: some governments are reinterpreting provisions in ways that heighten compliance burdens for foreign platforms. These cumulative legal and operational burdens, coupled with the lack of harmonized exceptions, create significant barriers for U.S. service providers, increase legal uncertainty, and risk chilling investment and innovation in Europe's digital economy.

The European Union enacted revisions to the DSA relating to liability for defective products in 2024.[334] 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 trader within a month. The revision also introduces changes that are likely to be disproportionately damaging for IT products, such as the inclusion of software in the definition of products and the de facto reversing of the burden of proof for complex products.[335]

---

[332] *Case C-401/19, Republic of Poland v. European Parliament and Council of the European Union* [European Union]. (2022). https://curia.europa.eu/juris/document/document.jsf?text=&docid=258261&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=758534.

[333] Moody, G. (2024, September 30). The Copyright Directive's Link Tax Has Been A Failure; Will Anyone Learn From This?*, TechDirt*. https://www.techdirt.com/2024/09/30/the-copyright-directives-link-tax-has-been-a-failure-will-anyone-learn-from-this/.

[334] *Directive (EU) 2024/2853 on liability for defective products* [European Union]. (2024), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402853.

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

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

In February 2023, in response to a campaign from incumbent European telecommunications providers, the European Commission launched an exploratory consultation on the financing of telecommunications networks. The consultation sought input on the suggestion that "large traffic generators" should make financial contributions, termed "network usage fees," to European telecommunications network operators to support network.[336] The incumbent telco association, the European Telecommunications Network Operators (formerly ETNO, now Connect Europe) proposed that large content and applications providers, mainly U.S. firms, should be required to pay fees to European ISPs to facilitate the delivery of content demanded by the ISPs' customers--analogous to the "sending-party--network pays" (SPNP) regime that reigned in telephony for over a century (and undermined efficient use of networks).

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 ISPs.[337] 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. Concerningly, the exploratory consultation appeared to accept the false "fair share" premise pushed by European telecom incumbents, with questions seemingly designed to justify the view that popular streaming and cloud services should be mandated by the EU to subsidize telecom operators. The technical nature of many questions narrowed participation to mainly tech and telecom firms thus excluding most stakeholders, notwithstanding the price they would pay.[338]

Given its focus on "large traffic generators," ETNO's proposal is by its very nature discriminatory (targeting certain CAPs but not others). It is also in tension with net neutrality principles, as it could justify the throttling or blocking internet users' access to specific services in case of a lack of agreement with content providers. Undermining the justification for such fees 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. 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 consultation, then-EU Commissioner

---

[336] European Commission. (2023). *The future of the electronic communications sector and its infrastructure.* https://digital-strategy.ec.europa.eu/en/consultations/future-electronic-communications-sector-and-its-infrastructure.
[337] ETNO. (2022, May). *Europe's internet ecosystem: Socio-economic benefits of a fairer balance between tech giants and telecom operators.* 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.
[338] CCIA. (2023, February). *Network fees: EU Commission launches consultation on telco demands* [Press release]. https://ccianet.org/news/2023/07/eu-countries-seal-data-transfer-deal-with-united-states-after-years-of-uncertainty/.

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."[339] The telco incumbents estimate that total payments under their proposal could amount to €20 billion annually.

Numerous member states have questioned a rush to instituting new fees.[340] In October 2022, the body of European telecom regulators (BEREC) stated that it "has found no evidence that such mechanism is justified" and warned 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 Open Internet Regulation (OIR). This is because it involves treating traffic unequally, contradicting the principles of equal treatment and non-discrimination 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)."[341]

The Commission released a summary of the responses received in the public consultation in October 2023, showing that a majority of respondents opposed any mandatory funding mechanism.[342] 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 to impose 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

---

[339] *Reuters*. (2022, September 9). EU to consult on making Big Tech contribute to telco network costs. *Reuters.* https://www.reuters.com/technology/eu-consult-big-tech-contribution-telco-networks-by-end-q1-2023-2022-09-09/.
[340] Bertuzzi, L. (2022, July 25). Seven EU Countries Warn the Commission Against Hasty Decisions on 'Fair Share.' *EURACTIV*. https://www.euractiv.com/section/digital/news/seven-eu-countries-warn-the-commission-against-hasty-decisions-on-fair-share/; *Reuters.* (2023, June 3). Majority of EU Countries Against Network Fee Levy on Big Tech, Sources Say. https://www.reuters.com/business/media-telecom/majority-eu-countries-against-network-fee-levy-big-tech-sources-say-2023-06-02/.
[341] BEREC. (2023). *BEREC response to the European Commission's Exploratory Consultation on the future of the electronic communications sector and its infrastructure*. https://www.berec.europa.eu/system/files/2023-05/BoR%20%2823%29%20131d%20Annex%20to%20Section%204.pdf.
[342] *The Register*. (2023, October 12). EU consultation on future telecoms cools on having big tech pay for network builds. https://www.theregister.com/2023/10/12/europe_comms_sector_future_consultation/; Internet Society. (2023, October 19). *Network Usage Fees: The European Commission Plays Politics with the Global Internet*. https://www.internetsociety.org/blog/2023/10/network-usage-fees-the-european-commission-plays-politics-with-the-global-internet/.

"Digital Networks Act").[343] In addition to commissioning a follow-on white paper, 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 infrastructure operators in the Single Market, accelerate deployment of technologies and attract more capital into networks."[344]

The white paper's consultation results were published in September 2024 and showcase similar widespread opposition against proposals for introducing network fees. Most recently, the new Executive Vice-President for Tech Sovereignty, Security and Democracy Henna Virkkunen, received a mission letter[345] from Commission President Von der Leyen, in which she is tasked to "work on a new Digital Networks Act to help boost secure high-speed broadband, both fixed and wireless. You should incentivize and encourage investments in digital infrastructure, taking into account responses to the Commission's White Paper of February 2024." A CCIA analysis found that 67% of respondents in the most recent consultation voiced opposition to regulatory intervention in the IP interconnection market.[346]

This issue remains front-and-center, as Deutsche Telekom (DT) has recently sought to leave behind the long-standing and mutually beneficial process of free peering relationships, to instead require large customers to pay DT extra funds to allow DT customers to access U.S. firms' services on DT networks.[347] In response, one U.S. firm has terminated its peering relationship with DT,[348] in response to actions that broadband policy expert Barbara van Schewick highlighted as blatantly violative of the EU's network neutrality rules: "If your website or service uses a hosting provider or content delivery network that isn't paying Deutsche Telekom for a direct, uncongested connection, your site or service will load slowly for Deutsche Telekom subscribers in Germany, and you may not even know it. If you buy internet access from Deutsche Telekom, you pay Deutsche Telekom for a fast connection to the internet. But whether the apps and services you want to use actually work well, completely depends on whether they

---

[343] Breton, T. (2023, October). *A "Digital Networks Act" to redefine the DNA of our telecoms regulation.* LinkedIn. https://www.linkedin.com/pulse/digital-networks-act-redefine-dna-our-telecoms-thierry-breton/.
[344] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* [European Union]. (2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022DC0230.
[345] *Mission letter to Henna Virkkunen from the European Commission* [European Union]. (2024). https://commission.europa.eu/document/download/3b537594-9264-4249-a912-5b102b7b49a3_en?filename=Mission%20letter%20-%20VIRKKUNEN.pdf.
[346] Stecher, M. T. (2024, September 23). Consultation on EU's Future Connectivity Networks: (Again) No Support for Regulatory Intervention. *Project DisCo*. https://project-disco.org/european-union/consultation-on-eus-future-connectivity/.
[347] Bode, K. (2024, September 27). *Meta, Deutsche Telekom Standoff in The EU Is Something to Keep an Eye On.* Tech Dirt. https://www.techdirt.com/2024/09/27/meta-deutsche-telekom-standoff-in-the-eu-is-something-to-keep-an-eye-on/.
[348] Meta. (2024, September 25). *Why We're Having to End Our Direct Peering Relationship With Deutsche Telekom*. https://about.fb.com/news/2024/09/why-were-having-to-end-our-direct-peering-relationship-with-deutsche-telekom/.

have paid Deutsche Telekom's ransom. That violates Europe's net neutrality law. The law protects people's right to use the applications of their choice; that right is not limited to apps that have paid people's ISP.**"**[349]

In June 2025, the European Commission launched a call for evidence and questionnaire on the Digital Networks Act, to which CCIA Europe responded.[350] In this consultation, the Commission identified as a problem to be solved, the "challenges in the cooperation between the various digital players in the digital infrastructure ecosystem." This phrasing hints at the relationship between CAPs and incumbent telecom operators for the transport of data and suggests the potential establishment of a dispute resolution mechanism in the IP interconnection. Specifically, due to continued lobbying from European telcos, and despite broad opposition from industry, consumer associations, civil society organizations and telecoms regulators, the Commission is considering using the Digital Networks Act to extend the European Electronic Communications Code (EECC) to IP interconnection. This would make internet-enabled CAPs and CDNs subject to out-of-court dispute resolution mechanisms in commercial disputes with telcos. The introduction of these dispute resolution mechanisms would allow European telecommunications operators, who control access to internet users as 'termination monopolies,' to launch interconnection disputes against CAPs and CDN providers, and extract additional payments for the delivery of internet traffic to users. This would result in a proliferation of disputes against CAPs and CDN providers that deliver the majority of internet content, with U.S. providers being the primary targets. By multiplying disputes against U.S. CAPs and CDN providers, and building on the precedent set by these disputes, European telecommunications operators will be able to establish de facto network fees. Such a move would lead to the introduction of network usage fees,[351] directly contradicting the recent EU-US trade agreement, where the European Union expressly confirmed that it would not adopt or maintain network usage fees.[352] In addition to considering the introduction of backdoor network fees, the Commission is also evaluating an extension of the EECC to 'private networks' operated by large technology and content providers. This approach would result in an asymmetric regulatory intervention, mainly impacting U.S. cloud services and infrastructure (including submarine cables), and satisfying ambitions from

---

[349] van Schewick, B. (2024, September 25). *A Deutsche Telekom Shakedown: Will Instagram, Facebook and WhatsApp slow to a crawl in Germany as DT tries to get paid twice, and will German regulatos have the courage to stop DT's bullying?* CIS. https://cyberlaw.stanford.edu/blog/2024/09/a-deutsche-telekom-shakedown-will-instagram-facebook-whatsapp-slow-to-a-crawl/.

[350] European Commission. (2025). *Have your say: Digital Networks Act*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14709-Digital-Networks-Act_en; CCIA. (2025). *CCIA Europe Response to Digital Networks Act call for evidence*. https://ccianet.org/library/ccia-europe-response-to-digital-networks-act-call-for-evidence/.

[351] Felten, B. (2025, May 7). *Study on the negative impacts of mandated dispute resolution in IP Interconnection*. Plum. https://plumconsulting.co.uk/study-on-the-negative-impacts-of-mandated-dispute-resolution-in-ip-interconnection/.

[352] European Commission. (2025, August 21). *Joint Statement on a United States-European Union framework on an agreement on reciprocal, fair and balanced trade*. https://policy.trade.ec.europa.eu/news/joint-statement-united-states-european-union-framework-agreement-reciprocal-fair-and-balanced-trade-2025-08-21_en.

European telecommunications operators to become alternatives to U.S. cloud through regulatory intervention rather than market competition. The European Commission is expected to publish the Digital Networks Act in December 2025, even though it is likely that the publication will be delayed to 2026.

CCIA urges USTR to continue engaging the EU firmly to dissuade the advancement of discriminatory and anticompetitive rules forcing network usage fee in whatever name or form,[353] and welcomes efforts to date,[354] which appears to have materially helped resist the adoption of this policy so far.

Potential Challenges to the Development of AI

In June 2024, the EU adopted the AI Act, the world's first comprehensive horizontal framework for regulating artificial intelligence across all sectors, with the stated objective of supporting AI innovation in the EU while protecting EU citizens. The regulation entered into force in August 2024 and will be phased in between February 2025 and August 2027, establishing a risk-based framework that categorizes AI systems into prohibited, high-risk, and low-risk categories. The Act is being operationalized through a series of Implementing Acts and harmonized standards developed by CEN and CENELEC (JTC 21), which aim to provide a common framework for AI trustworthiness, risk management, and quality assurance. However, these standards are not expected before mid-2026, creating serious timing challenges since compliance for high-risk systems begins in August 2026. To address this, industry has called for a delay in application, and the European Commission is considering targeted legislative amendments through the upcoming Digital Omnibus. It remains uncertain whether EU standards will fully align with ISO standards (e.g., ISO 42001); if not, firms will face dual compliance burdens. The Act also imposes training data transparency obligations for general-purpose AI models, requiring providers to submit a "sufficiently detailed" disclosure of their training data using a Commission-developed template finalized in July 2025. U.S. and global industry stakeholders have raised concerns about the commercial sensitivity of such disclosures, including potential exposure of trade secrets and the unclear interaction with EU copyright law, which the Commission may apply extraterritorially to any model, regardless of where training occurred.

Like the GDPR, the AI Act is designed to set global norms and exert regulatory influence internationally. It defines "AI system" in line with the OECD definition, applying risk-based obligations: low-risk systems are subject to transparency obligations, high-risk systems must undergo conformity assessments, auditing, and post-market monitoring, and prohibited systems are banned outright. Additional obligations introduced late in the legislative process target

[353] Arts, P. & Conlow, M. (2023, May 8). *The European Network Usage Fees proposal is about much more than a flight between Big Tech and Big European telcos*. Cloudflare. https://blog.cloudflare.com/eu-network-usage-fees/.
[354] U.S. National Telecommunications and Information Administration. (2023, May 25). *United States comments on European Consultation: "The future of the electronic communications sector and its infrastructure."* https://www.ntia.gov/other-publication/2023/united-states-comments-european-consultation-future-electronic.

general-purpose AI models, with stricter requirements for those posing systemic risks. A voluntary Code of Practice for such models was released in August 2025, endorsed by many providers. The law applies to both providers and users of AI systems where outputs are used in the EU, and fines for non-compliance can reach 7% of annual global turnover. Despite partial alignment with OECD frameworks, the AI Act suffers from definitional ambiguity—particularly around what constitutes an AI system, a general-purpose AI model, and high-risk or prohibited applications. Unclear allocation of responsibilities along the value chain between providers and deployers, combined with the expansive definition of "high-risk", creates complex, often unworkable compliance obligations, particularly for SMEs and U.S. companies. The vague wording of some prohibited categories introduces additional legal uncertainty, potentially restricting low-risk applications.[355] This compliance environment, coupled with administratively burdensome obligations and steep penalties, has already led some firms to limit AI product offerings in Europe. In response to these concerns, the European Commission launched a consultation in September 2025 to explore simplification measures and reduce regulatory burden, with potential adjustments expected in the Digital Omnibus Package planned for late 2025.

Restrictions on Cross-Border Data Flows

The EU's evolving privacy framework, anchored in the General Data Protection Regulation (GDPR), which entered into force on May 25, 2018,[356] has created increasing compliance burdens and legal uncertainty for U.S. exporters, particularly small businesses. The GDPR seeks to harmonize EU data protection rules and regulate personal data transfers abroad, but its complexity and cost have already prompted some businesses and online services to withdraw from the EU market. Since its adoption, app market exits have increased while new innovation has slowed.[357] This foundational regulation has been layered with additional, often asymmetric rules targeting U.S. firms, including the DMA, which prohibits five major U.S. companies from internal data sharing without consent; the Data Act, which restricts these same firms from receiving data from their own services even with user consent; the DSA, which limits advertising based on special data categories; and the proposed e-Privacy Regulation, which could subject routine data processing (e.g., messaging and email) to strict consent requirements. These overlapping obligations exacerbate regulatory fragmentation, driving up compliance costs and creating uncertainty for transatlantic operators.

---

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

[356] *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* [European Union] 95/46/EC, 2016 O.J. (l 119). (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[357] Janßen, R., Kesler, R., Kummer, M. E. & Waldfogel, J. (2022). *GDPR and the Lost Generation of Innovative Apps*. NBER. https://www.nber.org/papers/w30028.

Compounding these challenges, transatlantic data transfers have faced prolonged instability following the 2020 CJEU Schrems II decision. Though partially resolved with the U.S. Executive Order on Signals Intelligence and the EU-U.S. Data Privacy Framework adequacy decision in 2023,[358] retroactive liability remains a risk. The EDPB and the Dutch Data Protection Authority have fined companies for transfers made during the interim period,[359] despite the lack of practical compliance mechanisms, illustrating the rigid and formalistic approach of EU enforcement. These actions have disproportionately impacted U.S. companies, particularly those already subject to GDPR. While an annulment challenge was brought against the adequacy decision by French lawmaker Philippe Latombe, the EU General Court recently upheld the Commission's determination that U.S. safeguards are adequate.[360]

GDPR also imposes operationally burdensome obligations through its "right to erasure" (Article 17), requiring companies to delete personal data "without undue delay" under several conditions. For large platforms, this has translated into processing hundreds of thousands of deletion requests, each requiring individual review.[361] For smaller U.S. firms, this can be an entry barrier, as they lack the resources to handle such high volumes of legally sensitive requests. Additionally, GDPR noncompliance can lead to fines of up to 4% of global turnover, amplifying risk exposure.

Further complicating the regulatory landscape, an Advocate General opinion issued in September 2022 recommended that any European authority, not just data protection authorities, could investigate and enforce GDPR.[362] It also suggested that companies could be barred from processing personal data for personalized services, ad delivery, and integrated product experiences without explicit user consent, and that dominant companies could face restrictions even when consent is obtained. This expansion of enforcement authority undermines legal predictability, increases exposure to multi-agency interventions, and significantly raises the cost and risk of operating in the EU market for U.S. businesses.

---

[358] CCIA. (2022, October 7). Transatlantic Data Flows: CCIA Welcomes Signing of Executive Order Enhancing Privacy Protections for Europeans and Facilitating Transfer. https://www.ccianet.org/2022/10/ccia-welcomes-signing-of-executive-order-enhancing-privacy-protections-for-europeans-and-facilitating-transfers/; CCIA. (2023, July 10). *Press Release, EU Countries Seal Data Transfer Deal With United States After Years of Uncertainty*. https://ccianet.org/news/2023/07/eu-countries-seal-data-transfer-deal-with-united-states-after-years-of-uncertainty/.

[359] European Data Protection Board, (2023). 1.2 billion euro fine for Facebook as a result of EDPB binding decision. [Press Release]. https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en; *Besluit boete Uber doorgifte naar VS* [Netherlands]. (2024). https://www.autoriteitpersoonsgegevens.nl/system/files?file=2024-08/Besluit%20boete%20Uber%20doorgifte%20naar%20VS.pdf.

[360] *Case T-553/23, Latombe v. Commission* [European Union]. (2025). https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-09/cp250106en.pdf.

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

[362] *Case C-252/21, Meta Platforms Inc., et al. v. Bundeskartellamt* [European Union]. (2023). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021CC0252&from=en.

The EU Data Act, adopted in November 2023 and entering into force in January 2024, builds on the Digital Markets Act and Digital Services Act to regulate how companies can access, process, and share personal, commercial, and industrial data generated within the EU.[363] It introduces prescriptive rules governing when, where, and how data can be used, including restrictions on U.S. companies: gatekeepers are barred from becoming third parties for receiving EU Internet-of-Things data;[364] separate regimes apply to cross-border transfers of non-personal data for cloud service providers subject to third-country data access requests; companies face obligations to share data containing proprietary information; and national regulators may be empowered to enforce aspects of the law, risking fragmented, duplicative oversight across the 27 Member States. These requirements could place U.S. companies at a disadvantage in the fast-evolving IoT market.

The Data Governance Act (DGA), published in June 2022 and enforceable since September 24, 2023, further expands EU restrictions by regulating transfers of non-personal data held by public intermediaries to third countries when protected by EU trade secrets or IP.[365] Modeled on GDPR, it applies mechanisms such as adequacy decisions, consent, and standard contractual clauses, and imposes outright bans for sensitive non-personal data, thereby extending data transfer restrictions beyond personal data to include a broad range of industrial and commercial information. Together, the Data Act and DGA create a complex, overlapping regulatory framework that increases compliance costs and legal uncertainty for foreign providers, especially U.S. firms.

Threats to the Security of Devices and Services

The EU cybersecurity directive ('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). This could also include the obligation for such providers to be certified against an EU certification scheme to be developed under the EU Cybersecurity Act ('CSA').[366] Currently, this scheme is voluntary. One of the first EU cybersecurity schemes under development relates to cloud services and previous drafts of the scheme featured overt discriminatory requirements against non-EU cloud providers. The NIS2 Directive also intensifies reporting requirements and punishments. The implementing regulation for this law features an excessively low incident reporting threshold which is likely to result in over-reporting of

---

[363] *Regulation (EU) 2023/2854 on Harmonised Rules on Fair Access to and Use of Data* [European Union] (2023). https://eur-lex.europa.eu/eli/reg/2023/2854.
[364] Breton, T. (2023, April 5). *A European Cyber Shield to step up our collective resilience: Opening of the International Cybersecurity Forum* [Speech]. *European Commission.* https://ec.europa.eu/commission/presscorner/detail/en/speech_23_2145.
[365] *Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)* [European Union]. (2022). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.
[366] *Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity Across the Union* [European Union]. (2022). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.

insignificant incidents that do not pose real risks to society or the economy.[367] Member states had until October 17, 2024 to transpose NIS2 into national law, but as of September 2025, or 14 of the 27 member states had done so.[368]

In October 2023, the European Union adopted the Cyber Resilience Act (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.[369] The 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. This elaborate approval process has the potential to lead to major delays in both consumer and non-consumer goods as already seen with the approval of process related to the delegated regulation under the Radio Equipment Directive with companies having to wait up to 6 months to have their products approved. The CRA also has ramifications for all services which use software and hardware covered by the CRA throughout their supply chain, including 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, which 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.[370]

Other Barriers to Digital Trade

The Foreign Subsidies Regulation (FSR) entered into force on July 12, 2023, establishing an expansive framework designed to address what the European Commission characterizes as "distortions" in the EU single market caused by financial contributions from non-EU governments.[371] The FSR defines subsidies broadly as any financial contribution provided directly or indirectly by a non-EU government that confers a selective benefit on a company or sector.[372] While the regulation was politically framed as a tool to counter Chinese subsidies, in

---

[367] European Commission. (n.d.). *Cybersecurity risk management & reporting obligations for digital infrastructure, providers and ICT service managers*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en.

[368] ECSO. (n.d.). *NIS2 Directive Transposition Tracker*. https://ecs-org.eu/activities/nis2-directive-transposition-tracker/.

[369] European Commission. (2022, September 15). *Cyber Resilience Act*. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[370] Clasen, A. (2024, March 10). Cyber Resilience Act: Disclosure requirement concerns raised by experts. *EURACTIV*. https://www.euractiv.com/section/cybersecurity/news/cyber-resilience-act-disclosure-requirement-concerns-raised-by-experts.

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

[372] 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. European Commission. (n.d.). *Facing the challenges of globalisation*. https://ec.europa.eu/competition/international/overview/proposal_for_regulation.pdf.

practice it also captures U.S. firms, subjecting them to heavy disclosure and compliance obligations. Since October 2023, companies participating in public procurement procedures valued at €250 million or more, or in M&A transactions with aggregate EU revenues exceeding €500 million, have been required to notify the Commission of all non-EU financial contributions received up to three years prior. The Commission can also investigate ex officio outside these contexts, with powers to disqualify companies from tenders, restrict mergers and acquisitions, or impose redressive measures such as subsidy repayments if it finds a subsidy "distortive." Compliance with these requirements has proven exceptionally onerous, with FSR filings often the most resource-intensive filings for any global transaction. U.S. companies, in particular, face disproportionate burdens, as they must track and report on a wide range of U.S. federal, state, and local incentive schemes that do not fall under the FSR's own definition of a subsidy, respond to expansive and repeated information requests, and meet unrealistic deadlines. Despite thousands of notifications, the Commission has initiated only a handful of investigations and issued just one formal decision, revealing the regulation's high compliance costs with minimal policy benefit. In March 2025, the Commission issued draft guidelines that would significantly expand the FSR's scope,[373] notably by introducing a cross-subsidization theory allowing subsidies with no EU nexus to be deemed distortive if they "free up" resources for use in the EU, by lowering the distortion test to a "reasonable link" between the subsidy and alleged harm (even if minor or ancillary), and by broadening procurement notification obligations to include financial contributions from any entity in a corporate group under vague circumstances. This broad interpretation dramatically increases legal uncertainty, undermines predictability for businesses, and creates disproportionate compliance costs and administrative burdens for U.S. firms seeking to participate in public tenders or M&A transactions in the EU. Collectively, these developments risk deterring U.S. investment, slowing cross-border transactions, and weakening transatlantic economic ties.

The EU's Corporate Sustainability Due Diligence Directive (CS3D),[374] adopted in 2023, poses significant and disproportionate compliance costs for U.S. companies due to its extraterritorial scope and expansive obligations. For most U.S. businesses active in the EU, the directive requires the implementation of prescriptive sustainability-related due diligence obligations at the level of the U.S. parent company and all subsidiaries, extending to supplier relationships worldwide, even in the absence of a direct EU nexus. These requirements will compel companies to conduct complex and resource-intensive risk management and monitor activities across global operations, with direct implications for contractual arrangements and supply chain structures. The EU institutions are currently revising the CS3D as part of the "Omnibus I Package," which proposes amendments to the law's due diligence obligations, penalties, and civil liability

[373] European Commission. (n.d.). *Guidelines on foreign subsidies distorting the internal market*. https://competition-policy.ec.europa.eu/public-consultations/guidelines-foreign-subsidies_en.
[374] *Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859* [European Union] PE/9/2024/REV/1. (2024). https://eur-lex.europa.eu/eli/dir/2024/1760/oj/eng.

provisions, with a final agreement expected in late 2025. This revision could address several key concerns for U.S. businesses, including: (1) the directive's unprecedented extraterritorial reach, which affects all subsidiaries and suppliers regardless of location; (2) mandatory adoption of prescriptive due diligence systems across global operations, creating costly and time-consuming compliance exercises; (3) open-ended supply chain obligations, which make it difficult for firms to demonstrate adequate risk mitigation; (4) significant and potentially uncapped financial penalties, adding to legal and operational uncertainty; and (5) fragmented litigation risks across 27 EU Member States, which remain substantial even if mandatory EU-wide civil liability is excluded. Together, these provisions create a high-risk regulatory environment that could distort trade and investment decisions for U.S. companies engaged in or with the European market.

The European Union is implementing major new defense funding and investment initiatives that are reshaping market access conditions for foreign suppliers. The Security Action for Europe (SAFE) framework,[375] approved in May 2025, establishes a €150 billion loan instrument for defense procurement with strict European preference provisions that introduce tiered eligibility requirements for providers. For contracts exceeding 35% of the total value of SAFE loans, providers must be EU/EEA/EFTA/Ukraine-based, maintain local executive management, and demonstrate freedom from third-country control, undergo FDI screening, or provide security guarantees. Contracts representing 15–35% of total loan value require providers to be established with executive management in eligible regions or have existing contractor relationships, while maintaining the same control and screening obligations. Only contracts under 15% of total value are exempt from these eligibility requirements, creating significant structural barriers for non-EU defense and dual-use technology providers. The European Defense Industrial Programme (EDIP), a €1.5 billion funding instrument, is currently in negotiations after stalling in late 2024, with discussions resuming following SAFE's adoption and incorporating similarly restrictive European preference requirements. U.S. industry has proposed several technology-specific exemptions, including allowing technology services to qualify if delivered from EU/EEA territory, certified for classified information processing, and free from foreign military export controls, while also recommending a shift toward operational sovereignty rather than ownership and clearer requirements for software where foreign entities retain IP but European operators maintain operational control. Looking ahead, the 2028–2034 Multiannual Financial Framework (MFF) allocates €131 billion to defense and space, five times more than the previous MFF, and is expected to replicate the European preference requirements embedded in SAFE and EDIP. This trend toward preference-based procurement in strategic sectors signals an increasingly closed market for non-EU defense and dual-use technology providers, including U.S. firms, raising serious concerns about discriminatory treatment, market fragmentation, and reduced transatlantic defense cooperation.

[375] *Council Regulation (EU) 2025/1106 of 27 May 2025 establishing the Security Action for Europe (SAFE) through the Reinforcement of the European Defence Industry Instrument (Text with EEA relevance)* [European Union] ST/7926/2025/INIT. (2025). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R1106.

The European Commission is expected to propose a "Circular Economy Act" at the end of 2026, with the aim of strengthening EU circular economy models and facilitating the free movement of circular products, secondary raw materials, and waste. The proposal will also seek to increase the supply of high-quality recycled materials and stimulate demand for them within the EU. As part of this initiative, the Commission is reportedly considering making public procurement a central pillar, using it as a lever to drive demand for circular materials. In her 2025 State of the Union address, Commission President Ursula von der Leyen announced: "we will introduce a 'made in Europe' criterion in public procurement. [...] I am convinced: the future of clean tech will continue to be made in Europe. But for that, we also need to make sure that our industry has the materials here in Europe." Such European content requirements in public procurement would likely limit the market share of non-EU companies, creating new barriers to the free flow of goods and services between the EU and its global partners. Such requirements could also be inconsistent with EU obligations under the WTO Government Procurement Agreement.

France

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In March 2022, ANSSI, the French cybersecurity authority, instituted a cybersecurity certification and labeling initiative, SecNumCloud, that explicitly discriminates against non-French cloud providers serving the public sector and over 600 companies that operate "vital" and "essential" services.[376] Problematic provisions include requirements that "[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 a prohibition on veto power for non-EU entities (Article 19.6).[377] The certification standard is no longer voluntary—tenders have been published with SecNumCloud verification as a requirement.[378] The only companies verified to date under SecNumCloud have been French.[379] The Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique de France (the Ministry of the Economy, Finance and Industrial and Digital Sovereignty of France) has suggested that it could mandate its own SecNumCloud scheme to the broader private sector by defining "sensitive data," and

[376] ANSSI. (2022, March 9). *L'ANSSI actualise le référentiel SecNumCloud*. https://cyber.gouv.fr/actualites/lanssi-actualise-le-referentiel-secnumcloud.
[377] ITIF. (2021). *SecNumCloud 3.2.a*.[translation]. https://www2.itif.org/2021-secnumcloud-3.2.a-english-version.pdf.
[378] Official Journal of the EU. (n.d.). *399127-2022 - Competition*. https://ted.europa.eu/udl?uri=TED:NOTICE:399127-2022:TEXT:EN:HTML&tabId=0.
[379] ANSSI. (2025). *Liste des produits et services qualifies*. https://cyber.gouv.fr/prestataires-de-services-dinformatique-en-nuage-secnumcloud.

subsequently declaring when SecNumCloud would be required.[380] Further, some legislators are trying to expand certification requirements in subsequent legislation to health data.[381]

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.[382] While such extraterritorial reach is, for the United States, not new, it now has parallels in the EU, which passed an analogous "E-Evidence" law in July 2023, which allows EU member states to access data with a nexus to the EU wherever it is stored (including outside the EU).[383]

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 favorably than another locally-established supplier on the basis of the degree of foreign affiliation or ownership."[384] In addition to the existing discrimination, legislative amendments that would extend SecNumCloud ownership requirements to private entities active in the healthcare and other sectors have been considered. CCIA urges USTR to continue pressure on France to remedy this discriminatory treatment, both through the WTO and other bilateral mechanisms, and to consider WTO dispute settlement if France refuses to engage.

In May 2024, France passed a bill to secure and regulate the digital environment ("Projet de loi visant à sécuriser et réguler l'espace numérique").[385] The law includes certain provisions that would impose important fines on a list of allegedly unfair practices by 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 extend discriminatory SecNumCloud certification for non-European CSPs hosting broadly defined sensitive data, including health data, handled by central and local public authorities.[386]

---

[380] French Ministry of the Economy, Finance, and Industrial and Digital Sovereignty. (2022, September 12). *Cloud : Cinq nouveaux dispositifs pour soutenir le developpement du secteur*. https://www.economie.gouv.fr/cloud-cinq-nouveaux-dispositifs-soutenir-developpement-secteur.
[381] *Amendment No. CS765* [France]. (2023), https://www.assemblee-nationale.fr/dyn/16/amendements/1514/ESPNUM/765.
[382] Cerulus, L. (2021, September 13). France wants cyber rule to curb US access to EU data. *POLITICO*. https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/
[383] *Regulation (EU) 2023/1543 of the European Parliament and of the Council* [European Union]. (2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1543.
[384] *Article IV(2)(b) of the Agreement on Government Procurement (GPA)* [World Trade Organization]. (1994). https://www.wto.org/english/docs_e/legal_e/rev-gpr-94_01_e.pdf.
[385] French Government. (2024, May 22). *Loi numérique : vers une meilleure protection des citoyens et des entreprises en ligne*. https://www.economie.gouv.fr/actualites/numerique-loi-protection-citoyens-entreprises-internet#.
[386] *Projet de loi visant à sécuriser et réguler l'espace numérique* [France] Article 10 bis A. (2023). https://www.assemblee-nationale.fr/dyn/16/amendements/1674/AN/1138.

Forced Revenue Transfers for Digital News

In 2019, while in the process of implementing Article 15, France created an analogous right for press publishers. News publishers can now request money from platforms when platforms display their content online. In response, Google changed the way articles appear in search results rather than entering licensing agreements.[387] However, in April 2020 the French competition authority ordered Google to pay French publishers based on the new law.[388] 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.[389] 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.[390]

Government-Imposed Content Restrictions and Related Access Barriers

The French government discontinued the governmental use of popular messaging applications such as WhatsApp, Telegram, and Signal in November 2023, citing purported security and privacy concerns.[391] The directive told French Ministers and their staff to instead transition to Olvid, a messaging application of a Paris-based startup, and Tchap, a government-developed messaging and collaboration app. The decision, although couched in the language of security, does not obviously correlate to any finding of security flaws, as the government has decreed that several of the most secure messaging applications on the market be no longer used by the government, with no other aspects in common apart from all being from the United States. USTR is urged to evaluate France's WTO GPA compliance with respect to this ban.

---

[387] Gingras, R. (2019, September 25). *How Google invests in news*. The Keyword. https://www.blog.google/perspectives/richard-gingras/how-google-invests-news/.
[388] *Reuters*. (2020, April 9). France Rules Google Must Pay News Firms for Content. https://www.reuters.com/article/us-google-france/france-rules-google-must-pay-news-firms-for-content-idUSKCN21R14X.
[389] *Reuters*. (2020, October 7). Google Poised to Strike Deal to Pay French Publishers for Their News. https://www.reuters.com/article/us-alphabet-france-publishing/google-poised-to-strike-deal-to-pay-french-publishers-for-their-news-idUSKBN26S33C.
[390] French Competition Authority. (2021, July 13). *Rémunération des droits voisins : l'Autorité sanctionne Google à hauteur de 500 millions d'euros pour le non-respect de plusieurs injunction*. https://www.autoritedelaconcurrence.fr/fr/article/remuneration-des-droits-voisins-lautorite-sanctionne-google-hauteur-de-500-millions-deuros.
[391] Pollet, M. & Herrero, O. (2023, November 30). France bans ministers from WhatsApp Signal; demands French alternatives. *POLITICO.* https://www.politico.eu/article/france-requires-ministers-to-swap-whatsapp-signal-for-french-alternatives/; Pineau, E. & Hummel, T. (2023, November 29). Stop using WhatsApp, get Paris-made alternative, French PM tells ministers. *Reuters*. https://www.reuters.com/world/europe/stop-using-whatsapp-get-paris-made-alternative-french-pm-tells-ministers-2023-11-29/.

Potential Challenges to the Development of AI

France's expansion of problematic EU-wide laws has continued into the artificial intelligence realm. On June 28, 2024 the Competition Authority and its German counterpart co-published their opinion on competition in the generative AI sector.[392] The report finds several competition risks related to semiconductor supply, cloud services, and data access, and recommends responding through both the Digital Markets Act and the recently passed Law on Securing and Regulating the Digital Environment. On July 2, 2024, the Data Protection Authority published draft guidelines for protecting data while developing AI systems.[393] The guidelines provide a basis for ensuring GDPR compatibility while developing AI systems and offer guidance to controllers on how to draft a legitimate interest assessment.

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.[394] Like other DSTs, the tax only applies to firms meeting a high revenue threshold (€750 million), effectively targeting leading U.S. technology firms operating in France while carving out most French firms that offer comparable services. French Finance Minister Bruno Le Maire has regularly referred to the tax as a "GAFA tax" (*i.e.*, Google, Amazon, Facebook, Apple) and stated that the goal is to target the "American tech giants" for special taxation.[395] 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.[396] Based on French officials' own admission, the majority of firms that pay the tax are American.[397] France raised €866 million from the DST in 2024, double the amount collected when first implemented in 2019.[398] Since its

---

[392] French Competition Authority. (2019). *Algorithms and Competition*. https://www.autoritedelaconcurrence.fr/sites/default/files/Algorithms_and_Competition_Working-Paper.pdf.
[393] CNIL. (2024, July 2). *Artificial intelligence: the CNIL opens a new public consultation on the development of AI systems.* https://www.cnil.fr/en/artificial-intelligence-cnil-opens-new-public-consultation-development-ai-systems.
[394] *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* [France]. (2019). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038811588.
[395] CCIA. (2019, August 19). *Submission of CCIA In Re Section 301 Investigation of French Digital Services Tax, Docket No. USTR 2019-0009.* https://ccianet.org/wp-content/uploads/2020/07/Comments-of-CCIA-USTR-2020-0022-Section-301-Digital-Services-Taxes-.pdf.
[396] National Assembly. (2019). *Projet de loi de finances pour 2019*. https://www.gouvernement.fr/action/le-projet-de-loi-de-finances-2019; National Assembly. (2019, April 5). *Compte rendu de réunion n° 64 - Commission des finances, de l'économie générale et du contrôle budgétaire*. https://www.assemblee-nationale.fr/dyn/15/comptes-rendus/cion_fin/l15cion_fin1819064_compte-rendu.
[397] Cassel, B. & Cazes, S. (2019, March 2). «Taxer les géants du numérique, une question de justice fiscale», affirme Bruno Le Maire. *Le Parisien*. http://www.leparisien.fr/economie/taxer-les-geants-du-numerique-une-question-de-justice-fiscale-affirme-bruno-le-maire-02-03-2019-8023578.php.
[398] Dumoulin, S. (2023, October 9). The Gafa tax will bring in 800 million euros in 2024. *Les Echos*. https://www.lesechos.fr/economie-france/budget-fiscalite/la-taxe-gafa-va-rapporter-800-millions-deuros-en-2024-1985672.

inception, France has collected over US$3 billion from this measure, mostly from U.S. firms.[399] During the drafting of the 2026 Finance Bill, lawmakers in the National Assembly's passed amendments out of the Finance Committee that would raise the DST rate from 3% up to 15%, while simultaneously raising the threshold for scoping in firms as to exclusively capture five U.S.-based firms.[400] CCIA supported USTR's decision to pursue a Section 301 Investigation under the Trade Act of 1974 regarding the French DST, which concluded that the measure was unreasonable and discriminatory. While countermeasures were suspended pending OECD negotiations, the absence of a clear path forward on addressing digital-specific issues (OECD's Pillar One) means that USTR should consider revisiting 301 remedies.

Separately, 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. 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.

In the 2024 Finance Bill, finalized and entered into effect in December 2023, the French government imposed a new 1.2% tax on revenues generated in France for music streaming providers and social media companies that license and broadcast music and that earn more than 20 million euros in annual turnover.[401] The tax is added to these companies' current tax obligations, and early indications suggest the tax is onerous for foreign companies operating in the country. One major player in the market is now passing the tax onto its local customers who now pay more for that service than in any other EU market.[402] The tax is intended to generate funding for the domestic music industry and would go towards the Centre National de la Musique, a body founded in 2020 and already partly supported by the live music sector. This new form of taxation now leaves U.S. services paying four streams of taxation, with several serving as cross-subsidies for local industries. USTR is urged to engage with France to press for reconsideration of this discriminatory treatment.

---

[399] CCIA. (2025, July 8). *Status of Key Digital Services Taxes in July 2025*. https://ccianet.org/library/status-of-key-digital-services-taxes-in-july-2025/.
[400] *Amendement n°I-CF1827* [France]. (2025). https://www.assemblee-nationale.fr/dyn/17/amendements/1906A/CION_FIN/CF1827.
[401] LOI n° 2023-1322 du 29 décembre 2023 de finances pour 2024 [France]. (2023). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048727345; Smirke, R. (2023, December 21). Streamers Decry France's New Tax to Help Support Local Music: "It is the Worst Possible Outcome." *BILLBOARD*. https://www.billboard.com/pro/france-streaming-taxes-spotify-deezer-dsp-response-reaction/.
[402] Brandle, L. (2024, March 7). Spotify is Hiking Its Subscription Prices in France Following Music Streaming Tax. *BILLBOARD.* https://www.billboard.com/business/streaming/spotify-hiking-subscription-prices-france-music-streaming-tax-1235625833/.

In the 2025 and 2026 Finance Bills, the French government considered a measure broadening the scope of the existing tax on services provided by electronic communications operators to encompass all companies designated as Very Large Online Platforms under the EU's DSA. These amendments would impose a levy of 1.3 percent on annual taxable receipts—excluding VAT—above a €5 million threshold.[403] This measure risks layering additional turnover-based obligations on top of the EU's existing regulatory regime for large platforms and creating the potential for double taxation. Moreover, when introduced, lawmakers stated its goal in making predominantly U.S.-based technology firms pay into the tax.[404]

Germany

Asymmetric Platform Regulation

Germany reformed the *German Act Against Restraints of Competition* (GWB) in 2021 to target companies of "paramount significance for competition across markets."[405] 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 where the case involves companies deemed to be of "paramount significance." As part of this reform, Germany also eliminated the Higher Regional Court of Düsseldorf from the appeals process which otherwise normally applies to defendants in competition cases, requiring defendants to appeal directly to the Federal Court of Justice.

Under the 2021-amended GWB, there is a two-step procedure: the German Federal Cartel Office (FCO) needs to first designate companies that have "paramount importance for competition across markets" 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 presumptively 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 "abusive" practices, such as: self-preferencing, abusive leveraging, data processing, and hampering of portability/interoperability.

---

[403] *Projet de Loi de finances pour 2025* [France] No. 39. (2024). https://www.senat.fr/petite-loi-ameli/2024-2025/143.html.
[404] *Amendement No. I-396* [France]. (2024). https://www.senat.fr/amendements/2024-2025/143/Amdt_I-396.html.
[405] German Federal Cartel Office. (2021, January 19). *Amendment of the German Act against Restraints of Competition*. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html.

While companies can seek to justify these practices on objective grounds, 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 affected company may not have the means to obtain the market-wide information necessary to meet that burden of proof.

Since 2021 the FCO has initiated proceedings and/or made findings of "paramount significance" against Apple,[406] Amazon,[407] Google,[408] Meta,[409] and Microsoft.[410] Like the EU's Digital Markets Act, these rules prohibit or otherwise reduce the ability of the targeted companies to engage in pro-competitive behavior that their rivals are free to pursue. The targets of this competition law reform appear to be, so far, exclusively U.S. companies. To the extent that targeted firms are put at a competitive disadvantage by virtue of additional obligations that are not clearly justified, this measure, like the DMA, implicates EU trade obligations.

A further amendment to the GWB in November 2023, the 11th Amendment,[411] significantly expanded the powers of the FCO in three key areas, heightening U.S. industry concerns over Germany's competition regime and its discriminatory targeting of U.S. companies. First, the FCO was granted authority to impose corrective measures, including divestitures, following a sector inquiry that identifies a 'significant and ongoing distortion of competition,' even in the absence of a specific antitrust violation.[412] Second, the process for disgorging profits from antitrust infringements was streamlined through the introduction of a statutory presumption that

---

[406] Waldheim, S. (2023, May 17). *Germany: Apple is found to be of paramount significance for competition across markets*. Bird & Bird. https://www.twobirds.com/en/insights/2023/germany/apple-is-found-to-be-of-paramount-significance-for-competition-across-markets/.

[407] *German Federal Cartel Office. (2022, July 6). Amazon now subject to stricter regulations – Bundeskartellamt determines its paramount significance for competition across markets (Section 19a GWB)*. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/06_07_2022_Amazon.html.

[408] German Federal Cartel Office. (2022, January 5). *Alphabet/Google subject to new abuse control applicable to large digital companies - Bundeskratellamt determines "paramount significance across markets."* https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/05_01_2022_Google_19a.html.

[409] German Federal Cartel Office. (2022, May 4). *New rules apply to Meta (formerly Facebook) - Bundeskartellamt determines its "paramount significance for competition across markets."* https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/04_05_2022_Facebook_19a.html.

[410] German Federal Cartel Office. (2023, March 28). *Federal Cartel office examines Microsoft's cross-market significance for competition.* https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/28_03_2023_Microsoft.html?nn=3591286.

[411] German Federal Cartel Office. (2023, November 7). *Amendment to the German Competition Act (Gesetz gegen Wettbewerbsbeschränkungen – GWB; 11th amendment to the GWB)*. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/07_11_2023_GWB_Novelle.html; German Federal Cartel Office. (2023, August 23). *GWB-Novelle: Mehr Wettbewerb auf vermachteten Märkten*. https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Schlaglichter-der-Wirtschaftspolitik/2023/09/03-11-gwb-novelle.html.

[412] The FCO initiated its inaugural proceeding under this provision against the fuel wholesale sector in April 2025. Louven, S. (2025, April 16). *Examination of Significant Competition Disruptions in Fuel Wholesale: BKartA Initiates First Proceeding Under Section 32f(3) GWB*. https://louven.legal/en/examination-of-significant-competition-disruptions-in-fuel-wholesale-bkarta-initiates-first-proceeding-under-section-32f3-gwb/.

excess profits amount to at least 1% of a company's relevant domestic turnover, with limited opportunities to challenge this finding. Third, the FCO received expanded powers to investigate potential breaches of the EU DMA, enabling it to support the European Commission in enforcing obligations against so-called gatekeeper platforms. In parallel, discussions have begun on a possible 12th Amendment to the GWB, which may further strengthen consumer protection law enforcement, though its final scope remains uncertain.[413]

Discriminatory Local Content Quotas and Audiovisual Service Mandates

In 2025, the German government, led by the Minister of State for Culture and Media (Culture Minister), began preparing legislation for a new Investment Obligation Act (InvestVG), a core component of a broader cultural and digital policy reform.[414] The central feature of the proposal is a mandatory local spending quota, requiring large streaming service providers and potentially TV broadcasters to reinvest a percentage of their locally generated revenue into German or European audiovisual productions. Earlier reform proposals advanced by former Culture Minister Claudia Roth in early 2024 included a 20% reinvestment obligation, a significant portion earmarked for German content, while the current government, under pressure from the Ministry of Finance, is advancing a 10% reinvestment requirement, tied to the idea of a "digital levy" or tax. The policy's stated goal is to strengthen Germany's domestic film and television industry by ensuring that global streaming platforms contribute financially to the cultural ecosystem in which they operate. The InvestVG is expected to form the second major pillar of Germany's film funding reform, following amendments to the German Film Law that took effect on January 1, 2025. While the final investment percentage and implementation timeline remain under negotiation, the legislation is anticipated to be adopted in late 2025, with enforcement likely to begin thereafter. The combined investment obligation and digital levy could have significant implications for U.S. streaming and digital service providers, particularly those who whose business model is not based on direct production (but based, for example, on licensing).

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.[415] The NetzDG law mandates the removal of "manifestly unlawful" content within 24 hours and provides for penalties of up to 50 million euros. Unlawful content under the law includes a wide range of content from hate speech

[413] Gürer, K. (2025, May 14). Koalitionsvertrag 2025 und Kartellrecht. *Deutscher AnwaltSpiegel*. https://www.deutscheranwaltspiegel.de/deutscheranwaltspiegel/kartellrecht/koalitionsvertrag-2025-und-kartellrecht-159484/.
[414] Zentner, L. M., Bensinger, V., Enaux, C. & Stöber, S. (2025, April 25). *Germany's 2025 Coalition Agreement: Reforms for the Media, Film, and Creative Industries*. GreenbergTraurig. https://www.gtlaw.com/en/insights/2025/4/media-and-film-policy-highlights-of-the-german-coalition-agreement-2025.
[415] *Beschlussempfehlung und Bericht* [Germany] [BT] 18/13013. (2017). http://dip21.bundestag.de/dip21/btd/18/130/1813013.pdf.

to unlawful propaganda. The large fines and broad considerations of "manifestly unlawful content"[416] have led to companies removing lawful content, erring on the side of caution in attempts to comply.[417] 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[418] and groups such as Human Rights Watch have expressed concerns about its threats to free expression.[419] Of further concern is the potential domino effect of this policy on other regimes. This law has been used as the basis for several onerous content regulations, including in Russia, Singapore, Türkiye, and Venezuela.[420] Cases arising under this law will also have implications on extraterritoriality, where governments seek the takedown of content accessible not only in their territory, but globally. Amendments to the law that require identifying and removing certain hate speech within 24 hours at risk of fines of up to €50 million 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 their obligations.[421]

Taxation of Digital Products and Services

In 2025, German Culture Minister Wolfram Weimer announced plans to introduce a 10% "platform" or "digital levy" targeting large digital platforms that use or distribute media and cultural content in Germany.[422] Although no official legislative draft has been published, Weimer

---

[416] 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. Gesley, J. (2017, July 11). Germany: Social Media Platforms to Be Held Accountable for Hosted Content Under "Facebook Act." Library of Congress. https://perma.cc/KX9D-V6JL.

[417] Echikson, W. & Knodt, O. (2018). *Germany's NetzDG: A Key Test for Combatting Online Hate*. CEPS. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3300636.

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

[419] Human Rights Watch. (2018, February 14). *Germany: Flawed Social Media Law: NetzDG is Wrong Response to Online Abuse. Human Rights Watch*. https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.

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

[421] POLITICO. (2022, February 2). *Big Tech Takes on Germany*. https://www.politico.eu/article/big-tech-takes-on-germany-over-demands-to-forward-illegal-content-to-federal-police/; Jurist. (2022, March 2). *Germany Administrative Court Holds New Online Hate Speech Regulation Violates EU Law*. https://www.jurist.org/news/2022/03/germany-administrative-court-holds-new-online-hate-speech-regulation-violates-eu-law/; Gesley, J. (2022, March 30). *Administrative Court of Cologne Grants Google and Facebook Interim Relief; Holds Network Enforcement Act Partially Violates EU Law.* U.S. Library of Congress. 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/.

[422] German Ministry of Culture. (2025, May 20). *Weimer fordert Plattform-Soli*. https://kulturstaatsminister.de/weimer-fordert-plattform-soli.

indicated that a non-binding position paper outlining the proposal is expected in 2025. While the detailed design of the levy remains unclear, Weimer has repeatedly referenced the Austrian DST, implemented in 2020, as a potential model. If implemented, the German proposal would represent a significantly higher rate than either Austria or France.

Greece

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In March 2025, under Greece's Recovery and Resilience Facility, the Ministry of Finance formalized a requirement that all data centers used in funded digital projects must be listed as participants in the European Code of Conduct on Data Centre Energy Efficiency (EU CoC).[423] Although the EU CoC is a voluntary initiative at the EU level, Greece has made compliance with it a mandatory eligibility criterion for participation in RRF-funded tenders. As a result, U.S. cloud service providers whose data centers are not registered in the EU CoC, despite meeting equivalent or higher international standards (such as EN 50600 and ISO certifications), are automatically disqualified from competing for these projects. This exclusionary procurement practice effectively prevents U.S. CSPs from participating in Greece's largest EU-funded digital modernization initiatives, creating a significant market access barrier and undermining fair competition.

Hong Kong

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Under pressure from China's mainland authorities, in June 2020 Hong Kong promulgated its National Security Law.[424] This law 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,[425] 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.[426] Hundreds of people have reportedly been arrested

[423] Greek Ministry of Economy and Finance. (2025). *Medium-Term Fiscal-Structural Plan.* https://minfin.gov.gr/wp-content/uploads/2024/09/EN_Greece_MTFSP_2025_28_final.pdf.
[424] Lindberg, K. S., Lung, N. & Robles, P. (2021, October 5). How Hong Kong's National Security Law is Changing Everything. *Bloomberg*. https://www.bloomberg.com/graphics/2021-hong-kong-national-security-law-arrests/.
[425] *Reuters*. (2021, January 14). Hong Kong Telecoms Provider Blocks Website for First Time Citing Security Law. https://www.reuters.com/article/us-hongkong-security-censorship/hong-kong-telecoms-provider-blocks-website-for-first-time-citing-security-law-idUSKBN29J0V6.
[426] Power, J. (2022, February 17). As 'Great Firewall' looms, fears for Hong Kong's free internet. *Al Jazeera*. https://www.aljazeera.com/economy/2022/2/17/as-great-firewall-looms-fears-for-hong-kongs-free-internet; Pomfret,

under the law,[427] as human rights experts have alerted world leaders to the harms of the law.[428] As noted elsewhere in these comments further, website blocks are barriers to maintaining a free and open internet which is critical to digital trade.

Hong Kong's Personal Data (Privacy) (Amendment) Ordinance of 2021 entered into force on October 8, 2021, which included concerning anti-doxing provisions.[429] 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 doxing 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. To the extent that these rules lead to the blocking of websites or platforms, the U.S. government should seek to ensure that U.S. business operations in Hong Kong, and the openness of the global internet, are not unduly restricted.

On March 23, 2024, Hong Kong passed the Safeguarding National Security Ordinance,[430] which allows the government to punish acts of treason, sabotage, sedition, theft of state secrets, external interference and espionage with heavy jail time, including life sentences. Critics of the law predict that the government's broad new powers under the Bill will significantly chill freedom of expression and speech online. Among other notable clauses, the Bill bans the publishing (defined as communicating "in any form," including speaking and writing) of false or misleading statements while colluding with an external force.

Threats to the Security of Devices and Services

On July 25, 2025, the government passed the Protection of Critical Infrastructure Act.[431] The Law establishes "information technology and communications" as a covered category of critical infrastructure and imposes new requirements for preventing and reporting cybersecurity incidents. However, this category is defined so broadly that it risks encompassing companies

---

J. & Kwok, D. (2022, February 15). Hong Kong Rights Group Says Website Not Accessible Through Some Networks. *Reuters*. https://www.reuters.com/world/china/hong-kong-rights-group-says-website-not-accessible-through-some-networks-2022-02-15/.

[427] *BBC*. (2022, June 28). Hong Kong National Security Law; What Is It and Is It Worrying? https://www.bbc.com/news/world-asia-china-52765838; Human Rights Watch. (2021). *Hong Kong One Year after the National Security Law*. https://www.hrw.org/feature/2021/06/25/dismantling-free-society/hong-kong-one-year-after-national-security-law.

[428] *UN News*. (2022, July 27). Top rights experts urge repeal of Hong Kong's national security law. https://news.un.org/en/story/2022/07/1123432.

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

[430] Hong Kong Security Bureau. (2024). *Safeguarding National Security Ordinance and other relevant documents*. https://www.sb.gov.hk/eng/bl23/consultation.html.

[431] *Protection of Critical Infrastructures (Computer Systems) Bill* [Hong Kong] C2885. (2025). https://www.legco.gov.hk/yr2024/english/bills/b202412061.pdf.

with little or no connection to the core functions of critical infrastructure protection.[432] The Act also grants the government extensive investigatory powers, drawing widespread criticism from commercial entities that warn it could provide Hong Kong authorities with unprecedented access to private systems.[433] In addition, the legislation has extraterritorial reach, enabling government demands on infrastructure and systems of companies operating outside Hong Kong.[434] The law further authorizes the Commissioner's Office to connect equipment to, or install programs in, the critical computer systems of designated operators—a category that may include a wide range of digital services providers under the statute's definitions. AmCham Hong Kong describes the implications as follows: "Such unprecedented power directly intervenes in, and could have a significant impact on, a CIO's operation and could harm the users of the services provided by the CIO. Moreover, as such power might be exercised within a third-party service provider's environment, it could further interfere with the operations of the third party, create potential vulnerabilities and weaknesses, and cause the third party to breach its contractual arrangements with its customers or violate any applicable laws.[435]

Other Barriers to Digital Trade

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.[436] 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. Cybercrime-specific legislation has yet to be introduced, but if it is, 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

---

[432] Asia Internet Coalition. (2024, July 29). *Asia Internet Coalition (AIC) Industry Comments on the Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructure (CI)*. https://aicasia.org/download/1079/.
[433] Purnell, N. (2024, August 19). U.S. Firms Warn Against 'Unprecedented' Hong Kong Cyber Rules. *Bloomberg*. https://www.bloomberg.com/news/articles/2024-08-20/us-firms-warn-against-unprecedented-hong-kong-cyber-rules.
[434] The American Chamber of Commerce in Hong Kong. (2024, August 1). *Proposed legislative framework to enhance protection of the computer systems of critical infrastructure*. https://www.amcham.org.hk/sites/default/files/2024-08/AmCham%20HK%20-%20Critical%20Infrastructure%20Consultation%20%28combined%29.pdf.
[435] The American Chamber of Commerce in Hong Kong. (2024, August 1). *Proposed legislative framework to enhance protection of the computer systems of critical infrastructure*. https://www.amcham.org.hk/sites/default/files/2024-08/AmCham%20HK%20-%20Critical%20Infrastructure%20Consultation%20%28combined%29.pdf.
[436] Hong Kong Government. (2022, July 20). *Consultation Paper on Cyber-Dependent Crimes and Jurisdictional Issues published (with photo/video)*. https://www.info.gov.hk/gia/general/202207/20/P2022072000144.htm.

established at the Department of Justice, which will closely cooperate with the Cyber Security and Technology Crime Bureau under the Hong Kong Police Force.

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 imposes rules on how state and local government bodies and organizations providing essential services manage data.[437] The measure includes broad data localization requirements. 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 to 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.

India

Asymmetric Platform Regulation

On December 22, 2022, an Indian parliamentary panel recommended that India adopt a "Digital Competition Act," which would include EU DMA-like ex-ante regulations for "systemically important digital intermediaries." The proposed rules appear to be largely targeted at U.S. tech companies. The panel gave recommendations on a range of DMA-inspired rules for select market participants, relating to, *inter alia*, 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 (CCI) issued far-reaching orders seeking changes to how the Android operating system and the Google Play store function in India.[438] While ostensibly seeking to address competition issues, the order, which is under appeal, may

[437] 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 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.

[438] *Umar Javeed et al. v. Google LLC & Google India Private Limited* [Competition Commission of India]. (2018). https://www.cci.gov.in/antitrust/orders/details/1070/0; *XYZ (Confidential) v. Alphabet Inc. et al.* [Competition Commission of India]. (2022). https://www.cci.gov.in/antitrust/orders/details/1072/0.

lead to a fragmented, more expensive, and less sustainable market for applications, introduce interoperability problems, and significantly increase cybersecurity risks in the mobile ecosystem.

In 2024, the Indian government released a draft Digital Competition Bill,[439] an ex-ante regulatory framework aimed at preventing systemically significant digital enterprises from engaging in presumptively anticompetitive behavior. However, in a welcome development, the government has since withdrawn the draft in its current form and announced that it will first commission a comprehensive market study before introducing a fresh version of the legislation. developments closely and re-engage at the stage when concrete recommendations from the market study emerge.

Barriers to the Deployment and Operation of Network Infrastructure

In May 2025, India's Department of Telecommunications introduced new rules for satellite operators functioning under the Global Mobile Personal Communications by Satellite Services (GMPCS) license, imposing 30 new security requirements.[440] These requirements include: mandated establishment of either local data centers or Points of Presence for satellite services within India, mandated domestic Domain Name System resolution, a commitment not to transfer or decrypt telecom data outside of India, a commitment to install emergency-response mechanisms to shut off service to regions or users if ordered to do so by national security agencies, compulsory location tracking for mobile terminals, and a requirement to source a minimum of 20% of ground infrastructure equipment from Indian manufacturers within five years of launch. These requirements result in numerous barriers to foreign satellite providers. Requiring satellite operators to localize infrastructure, including building data centers or Points of Presence, and mandating domestic DNS resolution, preferences domestic operators who already maintain facilities in-country, raising costs for new market entrants. Restrictions on transferring or decrypting telecom data abroad, coupled with compulsory location tracking and emergency shut-off mechanisms, create operational and compliance risks that could limit cross-border service provision. Finally, the obligation to source at least 20% of ground equipment from Indian manufacturers within five years introduces a discriminatory local content requirement.

Customs-Related Restrictions and Import Barriers for Goods

As of August 3, 2023, India imposed import restrictions on laptops, tablets, all-in-one personal computers, ultra-small form factor computers, and servers, transitioning these products from

[439] *Draft Digital Competition Bill 2024* [India] Annexure IV. (2024). https://www.medianama.com/wp-content/uploads/2024/03/DRAFT-DIGITAL-COMPETITION-BILL-2024.pdf.
[440] Indian Department of Telecommunications. (n.d.). *Instructions Related to Security Aspects of Chapter XII UL Agreement, Provisions for GMPCS Services*. https://dot.gov.in/latestupdates/instructions-related-security-aspects-chapter-xii-ul-agreement-provision-gmpcs-service.

"free" to "restricted" status.[441] Industry feedback led the government to defer the full implementation of these import restrictions, and instead to implement the Import Management System (IMS) on November 1, 2023.[442] Under the IMS, importers must register and obtain authorization for their imports, although no strict quotas or hard caps have been imposed yet. The import authorization mandate has already caused uncertainty, with imports of these products totaling US$8.4 billion in FY 2023–24 compared to authorized levels of about US$9.5 billion.[443] Looking forward, the Indian government is reportedly considering the adoption of an annual quota system for these imports.[444] Any such quota would risk serious supply chain disruptions and could deny companies access to ICT hardware not produced locally. It would also likely raise questions about India's compliance with its WTO commitments.

In April 2025, India introduced a regulatory requirement mandating that entities exporting certain ICT equipment, including server racks, into the country must obtain a Bureau of Indian Standards (BIS) certificate. For factories located in Southeast Asian countries, this certification process additionally requires a No-Objection Certificate (NOC) from the Ministry of Electronics and IT (MeitY), which substantially delays the issuance of the BIS certificate for manufacturers delivering Highly Specialized Equipment (HSE) into India. These delays disrupt the supply chain of critical data center infrastructure at a time when global AI development cycles are rapidly accelerating, and customers require landed capacity within weeks to meet evolving demands. Under the current dual licensing system, which combines BIS certification with DGFT import authorization, importing AI/ML server racks typically takes six to eight months, often rendering equipment obsolete before deployment. This prolonged process slows the delivery of cutting-edge cloud infrastructure and hampers customers' ability to access advanced services in a timely manner. Industry stakeholders have called for removing BIS requirements for equipment imported for self-use when cloud service providers comply with IEC and local safety standards, eliminating the 100-unit HSE cap, and streamlining the certification process by removing the MeitY NOC restriction based on manufacturer location. These measures would enable the rapid deployment of AI/ML technologies in India and support the country's ambition to become a global digital hub.

---

[441] *Amendment in Import Policy of Items under HSN 8471 of Chapter 84 of Schedule-I (Import Policy) of ITC (HS), 2022 –reg* [India] Notification No. 23/2023. (2023). https://content.dgft.gov.in/Website/dgftprod/ee5324b8-9a25-4c3a-908e-5af57e857634/Notification%20No.%2023%20dated%2003.08.2023%20Eng.pdf.

[442] Bhardwaj N. & Cyril, M. (2023, September 13). Government May Reconsider Implementing India's Import Restrictions on Laptops, Tablets, and PCs from November 1. *India Briefing.* https://www.india-briefing.com/news/india-announces-import-restrictions-on-laptops-tablets-and-pcs-29164.html/.

[443] *The Economic Times*. (2024, December 11). Importers of laptops, tablets to seek fresh authorisation for next year; window to open on December 13. https://economictimes.indiatimes.com/tech/technology/importers-of-laptops-tablets-to-seek-fresh-authorisation-for-next-year-window-to-open-on-december-13/articleshow/116217494.cms?from=mdr.

[444] Acharya, S. (2024, October 18). India plans laptop import curbs to boost local manufacturing, sources say. *Reuters*. https://www.reuters.com/technology/india-plans-laptop-import-curbs-boost-local-manufacturing-sources-say-2024-10-18/.

India's Quality Control Orders (QCOs) in the electronics sector have emerged as a significant non-tariff trade barrier due to their rapid expansion and broad application across the entire supply chain, creating severe disruptions for global manufacturers and suppliers. QCOs, issued by various ministries and enforced by BIS, make compliance with Indian standards mandatory for both imported and domestically manufactured products. Originally intended for finished goods, these requirements have been expanded to intermediate inputs and capital machinery, such as specialized copper products, electronic chemicals, and printed circuit board components. While the stated objective is consumer safety, the surge in QCOs from 88 in 2019 to over 700 by late 2024[445] is widely viewed as a protectionist measure. Because India's electronics manufacturing depends on 70–85% imported components,[446] sudden QCO application has caused major supply chain disruptions, delaying factory operations and creating bottlenecks for domestic and foreign electronics producers, including those operating under the PLI scheme. These problems are compounded by India's limited domestic testing and production capacity for many of the affected inputs, which leaves companies waiting months for BIS certification. The non-consultative and retroactive implementation of QCOs, often with little notice, has heightened regulatory uncertainty for global suppliers and investors, particularly for MSMEs, and has prompted industry calls for a phased rollout starting with finished goods before extending to components and inputs. Without greater transparency, stakeholder engagement, and realistic compliance timelines, the QCO regime risks undermining India's ambition to attract global electronics investment and integrate more deeply into international supply chains.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In 2020, the Ministry of Commerce and Industry's Department of Promotion of Industry and Internal Trade (DPIIT) extended local content requirements to the public procurement of software and services.[447] Based on this Notification, the local content requirements necessary to qualify as a "Class I" supplier is 50% and for a "Class II" Supplier, 20%. However, the formula for calculating "local content" was not defined and was left to the discretion of the different procurement agencies. This led to significant uncertainty for industry, especially for global software and cloud providers, who typically operate through distributed R&D and supply chains and therefore cannot assign the costs of product development to a single jurisdiction. Moreover, non-tangible contributions such as investments in data centers, digital upskilling, or startup ecosystems were not recognized as "local content." In July 2024, DPIIT issued a Revision Order clarifying how "local content" would be defined. These new rules explicitly exclude certain

[445] Prabhakar, P. (2025, September 24). *India's Quality Control Orders: Understanding Key Trends*. Center for Social and Economic Progress. https://csep.org/blog/indias-quality-control-orders-understanding-key-trends/.
[446] IBS Electronic Group. (2024, July 24). *India Heavily Reliant on Imports for Component Manufacturing and Design Capabilities in Electronics: Niti Aayog Report*. https://www.ibselectronics.in/resources/news/india-heavily-reliant-on-imports-for-component-manufacturing-and-design-capabilities-in-electronics/.
[447] *Public Procurement (Preference to Make in India), Order 2017 - Revision* [India] No. P-45021/2017-PP. (2020). https://dpiit.gov.in/sites/default/files/PPP%20MII%20Order%20dated%2016%2009%202020.pdf.

imported components and services from qualifying toward the "local content" thresholds, thereby tightening compliance obligations for foreign suppliers.

DPIIT's order imposed a significant compliance burden on U.S. and other foreign software and cloud service providers 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 by upskilling the workforce and investing in areas such as cloud innovation centers and quantum computing laboratories. Even if cloud services providers are not bidding directly for government contracts, their customers are 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. The Indian government is currently planning to further and raise the minimum local content requirement for Class I suppliers to 50% and Class II suppliers to 20%.[448]

In February 2021, guidelines regarding geospatial data and associated services were introduced with the goal of deregulation and liberalizing India's mapping policy.[449] 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 creating and owning geospatial data above a certain threshold; and by exempting Indian entities from prior approvals, licenses or clearances for geospatial data generation and publication that foreign entities are subject to. Although 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 must be stored and processed on a domestic cloud or on servers physically located in India. Compliance with the guidelines is mandatory.[450] CCIA urges USTR to raise these concerns by asking India to allow foreign service providers to create and own geospatial data above the threshold, to permit foreign entities to reuse and resell geospatial data obtained from Indian entities, and to eliminate mandatory localization requirements for the storage and processing of such data.

In April 2022, India's Computer Emergency Response Team began to tighten its restrictions on cloud services providers and VPN providers through Section 70B of the IT Act to strengthen incident reporting, logging, and security practices. Based on these requirements, cloud service

---

[448] Mishra, A. R. & Saha, D. (2024, May 13). Public procurement norms: Govt may hike local content requirement. *Business Standard*. https://www.business-standard.com/industry/news/dpiit-proposes-higher-local-content-threshold-for-public-procurement-124051200501_1.html,

[449] *Guidelines for acquiring and producing geospatial data and geospatial data services including maps* [India]. (2021, February 15). https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data.pdf.

[450] Vengattil, M., & Kalra, A. (2022, September 26). India's push for home grown navigation system jolts smartphone giants. *Reuters.* https://www.reuters.com/technology/exclusive-indias-push-home-grown-navigation-system-jolts-smartphone-giants-2022-09-26/.

and VPN providers must collect 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 the Indian market.[451] As a result, many VPN operators left the market due to regulatory uncertainty and impending invasive oversight, undermining digital security and services exports to the country.[452] By October 2024, Indian authorities had blocked 39 VPN providers for noncompliance, demonstrating the sweeping impact of the regime. To mitigate these concerns, CCIA urges USTR to press India to issue clear implementation guidelines for the Cyber Security Directions that would confirm cloud and VPN providers are not obligated to log and disclose customer activity as a precondition for market access, thereby aligning India's framework more closely with international norms for cybersecurity and data protection.

Indian Telecom licensees are required to connect their networks only with telecom equipment that have been tested and certified under the Mandatory Testing and Certification Framework (MTCTE). The mandatory testing and certification scheme is in place for certain IT and telecom products, with the justification being a need for safety, functionality, and security. The scope of this requirement was recently increased to include cloud software (such as hypervisors). This marks a significant policy shift, extending regulatory oversight from physical network equipment to virtualized and software-defined network elements, thereby broadening the ambit of compliance obligations for cloud service providers and telecom operators alike. This expansion introduces onerous localization and testing requirements for software that is not manufactured or deployed solely in India. Hypervisors and other virtualization software are typically developed, tested, and maintained globally, often as part of multi-tenant, cloud-native architectures. Requiring such software to undergo local testing and potentially disclose proprietary source code or security configurations can expose intellectual property, conflict with global security standards, and delay product deployment cycles. Moreover, since MTCTE is applied only to equipment and software used by Indian telecom licensees, it disproportionately affects foreign suppliers who serve the Indian market, while domestic software or cloud providers may face fewer compliance hurdles if their infrastructure is already localized. In practice, this creates a de facto barrier to market access, inconsistent with India's commitments under the WTO's TBT Agreement, which discourages discriminatory treatment and mandates that conformity assessments not be more trade-restrictive than necessary. The inclusion of cloud-based software like hypervisors under MTCTE represents an undue regulatory burden, one that duplicates existing international certifications and cybersecurity frameworks (such as ISO/IEC 27001, SOC

[451] *FAQs on Cybersecurity Directions* [CERT-In, Republic of India]. (2022, April 28). https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf; Stokel-Walker, C. (2022, May 5). VPN providers threaten to quit India over new data law. *Wired.* https://www.wired.com/story/india-vpn-data-law/.
[452] Bhatia, A. (2022, June 24). India's new cybersecurity order drives VPN providers to leave. *Center for Democracy & Technology.* https://cdt.org/insights/indias-new-cybersecurity-order-drives-vpn-providers-to-leave-chilling-speech-and-subjecting-more-indians-to-government-surveillance/.

2, or FedRAMP) already adhered to by global providers. Instead of enhancing national security, it risks fragmenting global cloud operations, increasing compliance costs, and reducing the competitiveness of international firms in India's rapidly growing digital infrastructure market.

On July 31, 2025, the Securities and Exchange Board of India (SEBI) published a Circular on Mandatory Compliance to Digital Accessibility,[453] creating a barrier for U.S. technology companies seeking to serve India's rapidly growing private financial sector. SEBI's cloud adoption framework applies to critical financial entities such as stockbrokers, asset management companies, and fintech firms, requiring any technology provider servicing these institutions to obtain accreditation and auditing by MEITY. The certification process imposes onerous and technically impractical requirements, including strict data localization mandates, mandatory government empanelment, and broad audit rights granting regulators unfettered access to provider infrastructure and operations. These rules effectively require foreign companies to replicate or relocate their infrastructure to India, creating steep compliance and operational costs. By contrast, Indian providers with existing localized infrastructure are automatically positioned at a competitive advantage, leading to an uneven playing field that severely restricts market access for U.S. cloud and technology companies. This framework not only raises concerns about regulatory overreach and data security but also conflicts with international best practices on cross-border data flows and non-discriminatory treatment in digital trade.

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 but increased government control over online speech. Of significant concern is the speed at which Indian policymakers and political leaders have increased censorship practices and restrictions on companies that fail to take down content political leaders deem "objectionable" and an increase in the number and nature of enforcement actions targeting U.S. firms with novel, aggressive tactics.[454]

Continued Internet shutdowns have left widespread human rights impacts as well as economic losses. The U.S. International Trade Commission estimated losses of US$549.4 million incurred by Facebook, Instagram, YouTube, and Twitter between 2019-2021 due to repeated internet shutdowns.[455] India has been the global leader in the number of internet shutdowns for the last

[453] *Compliance Guidelines for Digital Accessibility Circular 'Rights of Persons with Disabilities Act, 2016 and rules made thereunder- mandatory compliance by all Regulated Entities'* [India] Circular No. SEBI/HO/ITD-1/ITD_VIAP/P/CIR/2025/111. (2025). https://www.sebi.gov.in/legal/circulars/sep-2025/compliance-guidelines-for-digital-accessibility-circular-rights-of-persons-with-disabilities-act-2016-and-rules-made-thereunder-mandatory-compliance-by-all-regulated-entities-dated-july-31-2025-_96862.html.

[454] Singh, M. (2021, May 27). Twitter says it's concerned with India intimidation, requests 3 more months to comply with new IT rules. *TechCrunch*. https://techcrunch.com/2021/05/27/twitter-says-concerned-with-india-intimidation-requests-3-more-months-to-comply-with-new-it-rules/.

[455] U.S. International Trade Commission. (2022). *Foreign Censorship, Part 2: Trade and Economic Effects on U.S. Businesses*. https://www.usitc.gov/publications/332/pub5334.pdf.

six years, with local authorities having restricted connectivity since at least 2010.[456] While the frequency, geographic distribution, and duration of shutdowns had been increasing, the overall number has declined in recent years: the Internet Shutdown Tracker from the Software Freedom Law Center reported 132 shutdowns in 2020, 100 in 2021, 77 in 2022, 96 in 2023, and 60 in 2024.[457] Indian authorities also rely on Section 5(2) of the Telegraph Act, 1885, to order shutdowns, which grants broad power to suspend message transmission in the event of a "public emergency" or for "public safety."[458] The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, issued under Section 7 of the Act, authorize only senior national- or state-level officials to impose suspensions and require orders to be justified and reviewed by a designated committee.[459] However, many shutdowns since 2017 have been issued instead under Section 144 of the Code of Criminal Procedure (presently, Section 163 of the Bharatiya Nagarik Suraksha Sanhita, 2023) by officials not designated under the Telegraph Act rules,[460] raising concerns about weak safeguards and accountability. Although the rules were amended in 2020 to cap shutdown orders at 15 days,[461] the ability to continually renew them has drawn strong criticism. The Temporary Suspension of Telecommunication Services Rules, 2024 retains this 15-day limit on suspension orders and the 5-day timeline for Review Committee evaluation.[462]

As noted above, orders by the Indian government to block websites or take down specific content have long been a feature of the Indian market. However, recent legislative changes relating to digital services will pose greater challenges to U.S. exporters.[463] The Intermediary Guidelines

---

[456] Bhardwaj, S., Nayak, N., Dandamudi, R. V. K., Singh, S., & Handa, V. (2020). Rising internet shutdowns in India: A legal analysis. *Indian Journal of Law and Technology, 16*(1), Article 7. https://repository.nls.ac.in/ijlt/vol16/iss1/7.

[457] SFLC.in. (n.d.). *Internet shutdowns tracker.* https://internetshutdowns.in/; Access Now. (2023, March 1). Five years in a row: India is 2022's biggest shutdown offender. Our #KeepItOn report reveals that since 2016, India has ordered about 58% of all documented shutdowns. India hit the kill switch at least 84 times in 2022. That's 84 attacks on human rights [Tweet]. *Twitter.* https://twitter.com/accessnow/status/1630772362294575106.

[458] *The Indian Telegraph Act* [India]. (1885). https://www.indiacode.nic.in/bitstream/123456789/13115/1/indiantelegraphact_1885.pdf.

[459] *The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules* [India]. (2017). https://thc.nic.in/Central%20Governmental%20Rules/Temporary%20Suspension%20Of%20Telecom%20Services%20Rules,%202017.pdf.

[460] Vishwanath, A. (2020, January 11). Explained: The laws being used to suspend internet, and what the SC laid down. *The Indian Express.* https://indianexpress.com/article/explained/kashmir-supreme-court-internet-shutdown-laws-6215481/; Jalan, T. (2019, November 11). Internet shutdown in parts of Rajasthan and Uttar Pradesh during Ayodhya verdict. *Medianama*. https://www.medianama.com/2019/11/223-ayodhya-internet-shutdowns/.

[461] Mihindukulasuriya, R. (2020, November 12). Modi govt amends telecom suspension rules, restricts internet shutdowns to 15 days. *The Print.* https://theprint.in/india/governance/modi-govt-amends-telecom-suspension-rules-restricts-internet-shutdowns-to-15-days/539510/.

[462] *The Temporary Suspension of Telecommunication Services Rules* [India]. (2024). https://egazette.gov.in/Writereaddata/2024/256731.pdf.

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

and Digital Media Ethics Code Rules, 2021 (IT Rules)[464] impose new obligations on intermediaries.[465] The 2023 amendments to the IT Rules require online intermediaries to prevent the display, upload, modification, publication, transmission, storage, updating and sharing of a broad range of information, including any information that is obscene, harmful to children, deceptive or misleading, and that "threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence, or prevents investigation of any offence, or is insulting other nation." India's classification of VPN, cloud, and Internet infrastructure businesses as "intermediaries" under the IT Rules has allowed the government to impose sweeping blanket obligations that contradict global digital trade norms. These restrictions significantly curtail the use of these technologies and impose immense operational and regulatory risks on U.S. companies.

The amended IT Rules also include strict timelines for intermediaries to take down content upon government request and onerous due diligence requirements for certain intermediaries to put in place additional resources and processes for user complaints and redress, monitoring for harmful content, and producing compliance reports. The IT Rules also include localization requirements and traceability requirements that could potentially require service providers to break security encryptions, thus posing greater privacy and security risks and having a potentially chilling effect on human rights and future investment along with over-removal and censorship of legitimate content, including political speech.

Additionally, the IT Rules provide expansive government oversight and regulatory control over internet content. They establish Grievance Appellate Committees to review content moderation decisions, empower government-notified fact-checking bodies to order takedowns of information deemed "false or misleading" about the Government of India and subject online gaming intermediaries to the regulatory ambit of the IT Rules. Collectively, these measures deepen the Indian government's influence over digital platforms, blurring the line between self-regulation and state control.

Furthermore, the government issues issue-specific interventions from time to time to supplement broader regulatory pressures. In November 2023, India's IT ministry issued an advisory to social media companies directing them to identify and remove "deepfakes" within 36 hours of receiving a complaint.[466] The advisory framed these obligations as part of existing due diligence requirements under the IT Rules, warning that failure to comply could jeopardize platforms' safe

[464] *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules* [India]. (2021). https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf.
[465] *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules* [India]. (2021). https://www.meity.gov.in/writereaddata/files/Revised-IT-Rules-2021-proposed-amended.pdf.
[466] Press Information Bureau. (2023, November 7). Union government issues advisory to social media intermediaries to identify misinformation and deepfakes. *PIB.gov*. https://pib.gov.in/PressReleasePage.aspx?PRID=1975445.

harbor protection under Section 79(1) of the IT Act, 2000. The short timeframe heightened compliance pressures and raises risks of arbitrary or excessive takedowns. While the 2023 advisory was modified by subsequent advisories in 2024, which clarified the non-binding status of the advisory and narrowed its scope, it nonetheless demonstrates the pressure that the Indian government is willing to exert on digital platforms with respect to the content they carry.

Exacerbating what is a difficult market is India's 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. As a result, India represents one of the battlefronts of the growing—and concerning—global trend of employee intimidation.[467] In October 2024, the government further expanded its powers through the launch of the Sahyog portal, which enables officials at multiple levels to issue takedown or blocking notices under both Section 69A and Section 79(3)(b); by mid-2025, this mechanism was used to block several OTT platforms and websites over alleged misinformation and prohibited content. On 24 September 24, 2025, a Single-Judge Bench of Karnataka High Court upheld the validity of the Sahyog portal and held that foreign companies like X Corp cannot invoke claim protection of fundamental rights under Article 19, which are only available to citizens of India.[468] Reportedly, X is likely to appeal to the Karnataka High Court's decision.[469] Furthermore, the Rules are being applied beyond their intended scope to operationalize this portal to expedite government content-blocking orders and data disclosure requests to technology companies, including U.S. technology firms. Intermediaries registered on this portal are required to provide a local 'nodal officer' for operational reasons although the Rules do not mandate this requirement for all intermediaries. This regime for requiring customer data and mandating content takedowns is a process lacking transparency and a high potential for arbitrary application, carrying tangible economic repercussions on U.S. businesses.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

On July 7, 2023, the Telecom Regulatory Authority of India (TRAI) released a consultation paper dubbed "Regulatory Mechanism for OTT Communication Services, and Selective Banning of OTT Services."[470] As part of this consultation, TRAI sought comment on bringing OTT providers into the licensing and registration framework required of telecommunications operators

[467] Deck, A. (2022, July 1). 'Hostage-taking laws' seem to be fueling a Twitter crackdown in India. *Rest of World.* https://restofworld.org/2022/twitters-censorship-india/.
[468] *X Corp v. Union of India & Ors.*, WP No. 7405 of 2025 (Sept. 24, 2025) [High Court of Karnataka, Republic of India].
https://drive.google.com/file/d/1woknI67KZw5u8wWFVnANkutmKA2P9LvL/view?ref=static.internetfreedom.in.
[469] *The Hindu*. (2025). X to appeal Karnataka High Court judgement upholding Sahyog portal.
https://www.thehindu.com/sci-tech/technology/deeply-concerned-by-karnataka-high-courts-order-x-corp/article70107687.ece.
[470] TRAI. (2023, July 7). *Press release: Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services.*
https://www.trai.gov.in/sites/default/files/PR_No.59of2023.pdf.

and on the merits of "selective banning" certain OTT services. The proposals triggered significant concern among industry stakeholders and digital rights advocates who argued that applying telecom-style regulations to OTT providers would result in regulatory duplication, especially since the Draft Telecommunications Bill, 2022 was still under consideration at the time. Such an approach overlooks the technical and functional differences between telecom networks and internet-based applications, and could stifle innovation, competition, and user choice. In addition to the risk of duplicative regulations for OTT services, including regulations still being developed through the Draft Telecommunications Bill, the proposal raised numerous substantive concerns that would affect U.S. suppliers operating in the market. Key concerns included the unjustified application of 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. CCIA outlined these concerns in the TRAI proceeding.[471] In December 2023, the Telecommunications Act, 2023 was enacted, replacing older statues such as the Indian Telegraph Act and potentially providing a new legal basis for telecom regulation authorities; however, as of 2025, TRAI has not issued final binding rules that impose licensing or enable selective banning of OTT communication providers in the broad sense proposed in 2023.

In December 2023, India enacted the Telecommunications Act,[472] consolidating prior telecom laws (including the Telegraph Act of 1885) while significantly expanding the definition of "telecommunication services" to include internet-enabled services such as OTT platforms, user-to-user communication, and cloud services. The Act overlaps with the IT Act and the Digital Personal Data Protection Act in areas such as interception, privacy, and consumer redress, and its interaction with forthcoming legislation like the Digital India Act remains unclear. Broad definitions mean that a wide range of internet services could now be subject to licensing, authorization fees, and mandatory contributions to the Digital Bharat Nidhi (formerly the Universal Service Obligation Fund), while at the same time not being able to access that fund, thereby disadvantaging foreign suppliers relative to local telecom operators.

On September 18, 2024, the TRAI issued Recommendations on the Framework for Service Authorisations under the Telecommunications Act, 2023, proposing new categories for infrastructure providers, satellite gateways, cable landing stations, captive private networks, cloud-hosted telecom networks, and mobile number portability providers.[473] In February 2025, the Department of Telecommunications issued an advisory to social media and application

[471] CCIA. (2023, August 18). *Comments on TRAI OTT regulation consultation*. https://ccianet.org/library/ccia-comments-on-trai-ott-regulation-consultation/.
[472] *Telecommunications Bill* [India]. (2023). https://prsindia.org/billtrack/the-telecommunication-bill-2023.
[473] *Recommendations on the Framework for Service Authorisations* [India]. (2023). https://www.trai.gov.in/sites/default/files/2025-02/Recommendation_28022025.pdf.

hosting platforms, requiring them to remove content or applications that abet offences under Section 42 of the Act, such as tools enabling caller line identification spoofing or tampering with identifiers like IP addresses and IMEIs.[474] Platforms were directed to comply by February 28, 2025, under threat of direct enforcement action. This illustrates how the Act's broad scope could expose internet platforms and services far removed from telecom operations to heavy-handed obligations and penalties.

The Act also carries other burdensome provisions, including biometric verification, government access to data, encryption mandates, liability for seizures, and potential support for internet shutdowns. Such requirements risk undermining privacy, digital security, and freedom of expression, while establishing one of the world's first general licensing regimes for internet-enabled services. Notably, authority has shifted from the independent regulator TRAI to the central government, raising concerns about unchecked oversight.[475] CCIA urges USTR to monitor implementation closely, as the evolving framework, through both TRAI's recommendations and DoT's enforcement actions, could distort competition against U.S. providers, deter investment in India's digital economy, and place India in violation of its WTO commitments under GATS.

In August 2024, the Ministry of Information and Broadcasting withdrew the latest draft of the Broadcasting Services (Regulation) Bill,[476] after initially sharing it with select stakeholders for comment.[477] The proposed Bill expanded its scope from traditional broadcasters and platforms with online curated content to also include social media platforms. It would have established regulatory oversight over social media accounts and online video creators and established a broad definition of "digital news broadcaster" to include independent content creators, subjecting them to broadcast-style oversight, including content evaluation committees and registration requirements. The proposal provoked widespread backlash from stakeholders, including content creators, digital rights groups, and broader industry, concerned about overreach, censorship risks, and opaque consultation processes.[478] Recent reports suggest that social media platforms may

[474] *Storyboard 18*. (2025, February 19). DoT asks social media platforms to remove content violating Telecom Act. https://www.storyboard18.com/how-it-works/dot-asks-social-media-platforms-to-remove-content-violating-telecom-act-57128.htm.
[475] *Telegraph India*. (2022, September 26). Crossed wires: Editorial on implications of Modi government's draft Telecom Bill 2022. https://www.telegraphindia.com/opinion/crossed-wires-editorial-on-implications-of-modi-governments-draft-telecom-bill-2022/cid/1888772.
[476] PRS. (2023, November 10). *Public notice on website of Ministry of Information & Broadcasting.* https://prsindia.org/files/parliamentry-announcement/2023-12-09/Draft_Broadcasting_Services_(Regulation)_Bill,_2023.pdf.
[477] Barik, S. (2024, August 13). *Facing criticism, govt withdraws new draft of broadcast bill. Indian Express.* https://indianexpress.com/article/explained/broadcast-bill-controversy-freedom-of-speech-code-of-ethics-it-act-violation-9510443/.
[478] Sharma, Y. (2024, August 12). *India wants to make influencers register with the government. Rest of World.* https://restofworld.org/2024/india-influencers-news-broadcasters-2024-bill/.

ultimately be excluded from the Bill's scope.[479] Even so, the government's intent to extend broadcasting-style regulation to online services raises alarms both for the internet ecosystem and the ability for online services providers to operate in India with regulatory certainty while also raising grave freedom of expression concerns.[480]

In September 2025, the Department of Telecommunications (DoT) in India proposed a regulatory framework including CDNs that has generated strong opposition from the TRAI and industry stakeholders,[481] who view it as an unnecessary regulatory layer between CDNs and ISPs. The core element of the proposal is the introduction of an authorization or registration requirement for CDNs under the Telecommunications Act, 2023, accompanied by a mandatory submission of confidential peering and interconnection agreements between CDN operators and ISPs to the DoT (with parallels to what Italy recently proposed). This deviates from TRAI's previous recommendations against full licensing for CDNs and diverges from global best practices, where CDNs are not regulated as telecom service providers because their function is limited to content delivery rather than providing access to telecommunications networks. The proposed framework would impose significant compliance costs on CDN operators, including U.S. firms, through new authorization procedures, regulatory reporting, and legal obligations, while also creating operational risks due to the requirement to disclose sensitive commercial agreements that contain proprietary pricing models and strategic network data. Moreover, the measure raises net neutrality concerns by enabling the regulator to review and potentially influence CDN–ISP traffic and pricing arrangements, creating scope for discriminatory treatment of content. It also threatens to undermine India's long-standing Settlement-Free Peering model, which allows networks to exchange traffic at no cost, thereby keeping latency low and content delivery affordable. Increased peering costs could be passed on to consumers and tilt the competitive landscape in favor of large domestic ISPs, erecting new barriers for foreign CDN providers and potentially harming the broader digital ecosystem. For the moment, DoT appears to have backed off, [482]but the issue merits close monitoring.

Restrictions on Cross-Border Data Flows

The Digital Personal Data Protection Bill was passed and entered into law on August 11, 2023.[483] The bill gives the Indian government broad discretion in interpreting key terms in the

[479] Fazal, I. (2025, June 25). Govt may exclude social media from Broadcasting Bill, stirring industry debate. *Storyboard 18.* https://www.storyboard18.com/television/govt-may-exclude-social-media-from-broadcasting-bill-stirring-industry-debate-71693.htm.
[480] Shoaib Daniyal, *Modi's plans to muzzle India's internet*, INDEX ON CENSORSHIP (Aug. 28, 2024), https://www.indexoncensorship.org/2024/08/modis-plans-to-muzzle-indias-internet/.
[481] Pandey, K. (2025, September 1). TRAI, Industry Push Back As DoT Seeks Control Over CDNs Via Light-Touch Regulation. *Medianama*. https://www.medianama.com/2025/09/223-trai-dot-cdns-light-touch-regulation.
[482] Pandey, K. (2025, October 16). DoT Keeps CDNs Unregulated Despite Earlier Push For Oversight. *Medianama*. https://www.medianama.com/2025/10/223-dot-cdns-unregulated-oversight/.
[483] *Digital Personal Data Protection Act 2023* [India] No. 22. (2023). https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

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 bases for data processing. The law also allows the government to deny the export of data to a country if it so chooses and can create a list of jurisdictions where personal data cannot be exported to from India, with no avenue for recourse, such as standard contractual clauses, and no clarity on the criteria for jurisdictions to be on the list. Coupled with the law allowing for the data localization requirements to be prescribed under other legislation (e.g., those governing the financial services sector), this results in significant uncertainty for industry in the overall environment for data protection and cross-border data flows.[484]

In 2025, the government began developing implementing rules under the DPDP Act that have further heightened industry concerns.[485] Draft provisions, including Articles 12 and 14, would impose expansive obligations on "significant data fiduciaries," giving the government nearly unfettered discretion to designate entities and to mandate that certain categories of personal or traffic data be stored domestically. Such rules risk creating significant compliance burdens by targeting specific companies rather than specific types of data, while leaving businesses uncertain whether they will be subject to future localization requirements. At the same time, proposed restrictions on cross-border transfers would allow personal data to be moved abroad only on terms set by the government, without clear criteria or mechanisms, such as standard contractual clauses, that would enable companies to ensure compliance. This framework diverges sharply from established best regulatory practices that permit data transfers with safeguards, and risks generating conflicts of law with other jurisdictions that require data disclosures for regulatory purposes. The lack of transparency and consistency in these rules could disrupt global data flows, undermine privacy protections, and place cross-border suppliers of digital services at a competitive disadvantage, raising concerns about India's adherence to its trade commitments under GATS.[486]

Taxation of Digital Products and Services

India's income tax laws[487] currently create uncertainty around whether the provision of data center services by an Indian entity to a foreign entity establishes a taxable presence, such as a permanent establishment or business connection, for that foreign entity. A foreign entity can be subject to Indian taxation, if it is considered to have a permanent establishment (fixed place of

[484] HuntonAK. (2023, August 22). *India passes Digital Personal Data Protection Act*. https://www.huntonprivacyblog.com/2023/08/22/india-passes-digital-personal-data-protection-act/.
[485] CCIA. (2025). *Comments on India's Proposed Digital Personal Data Protection Rule*. https://ccianet.org/wp-content/uploads/2025/03/CCIA-Comments-on-Indias-Proposed-Digital-Personal-Data-Protection-Rule.pdf.
[486] CCIA. (2025). *Comments on India's Proposed Digital Personal Data Protection Rule*. https://ccianet.org/wp-content/uploads/2025/03/CCIA-Comments-on-Indias-Proposed-Digital-Personal-Data-Protection-Rule.pdf.
[487] *Income Tax Act* [India]. (1961). https://incometaxindia.gov.in/pages/acts/income-tax-act.aspx; *Income Tax Rules* [India]. (1962). https://incometaxindia.gov.in/pages/rules/income-tax-rules-1962.aspx.

business in India)[488] or a business connection in India (any relationship or activity in India contributing to such foreign entity's income - even without a fixed place of business).[489] This interpretative ambiguity around the taxation model as well as how tax authorities and courts could apply these concepts to modern, service-based digital business models, exposes foreign firms to the risk of double taxation and excessive compliance burdens, even when transactions are conducted on a standard cost-plus basis. The resulting unpredictability raises operational costs. The recent Supreme Court ruling in Hyatt International has further underscored this risk, holding that substantive control from abroad may be sufficient to establish a permanent establishment in India, even without direct ownership of premises.

Other Barriers to Digital Trade

India discriminates against American e-commerce providers, including through limitations on foreign companies operating in "multi-brand retail trading."[490] This means that any company with foreign investment, including American e-commerce companies, cannot sell its own inventory directly to customers, requiring significant changes to their business models. These rules, which began in 2012 but were expanded in 2016 and 2018, establish several obstacles to American companies operating in India. American companies cannot invest more than 51% in a firm operating in India, with a minimum investment requirement of $100 million that carries obligations micromanaging companies' business decisions. For example, at least 50% of this initial FDI must fund backend infrastructure such as processing, storage, distribution, and logistics, and at least 30% procurement of manufactured or processed products must be from Indian micro, small, and medium industries. American companies are prohibited from selling their own inventory directly to consumers and are only permitted to operate a marketplace business model. They also face severe restrictions for marketplace e-commerce operations, including being unable to set prices, facing limitations on inventory management, and being prohibited from entering seller exclusivity arrangements. Specifically, American marketplaces and their group entities cannot provide more than 25% of the inventory for any of the vendors using their service. The regulation undermines American companies' ability to efficiently reach Indian consumers and optimize their supply chains. None of the above restrictions apply to domestic, non–FDI-funded entities. Domestic companies are permitted to operate inventory-based models without any additional conditions and have complete flexibility in pricing, inventory management, and seller exclusivity agreements for their e-commerce operations. These restrictions prevent leading U.S. e-commerce companies from accessing the rapidly growing

[488] Indian Income Tax Department. (n.d.). *Double Taxation Avoidance Agreements*. https://incometaxindia.gov.in/pages/international-taxation/dtaa.aspx
[489] *Income Tax Act*. [India] § 9(1)(i). (1961). https://www.indiacode.nic.in/bitstream/123456789/2435/1/a1961-43.pdf.
[490] Indian Ministry of Commerce & Industry. (2018, December 26). *Review of policy on Foreign Direct Investment (FDI) in e-commerce*. https://www.pib.gov.in/newsite/PrintRelease.aspx?relid=186804.

Indian market, undermine current and potential investments in the U.S., and diminish U.S. technology leadership.

Indonesia

Barriers to the Deployment and Operation of Network Infrastructure

The Minister of Fisheries and Marine Affairs' Decree No. 14/2021 on Subsea Pipelines and/or Cables requires all subsea cables in Indonesian waters to follow a limited number of prescribed routes and landing points.[491] More than half of existing cables are located out of these prescribed corridors and following such prescribed routes and landing points lacks sound justification. Moreover, different ministries interpret the landing points differently, and there is no clear 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.[492]

In addition, under Indonesia's subsea cable regulatory framework, subsea cable operators need to obtain overlapping licenses from multiple government ministries, which causes significant delays and uncertainty to investments by U.S. and other subsea cable operators. Additionally, the Ministry of Communication and Digital Affairs requires foreign subsea cable 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; include the local partner in the cable consortium with at least 5% stake to land the cable in Indonesia (i.e., precluding transiting Indonesian waters). Such requirements are significant market barriers for U.S. providers to establish their business operations in Indonesia, and USTR is encouraged to seek the removal of these impediments.

Further restricting flexibility are Indonesia's strict cabotage rules,[493] which only allow Indonesian flagged vessels to conduct subsea cable survey, installation and repair works, significantly reducing vessel supplies and therefore increasing the risk of project delays.

Customs-Related Restrictions and Import Barriers for Goods

Industry reports that Indonesia continues to act in violation of its WTO tariff binding for a set of imported technology products that should benefit from duty-free treatment under the commitments made by Indonesia to the Information Technology Agreement (ITA). Thus far,

---

[491] Afifa, L. (2021, February 23). Indonesia Officially Regulates Submarine Cables and Pipeline. *Tempo*. https://en.tempo.co/read/1435866/indonesia-officially-regulates-submarine-cables-and-pipeline.
[492] Goodman, M. P. & Wayland, M. (2022). *Securing Asia's Subsea Network: U.S. Interests and Strategic Option*. CSIS. https://www.csis.org/analysis/securing-asias-subsea-network-us-interests-and-strategic-options.
[493] Watson Farley & Williams. (2016). *Ownership, Cabotage, and Flag Issues Relating to Indonesia Maritime Assets*. https://www.wfw.com/wp-content/uploads/2019/07/WFW-Indonesia-1.pdf.

Indonesia only introduced ITA commitments for five categories of goods/HS codes (Semiconductors, Semiconductors Equipment, Computers, Telecommunications Equipment and Software, and Electronic Consumer Goods). Even within those categories, however, Indonesia has reclassified certain technology goods with similar functions into dutiable HS codes that would fall outside these 5 categories, as a method of increasing revenue. Examples of this include Indonesia's continued practice of applying duties for printers and related parts, equipment for data centers, and for connectivity (such as routers, switches, servers and server racks, optical modules, and optical cables), solid state drives, among other ICT products, all of which are covered by the ITA. In the view of industry, the reclassified HS codes should be protected by Indonesia's ITA commitments. By raising import costs, this practice broadly harms the IT industry and imposes burdens on U.S. investors and their workers alike.

The Ministry of Trade previously issued Regulation No. 87/2015 ("Reg 2015"), which imposed obligations on the imports of goods classified in specific HS codes, including servers. Under this now repealed regulation, entities importing such goods were required to 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, 2021, and implemented new HS codes.[494] 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 for waivers for capital goods, the government has not provided sufficient transparency and certainty for applying and receiving the exemption. Although both Reg 2015 and Reg 2021 allow for the import of capital goods without SR if the MOT issues an exemption letter, industry reports the government has provided limited transparency and timeline for the process of applying for and receiving an exemption.

On September 27, 2023, the Ministry of Trade issued Regulation No. 31/2023 that prohibits foreign merchants from selling any goods that are valued less than $100 to Indonesian customers through online marketplaces - with a positive list subject to periodic updates.[495] 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 requiring 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

[494] Baker McKenzie. (2022). *Indonesia: New Integrated Import Guidelines*. https://www.bakermckenzie.com/-/media/files/insight/publications/2022/01/thought-piece_new-integrated-import-guideline.pdf.
[495] Baker McKenzie. (2023, October 10). *Indonesia: The New E-Commerce Regulation*. https://insightplus.bakermckenzie.com/bm/consumer-goods-retail_1/indonesia-the-new-e-commerce-regulation-heightened-levels-of-responsibility-for-e-commerce-platforms-operators.

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.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In 2019, the Government of Indonesia issued Government Regulation 71/2019 (GR 71) to revise the previous Government Regulation 82/2012 (GR82). While this measure improved many aspects of data governance, certain data localization mandates were retained – while GR 71 relaxed data localization requirements under GR82 to allow private sector electronic system operators (ESO) to store systems and data outside Indonesia, subject to certain restrictions, GR71 still requires data localization for public sector ESOs.

In particular, the implementing regulations for GR71, (Circular 4/2022) require 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, poses additional barriers and operational costs to U.S. cloud services providers, and inhibits the ability of U.S. firms to participate in public sector procurement exercises.[496]

With respect to the private sector market, GR71 allows private ESOs to operate electronic systems and process data outside Indonesia. As the government seeks to amend GR71 as an effort to strengthen enforcement in content moderation, location flexibility should be maintained, and they should seek to balance safety and safeguards for human rights.[497]

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.[498] This effectively requires e-commerce business actors to locally store personal data for e-commerce customers. In September 2023, Trade Regulation 31/2023 came into force, adding new requirements such as protections for MSMEs, an import price floor, and limits on social-commerce activity. The regulation 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 with the government. Both GR 80 and TR 31 pose *de facto* data localization

[496] Pardede, D. et. Al. (2021, January 17). *Indonesia: Indonesia Regulates Foreign Private Electronic System Operators*. Global Compliance News. https://www.globalcompliancenews.com/2021/01/17/indonesia-indonesia-regulates-foreifn-private-electronic-system-operators11122020/.
[497] Aljannah, O. (2025, August 13). Kemenko Polkam Dorong Pemetaan Regulasi Keamanan Data PSE. *Radio Republik Indonesia*. https://rri.co.id/nasional/1765157/kemenko-polkam-dorong-pemetaan-regulasi-keamanan-data-pse.
[498] EY. (2020, January 15). *Indonesia Issues e-commerce Trading Regulation*. https://www.ey.com/en_gl/tax-alerts/ey-indonesia-issues-e-commerce-trading-regulation.

measures and local content requirements, which increase overhead costs for foreign entities and create undue market barriers.

Indonesia significantly restricts the use of public cloud technology involving overseas data transfers in the public sector and other regulated sectors.[499] This is particularly burdensome in the financial services sector. Financial service regulators have the authority to impose additional requirements with respect to data in the financial sector 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. With regard to using AI in the banking and financial services, OJK also imposes strict requirements on their supervised entities to only use AI models that can prove data residency in Indonesia.[500] This is a restrictive requirement that has prevented banks and the financial sector from using AI services from US companies.

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.

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

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

Through various regulations, the government has been requiring service providers to possess Indonesian National Standard (SNI) certificates as part of public procurement process, while not

[499] TechRepublic. (2021). *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/.
[500] Indonesian Financial Services Authority. (2025, April 29). *Artificial Intelligence Governance for Indonesian Banks*. https://ojk.go.id/en/Publikasi/Roadmap-dan-Pedoman/Perbankan/Pages/Indonesia-Artificial-Intelligence-Governance-for-Banking.aspx.

acknowledging the international equivalence (ISO). Most recently, Decree No. 519/2024 requires public cloud providers to possess local certificates to pre-qualify to be part of the National Data Center Ecosystem.[501] The standards listed are SNI ISO 9001, SNI ISO/IEC 27001, SNI ISO/IEC 27017, and SNI ISO/IEC 27018 – without accepting the international ISO equivalent. The requirements are designed to be more easily met by local providers, including by requiring local entity and local presence, as well as local content, presenting uneven playing field for international providers. Furthermore, some requirements are listed without further implementing guidelines, resulting in local certifiers incapable of issuing such certificates. The recent draft of cybersecurity law also suggests potential additional local standards and certifications for cybersecurity service and infrastructure providers. These requirements add to compliance costs and prevent international cloud providers from serving potential customers, especially in the public sector.

In May 2025, Indonesia introduced a draft Cybersecurity Bill, which raises significant concerns for cloud service providers and data center operators due to its expansive scope and overlapping regulatory authority.[502] The draft legislation distributes cybersecurity governance and incident response authority across multiple agencies, including the telecom regulator Kominfo (through Komdigi), the National Cyber and Crypto Agency, the Police, and the Military, without clearly defining their respective roles and responsibilities. This fragmented oversight structure creates regulatory uncertainty and could lead to operational complications, especially during security incidents when multiple agencies may issue conflicting directives. The bill also introduces new security requirements, certification processes, and compliance monitoring mechanisms, along with potential expansions of government access and ambiguous incident reporting rules that may conflict with global standards and best practices. Moreover, it signals a shift toward increased data localization and stringent compliance obligations, which would raise costs and complicate operations for international providers. The combination of overlapping authorities and unclear procedures undermines regulatory predictability, risks operational disruptions, and creates unnecessary market access barriers that could reduce the quality and availability of cloud services in Indonesia.

Forced Revenue Transfers for Digital News

In February 2024, the government signed a Presidential Regulation directing specific digital platforms to pay news organizations for news content that appears on those platforms.[503] Digital

---

[501] *Keputusan Menteri Komunikasi dan Informatika Nomor 519 Tahun 2024 tentang Penyelenggaraan Pusat Data Nasional* [Indonesia]. (2024). https://jdih.komdigi.go.id/produk_hukum/view/id/941/t/keputusan+menteri+komunikasi+dan+informatika+nomor+519+tahun+2024

[502] *Naskah Akademik Rancangan Undang-Undang Keamanan Ketahanan Siber* [Indonesia]. (2025). https://berkas.dpr.go.id/akd/dokumen/RJ1-20190617-025848-5506.pdf.

[503] *Presidential Regulation (Perpres) on the Responsibility of Digital Platform Companies to Support Quality Journalism* [Indonesia] No. 32. (2024). https://setkab.go.id/en/govt-issues-regulation-on-publisher-rights/.

platforms that would qualify are those that host content from Indonesian news outlets, Although these thresholds, albeit arbitrary, are facially neutral, the effects and intent of this measure make clear that U.S. companies are primary targets of this regulation.[504] The goal of extracting revenues and subsidizing local news outlets is evident from the explicit goal of the regulation, which states that digital services companies have a "responsibility" to support news organizations.

The Regulations require platforms to collaborate with media companies, with collaboration entailing paid licenses, profit sharing, data sharing, or other forms of cooperation. It further empowers the Implementing Committee (KTP2JB), a third party made up of mostly members of the Press Council and media companies, to implement the guidelines, prescribe further regulations, and oversee arbitration between digital platforms, a conflict of interest that greatly compromises any presumption of neutrality and objectivity between disputing parties. Under this regulation, the KTP2JB establishes the rules of engagement and simultaneously oversee mediation or arbitration if any disputes materialize, an authority that clashes with the confidentiality of alternative dispute resolutions. The regulation could also direct digital platforms to design their news distribution algorithms to support quality journalism, though it does not clearly mandate disclosure of algorithmic changes or user behavior data to news publishers.

Government-Imposed Content Restrictions and Related Access Barriers

Indonesia's excessive content takedown requests and internet shutdowns have affected U.S. firms financially and implicate broader concerns of freedom of expression online. The USITC estimated US$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.[505] The phenomenon of content restrictions continues to expand, between July 2023 and December 2023, Meta reported that the company restricted access to "47 million items allegedly violating local laws on gambling such as the Electronic Information and Transactions (EIT) Law and KOMINFO Regulation 5/2020 on Private Electronic Services Operator," compared to 1,458 items removed over the same period in 2022.[506]

In December 2020, the ICT Ministry (Kominfo) issued Ministerial Regulation 5/2020 to regulate private electronic systems providers ("ESPs")—the definition of which includes practically every

[504] Muskita, P. (2024, February 20). Indonesia to require Google, Meta to compensate new publishers. *Tech In Asia.* https://www.techinasia.com/indonesia-require-google-meta-compensate-news-publishers.
[505] U.S. International Trade Commission. (2022). *Foreign Censorship, Part 2: Trade and Economic Effects on U.S. Businesses*. https://www.usitc.gov/publications/332/pub5334.pdf.
[506] Meta. (2024, September 18). *Transparency Center, Indonesia Country Report.* https://transparency.fb.com/reports/content-restrictions/country/ID/; Potkin, F. & Sulaiman, S. (2022, March 23). Indonesia Preparing Touch New Curbs for Online Platforms. *Reuters*. https://www.reuters.com/world/asia-pacific/exclusive-indonesia-preparing-tough-new-curbs-online-platforms-sources-2022-03-23/.

internet website or internet-enabled service.[507] 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 systems and data. ESPs are expected to comply with demands for data access and access to ESPs' systems for "supervisory and law enforcement purposes" within 5 days. In early October 2025, TikTok's registration license was suspended from failing to comply with granular user data request from Komdigi.[508] System access required in the regulation remains problematic and its scope undefined. Provision of system access to law enforcers or government risks security breaches and may compromise users data. The process for registering and subsequent punishment for failing to do so is excessively opaque, and enforcement procedures lack transparency. The law stated that ESPs would be given 6 months of transition time to register in Indonesia's database, but Kominfo did not provide guidance until June 14, 2022 for compliance set for July 20.[509] 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.[510] Pursuant to this regulation, 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, service restrictions, and suspensions of registration.

Furthermore, Government Regulation 43/2023 introduces additional financial penalties of up to US$30,000 per non-compliant URL, amplifying compliance risks for online service providers.[511]

---

[507] Hogan Lovells DNFP. (2021). *Indonesian regulator set clearer terms for internet platforms (domestic and foreign): Registration, takedown, and (un)blocking*. 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 ; Rachmad, A. & Esmeralda, L. P. (2021, May 11). *Indonesia's New Regulation on Private Electronic System Operators: Important Notes for Corporate Compliance of Domestic and Foreign Information Technology Companies*. ZICO Law. 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/.

[508] *Antara*. (2025, October 3). Indonesia suspends TikTok license, House urges protection for SMEs. https://en.antaranews.com/news/383965/indonesia-suspends-tiktok-license-house-urges-protection-for-smes.

[509] Dentons. (2022). *The Obligation to Register as an Electronic System Operator with the Ministry of Communication and Informatics of the Republic of Indonesia*. https://dentons.hprplawyers.com/en/insights/articles/2022/july/19/-/media/ae78e9f3861d493ebb20a7cc30f60afa.ashx; Pardede, D. et al. (2022, July 5). *Indonesia: Deadline for registration of electronic system operators is now set for 20 July 2022*. Global Compliance News. https://www.globalcompliancenews.com/2022/07/05/indonesia-deadline-for-registration-of-electronic-system-operators-is-now-set-for-20-july-2022-01072022/.

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

[511] *GR 43/2023* [Indonesia]. (2023). https://peraturan.bpk.go.id/Download/321932/PP%20Nomor%2043%20Tahun%202023.pdf

Civil society groups have also raised concerns with aspects of the Regulation.[512] Recently, X was fined for failure to comply with a content takedown request within the prescribed 24 hours turn-around-time.[513] The combination of vague content definitions, a lack of transparency in the appeals process, and the sheer scale of content hosted on platforms creates a substantial risk of disproportionate and recurring fines for companies.

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).

Under Decree 172, Kominfo is mandated to operate a 'content moderation compliance system' ('Sistem Kepatuhan Moderasi Konten') to implement content takedown notices and issue corresponding fines. The system is currently in a pilot phase but scheduled to become permanent this year.[514] Lack of information about the appeal mechanism, turn-around-time, fair fine calculation, questionable security, and absence of an industry accepted technical guidelines remain concerns.

Indonesia's Child Safety Regulation (Government Regulation No. 17/2025, or locally known as PP Tunas), passed in April 2025, establishes a new online child safety framework that raises significant concerns for industry.[515] The regulation introduces broad and vague parameters for risk assessment, unclear age verification and parental consent mechanisms, and increases the age of consent to 18. It also bans teens under 16 from accessing digital platforms classified as "high risk," while allowing access to "low-risk" platforms only with parental consent. The criteria used to determine risk levels, including addiction, psychological or physiological harms, are vaguely defined, and meeting even a single criterion automatically designates a platform as high risk, without considering technological developments, platform-specific mitigation measures, or

[512] Rodriguez, K. (2021, February 16). *Indonesia's Proposed Online Intermediary Regulation May be the Most Repressive Yet*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2021/02/indonesias-proposed-online-intermediary-regulation-may-be-most-repressive-yet.
[513] Fajriadi, A. I. (2025, October 14). Indonesia Fines Elon Musk's X Rp78mn Over Pornographic Content. *Tempo*. https://en.tempo.co/read/2057160/indonesia-fines-elon-musks-x-rp78mn-over-pornographic-content.
[514] Makarim & Taira. S. (2025). *Update on Fines and Content Takedowns for Online Platforms in Indonesia*. https://www.makarim.com/news/update-on-fines-and-content-takedowns-for-online-platforms-in-indonesia.
[515] *Tata Kelola Penyelenggaraan Sistem Elektronik Dalam Pelindungan Anak* [Indonesia] Peraturan Pemerintah (PP) Nomor 17 Tahun 2025. (2025). https://peraturan.bpk.go.id/Details/316698/pp-no-17-tahun-2025.

evolving user behavior. This simplistic classification system risks depriving teens of access to platforms that can be beneficial to their development and creates compliance uncertainty for companies. The implementing regulation, currently being drafted by KOMDIGI, will be critical to addressing these gaps and ensuring a fair and proportionate risk assessment framework. PP Tunas is expected to come into effect in April 2027 and will apply to all digital platforms, not just those offering child-focused products or services.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

Additionally, the government continues to move forward with the 2019 draft Bill on Broadcasting that would place internet streaming platforms under the oversight of the Broadcasting Law, subjecting them to licensing and censorship laws. In March 2024, legislators amended the draft to include greater state control and stricter content standards, sparking alarm from civil society.[516] The law would have implications both for the delivery of online services and the open internet as well as freedom of expression online. The bill remains under discussion in the legislature.

Restrictions on Cross-Border Data Flows

On September 20, 2022, Indonesia's Parliament ratified its Personal Data Protection Bill.[517] The bill helpfully differentiates the responsibilities between data controllers and data processors. Data controllers must ensure that any data flows must only go to countries that have equivalent or higher standards of data protection than that available in Indonesia. 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.

In April 2023, Indonesia's Constitutional Court clarified several ambiguities in the Personal Data Provision Law (PDP) following its enactment.[518] The court found that "person" includes legal entities, and they therefore could be data controllers. The court also 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. The court also clarified that the contested terms national defense and security are defined through the principle of public interest

[516] International Federation of Journalists (2024, May 23). *Indonesia: New Broadcasting Bill threatens democracy and press freedom*. https://www.ifj.org/media-centre/news/detail/category/press-releases/article/indonesia-new-broadcasting-bill-threatens-democracy-and-press-freedom.
[517] Hunton. (2022, September 23). *Indonesia Enacts its First Data Protection Act*. https://www.hunton.com/privacy-and-information-security-law/indonesia-enacts-its-first-data-protection-act#page=1.
[518] Pardede, D. et al. (2023, June 13). *Indonesia: Clarification of certain provisions of the PDP Law by the Constitutional Court*. Baker McKenzie. https://insightplus.bakermckenzie.com/bm/data-technology/indonesia-clarification-of-certain-provisions-of-the-pdp-law-by-the-constitutional-court.

as defined by prevailing laws and regulations, subject to, for example, relevant regulations like the State Defense Law. This is a justification used in the PDP to limit a data subject's rights.[519]

On August 31, 2023, the then Ministry of Communications and Information Technology (now KOMDIGI) 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 rely on cross-border agreements, standard contract clauses, and enforceable group company rules to do so.[520] However, in July 2025, Indonesia and the U.S. announced a landmark trade agreement establishing a bilateral adequacy framework: Indonesia committed to recognize the U.S. as a jurisdiction providing adequate data protection under Indonesian law.[521] This commitment, once implemented, will provide legal certainty for U.S. companies, particularly cloud service providers, digital platforms, and multinationals consolidating data across markets, by ensuring that personal data can be transferred from Indonesia to the U.S. without additional contractual mechanisms. At the same time, the adequacy framework may require reconciliation with existing sector-specific localization mandates (e.g., in financial services and telecommunications), as well as with restrictions on certain categories of public data, which remain ineligible for transfer. USTR should closely track the implementation of this bilateral adequacy arrangement to ensure it is applied consistently and does not become undermined by conflicting localization measures or discretionary enforcement. Despite this agreement, KOMDIGI and the Coordinating Ministry of Politics and Security (KemenkoPolkam) continue to discuss revision of GR 71/2019 to include stronger data localization mandate. The revision is expected to be finished by the end of 2026.

Taxation of Digital Products and Services

Indonesia issued Regulation No.17/PMK.010/2018 (Regulation 17) in 2018 to revise its tariff schedule.[522] The Regulation amends Indonesia's HTS Chapter 99 to add: "Software and other digital products transmitted electronically." This makes Indonesia the only country in the world

---

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

[520] Dyson, A. & Serwin, A. (2023, September 15). *Indonesia: prepare now for the new Personal Data Protection Law*. DLA Piper. https://www.lexology.com/library/document?tk=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJleHAiOjE3NjE3MDQ5NjEsImRhdGEiOnsiRG9jdW1lbnRHdWlkIjoiNTkxOTg3NmMtNjA3MS00NGQxLTgwMzUtNzU1MTdiOWEzZDhjIiwiQ29udGFjdEd1aWQiOiIwMDAwMDAwMC0wMDAwLTAwMDAtMDAwMC0wMDAwMDAwMDAwMDAiLCJCeXBhc3NMb2dpbiI6dHJ1ZX19.UD7Sp5o-1jFEvYZh2HA6CGrTXegnRgbIfRavQlRLhH_2rYzJyco0krHEU_nGMNlZIvaFQPPtMByXtRTeKnR0GA..

[521] The White House. (2025, July 22). *Fact Sheet: The United States and Indonesia Reach Historic Trade Deal*. https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-the-united-states-and-indonesia-reach-historic-trade-deal/.

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

that has added electronically transmitted products to its HTS. This unprecedented step in laying the groundwork to impose customs requirements on purely digital transactions will result in significant and unnecessary compliance burdens on nearly every enterprise, including many SMEs. While the tariff rate is currently specified as zero, the policy conflicts with Indonesia's commitment under the WTO's moratorium on customs duties on electronic transmissions, dating back to 1998[523] and most recently reaffirmed in June 2022.[524] In July 2025, however, the United States and Indonesia announced a breakthrough under the U.S.-Indonesia Reciprocal Trade Agreement Framework, with Indonesia committing to eliminate HTS tariff lines on intangible products, suspend import declaration requirements, and unconditionally support a permanent moratorium on e-commerce duties at the WTO.[525] This marks a major step toward bringing Indonesia back into alignment with global norms. That said, questions remain regarding implementation, particularly whether these commitments will be applied across the board or limited to U.S. digital products. Effective follow-through will be essential to ensure that Indonesia fully removes Regulation 17 and Chapter 99 from its HTS, provides legal certainty for all digital suppliers, and strengthens multilateral efforts to preserve the WTO e-commerce moratorium ahead of the 14th Ministerial Conference in 2026.

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" in Indonesia. Significant economic presence will reportedly 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 to domestic tax regulations, a departure from long-established international tax principles. This definition of permanent establishment could conflict with existing tax treaties, including with the United States, resulting in a new "electronic transaction tax" applying to income sourced from Indonesia.[526] 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, while also basing application of the tax on arbitrary distinctions between digital and non-digital companies competing in the same consumer markets. U.S. companies were cited as targets of these tax measures, and industry reports that this tax in effect only applies to non-Indonesian entities, reflecting a discriminatory taxation regime. Indonesia's designation of foreign

[523] WTO. (1998, May 25). *The Geneva ministerial declaration on global electronic commerce.* https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm
[524] World Trade Organization. (2022, June 17). *WTO Members secure unprecedented package of trade outcomes at MC12* [Press release]. https://www.wto.org/english/news_e/news22_e/mc12_17jun22_e.htm
[525] The White House. (2025, July 22). *Fact Sheet: The United States and Indonesia Reach Historic Trade Deal*. https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-the-united-states-and-indonesia-reach-historic-trade-deal/.
[526] EY. (2020, March 19). *Indonesian Government proposes key tax changes*. https://taxnews.ey.com/news/2020-0604-indonesian-government-proposes-key-tax-changes.

companies with significant economic presence as permanent establishments contradicts international norms of determining permanent establishment and creates a significant barrier for cross-border suppliers. Industry urges vigilance from U.S. government over these harmful taxation measures that hinder U.S. exports and, ultimately, the U.S. tax base, as the tax moves nearer to going into effect—the Ministry of Finance (MOF) will first need to promulgate additional legal measures for these new taxes to become enforced.

A new VAT on digital goods and services went into effect on April 1, 2022.[527] 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).[528] As of 2025, all non-resident B2B and B2C digital sales exceeding an annual threshold of IDR 600 million (approximately US$40,000) are subject to the 11% GST.[529] The regime applies broadly to SaaS, streaming services, cloud storage, advertising, and online marketplaces, requiring foreign suppliers to register, validate customer tax IDs, apply the appropriate rate, and file GST returns.

In July 2025, Indonesia formally codified a new 0.5% final income tax on e-commerce transactions through PMK Number 37 of 2025.[530] The measure designates major online marketplaces as tax collectors for transactions conducted by domestic sellers. The tax is levied on the gross turnover of sellers whose annual revenue exceeds Rp 500 million (approximately US$30,000), thereby exempting smaller enterprises. Although the policy was initially slated to take effect in February 2026, its implementation has been temporarily postponed to sustain household purchasing power and allow the national economy to recover.[531] The Minister of Finance has indicated that the policy will be activated once Indonesia's economic growth surpasses 6%. This measure poses a trade barrier because it imposes additional compliance and administrative costs on e-commerce platforms and sellers and can result in double taxation, which may disadvantage foreign suppliers and distort market access conditions.

---

[527] *Regulation 60/PMK.03/2022* [Indonesia]. (2022). https://jdih.kemenkeu.go.id/api/download/1bfe41fc-a312-41f0-b107-70e55b69767a/60~PMK.03~2022Per.pdf; Orbitax. (2022, May 12). *Indonesia Revises Regulations for VAT on Digital Goods and Services*. https://orbitax.com/news/country/article/Indonesia-Revises-Regulations--49820.
[528] Beh, Y. et al. (2022, September 26). Indirect Tax Developments in Asia-Spotlight on the Digital Economy. *Bloomberg Tax*. https://news.bloombergtax.com/daily-tax-report-international/indirect-tax-developments-in-asia-spotlight-on-the-digital-economy.
[529] TaxDo. (2025, October 8). *Indonesia Expands GST Enforcement on Foreign Digital Sellers in 2025*. https://taxdo.com/resources/blog/post/indonesia-gst-foreign-digital-sellers-2025.
[530] *PMK-37/2025 on the Appointment of Other Parties as Income Tax Collectors and Procedures for Collection, Deposit, and Reporting of Income Tax Collected by Other Parties on Income Received or Obtained by Domestic Traders through Electronic System Commerce, Article 2 and 3* [Indonesia]. (2025). https://jdih.kemenkeu.go.id/dok/pmk-37-tahun-2025
[531] Estherina, I. (2025, October 14). Indonesia's Finance Ministry Postpones Implementation of E-Commerce Tax. *Tempo.* https://en.tempo.co/read/2057226/indonesias-finance-ministry-postpones-implementation-of-e-commerce-tax.

Other Barriers to Digital Trade

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. Under the 2016 Negative Investment List, ownership for physical distribution, warehousing, and further logistics was limited to 67%, provided that each of these services was not ancillary to the main business line. However, Indonesia scrapped the Negative Investment List and adopted the Positive Investment List (PR 10/2021), which liberalized many logistics and distribution lines (e.g., wholesale distribution is no longer capped at 67%). Legislation took effect in November 2020 that aims to add clarity for e-commerce firms.[532]

Indonesia's Ministry of Industry issued regulation No. 22/2020 (IR22) on the Calculation of Local Content Requirements 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 developing 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. Indonesia's issuance of Presidential 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.[533] In April 2025, however, the government enacted new rules relaxing some of these requirements.[534] Under the revised framework, government agencies may now procure goods with 25 percent local content, down from the previous 40 percent threshold, and may purchase goods with even lower domestic content or import them outright in cases of supply constraints or unavailability. However, significant barriers remain: local content rules continue to apply across numerous sectors, and enforcement has already led to market restrictions. These requirements still impose discriminatory burdens on foreign suppliers and remain a prominent non-tariff barrier in U.S.-Indonesia trade relations. U.S. officials should closely monitor how the relaxed thresholds are implemented and whether they are applied consistently across procurements.

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

---

[532] Carl, M. S. & Rahimi. (2020, June 22). *Indonesia: Indonesia Introduces New Requirements For E-Commerce Companies*. Mondaq. https://www.mondaq.com/corporate-and-company-law/956332/indonesia-introduces-new-requirements-for-e-commerce-companies.

[533] *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/.

[534] Strangio, S. (2025, May 7). Indonesia to Loosen Local Content Rules Amid U.S. Tariff Negotiations. *The Diplomat*. https://thediplomat.com/2025/05/indonesia-to-loosen-local-content-rules-amid-us-tariff-negotiations/.

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.[535] The former 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."[536] 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.

Ireland

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In 2021, Ireland's grid operator imposed a de facto moratorium on new data center grid connections, effectively halting further expansion of data center capacity and significantly impacting U.S. firms, that have invested billions of dollars in facilities there.[537] The measure was justified as a way to address electricity security concerns, with data centers widely scapegoated for power shortages, even though the root cause lay in insufficient investment by the authorities in new grid infrastructure and generation capacity. Since then, Ireland's energy regulator has struggled to finalize a new grid connection policy, having worked on it for nearly three years without completion. This prolonged regulatory paralysis has created significant uncertainty and has severely constrained U.S. data center operators' ability to proceed with long-planned projects, undermining investment strategies and Ireland's competitiveness as a digital infrastructure hub.

In September 2024, the Irish procurement authority launched a process to establish a cloud procurement framework intended to enable the purchase of services from U.S. cloud service providers, but the effort ultimately failed after the authority insisted on unworkable terms and conditions that no U.S. provider could meet. Despite Ireland being home to extensive U.S. cloud infrastructure, the lack of such a framework has effectively excluded U.S. firms from public

[535] Cabinet Secretary of the Republic of Indonesia. (2023, September 25). *Gov't to Amend Regulation on Social Media Use for E-Commerce*. https://setkab.go.id/en/govt-to-amend-regulation-on-social-media-use-for-e-commerce/.
[536] *AP*. (2023, October 4). TiTok ends retail business in Indonesia after ban on social media shopping. https://apnews.com/article/indonesia-tiktok-ecommerce-ban-china-62e5ef9f366d8cfd4a94427393bb5aba.
[537] Commission for Regulation of Utilities. (2021). *CRU Direction to the System Operators related to Data Centre grid connection processing*. https://cruie-live-96ca64acab2247eca8a850a7e54b-5b34f62.divio-media.com/documents/CRU21124-CRU-Direction-to-the-System-Operators-related-to-Data-Centre-grid-connection-.pdf.

sector cloud projects. A leaked internal government briefing note revealed that the extraterritorial application of the U.S. CLOUD Act, which it controversially likened to the Chinese Cybersecurity Law, was considered a red-line issue. The note also suggested that perceived "U.S. political turmoil" introduced excessive risk, which the government cited as justification for precluding the use of U.S. cloud services by the Irish public sector. This policy position creates a significant market access barrier for U.S. providers and constrains Ireland's ability to modernize its public sector IT systems.

Italy

Asymmetric Platform Regulation

On August 27, 2022, Law No. 118, the "2021 Annual Competition Law," went into effect.[538] The law presumes that commercial users of certain digital platforms are economically dependent, which platforms can challenge, where they offer digital intermediation services that facilitate transactions for end users or suppliers.[539] Examples of presumptively abusive behavior identified 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. The Italian Competition Authority now has the power to demand information from digital platforms even without launching a formal proceeding.[540]

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Ministry of Culture's interpretation of the Italian Cultural Heritage Code (D.Lgs. 42/2004) continued to create significant barriers to the provision of cloud services to educational institutions.[541] The Ministry's broad classification of public archives, including school records and educational documentation, as "cultural heritage" under Italian law effectively restricts the storage and transfer of digitalized public documents outside Italian territory. This restrictive interpretation, combined with the absence of clear harmonization between cultural heritage

---

[538] Beretta, M. & Tremolada, R. (2022, August 16). *The Italian Parliament Approves Competition Law Reform. Cleary Antitrust Watch*. https://www.clearyantitrustwatch.com/2022/08/the-italian-parliament-approves-competition-law-reform/.

[539] Canino, I. et al. (2022, August 26). *Entry into force of Italy's Annual Law for Competition (Legge annuale per il mercato e la concorrenza 2021) Brings Far-Reaching Changes to the Italian Competition Law and Economic Dependence Law*. JD Supra. https://www.jdsupra.com/legalnews/entry-into-force-of-italy-s-annual-law-9761724.

[540] Ashurst. (2022, October 3). *CN08 - Italian Competition Authority - new powers to address concentrations and conduct*. https://www.ashurst.com/en/insights/competition-law-newsletter-october-2022/cn08---italian-competition-authority---new-powers-to-address-concentrations-and-conduct/.

[541] *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137* [Italy]. (2004). https://presidenza.governo.it/usri/confessioni/norme/d_lgs_42-2004.pdf; *Linee guida per la gestione documentale nelle Istituzioni scolastiche* [Italy]. (n.d.). https://www.istruzione.it/responsabile-transizione-digitale/allegati/MI_RTD_Gestione%20documentale_Linee%20Guida%20Scuole_versione%20finale.pdf.

protection rules and modern cloud computing needs, creates a substantial obstacle to digital trade and disproportionately affects non-EU cloud providers seeking to serve Italian schools and educational institutions.

Discriminatory Local Content Quotas and Audiovisual Services Mandates

Italy implemented the EU Audiovisual Media Services Directive ("AVMS-D") in 2022. The implementing measure in question envisages a significant increase in mandatory investment in local productions—so excessive as to endanger 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 (which includes Italian works) that would grow, by 2025, to up to 25% of the given company's net revenues of the previous year. Such levels 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.[542] The quotas remained, with a slight reduction in the quota to 20% following 2024, which still reflects an excessively high level.[543]

Government-Imposed Restrictions on Internet Content and Related Access Barriers

In 2024, Italy put in place a national anti-piracy platform, called 'Piracy Shield', that enables rightsholders to obtain orders directing local ISPs to block websites offering illegal streaming or downloads of copyrighted content, such as movies, TV shows, live sports and music. This content then needs to be taken down within a very short time frame of 30 minutes, with rightsholders using an automated system administered by the Italian Audiovisual Authority (AGCOM) to submit such claims. CCIA has warned[544] about the over blocking effects of such a platform, leading to serious disruptions of legitimate services, which are now well documented.[545]

In 2025, the Italian authority proposed amendments to their copyright regime to formally incorporate and expand the use of the Piracy Shield platform to facilitate the expedited blocking of websites allegedly infringing copyright. CCIA warned the European Commission about the

[542] D'Arena, S. & Apa, E. (2022). [IT] *Italy transposes Directive (EU) 2019/790 (DSM Copyright), Directive (EU) 2019/789 (Sat Cab) and Directive (EU) 2018/1808 (Audio Visual Media Services)*. IRIS Merlin. https://merlin.obs.coe.int/article/9359.
[543] Apa, E. & Foco, E. (2022, February 21). *Focus: Transposition of the Revised AVMSD*. Portolano Cavallo. https://portolano.it/en/newsletter/portolano-cavallo-inform-digital-ip/focus-transposition-of-the-revised-avmsd.
[544] CCIA. (2025, February 18). *Overblocking From Anti-Piracy Measures Across EU Raises Concerns*. https://ccianet.org/news/2025/02/overblocking-from-anti-piracy-measures-across-eu-raises-concerns/.
[545] Sommese, R. (2025, October 17). *An Italian case study: Collateral damage from live-event site blocking with Piracy Shield*. APNIC. https://blog.apnic.net/2025/10/17/an-italian-case-study-collateral-damage-from-live-event-site-blocking-with-piracy-shield/.

negative effects this could have on the industry and formally submitted comments.[546] Based on these, the European Union warned the Italian authorities that the proposed changes were deviating from the DSA framework and invited the Italian authorities to ensure that the Piracy Shield operates with sufficient controls and safeguards to avoid over blocking and negative impact on information which is not illegal content. Industry is concerned that while the Italian authorities have introduced some modifications to the regime, they haven't significantly addressed the concerns expressed by them and echoed by the European Commission and therefore, the risk of over blocking is still high.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

In March 2025, AGCOM launched a consultation on the extension of the current rules for telecommunication companies to all CDNs operating on the Italian territory, along with all CAPs who own or operate CDNs in Italy, to which CCIA Europe responded.[547] In July 2025, the regulator has decided to extend the telecom regulatory framework to the above mentioned internet players. This decision threatens to open the door for network usage fees. While the regulator denies any link to the fair share debate, it is very clear that they are instating a dispute resolution mechanism, the prime mechanism that telecom incumbents have championed ever since 2022 at the start of their "fair share" campaign (first suggested by Connect Europe in 2022).[548] Mandatory dispute resolution would allow large ISPs to trigger repeated cases to set precedents for paid peering, gradually dismantling today's settlement-free model. It would also shift the internet towards a "Sending Party Network Pays" regime, forcing CAPs and CDNs, despite already covering most delivery costs, to pay ISPs simply because more traffic flows into their networks.

Taxation of Digital Products and Services

Italy's 2020 Budget introduced a 3% digital services tax closely aligned with the EU's original proposal. Covered services started accruing tax on January 1, 2020, with the global revenue threshold set at €750 million, and the local threshold at €5.5 million. 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);"

---

[546] CCIA. (2025, May 21). *TRIS – Italy's Piracy Shield – CCIA Europe's contribution*. https://ccianet.org/library/tris-italys-piracy-shield-ccia-europes-contribution/.
[547] *Avvio del procedimento istruttorio e della consultazione pubblica per la ricognizione delle condizioni di applicabilità del regime di autorizzazione generale previsto dal codice alle Content Delivery Network (CDN)* [Italy] Delibera 55/25/CONS. (2025). https://www.agcom.it/provvedimenti/delibera-55-25-cons; CCIA. (2025). *CCIA Europe Response to AGCOM's Consultation on Content Delivery Networks*. https://ccianet.org/wp-content/uploads/2025/04/CCIA-Europe-response-to-AGCOM-Consultation-on-Resolution.pdf.
[548] *Ricognizione delle condizioni di applicabilità del regime di autorizzazione generale previsto dal Codice delle comunicazioni elettroniche alle Content Delivery Network* [Italy]. (2025). https://www.agcom.it/provvedimenti/delibera-207-25-cons.

and the "transmission of data collected from users and generated by the use of a digital interface."[549] The tax predominantly affected 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.[550] Although it continues to collect the tax, Italy agreed to credit DST payments towards future OECD-based liability, and eliminate the DST based on implementation of the OECD Two Pillar solution.[551] However, the current government has explicitly stated its intention to maintain and potentially expand the DST if negotiations on Pillar 1 collapse.[552] U.S. officials should work to ensure that this discriminatory tax is removed and deter any potential expansion, given that Italy has already extracted $1.8 billion as of 2024,[553] largely from U.S. firms.

Japan

Asymmetrical Platform Regulation

Enacted on June 3, 2020, Japan's Act on Improving Transparency and Fairness of Digital Platforms (TFDPA) sets out a framework for oversight of large online platforms designated by the Ministry of Economy, Trade and Industry (METI) as "Specified Digital Platform Providers."[554] The law is intended to enhance transparency and fairness in platform operations by requiring disclosure of key terms and conditions, ranking criteria, data usage practices, and mechanisms for complaints. It also obliges designated providers to submit annual reports and take steps to improve user-provider relationships. METI conducts evaluations, may issue recommendations or orders, and can request action from the Fair Trade Commission in cases involving competition concerns. The Act empowers METI to request action from the Japan Fair Trade Commission in the event of noncompliance, and requires period review to account for changes in market and technological conditions. The Act can be onerous for U.S. firms as its implementation has disproportionately targeted four American platforms with burdensome reporting, opaque oversight, and requirements that extend beyond the law's original scope.

---

[549] EY. (2024, October 16). *Italy's Digital Services Tax enters into force as of 1 January 2020*. https://globaltaxnews.ey.com/news/2020-5083-italys-digital-services-tax-enters-into-force-as-of-1-january-2020.
[550] CCIA. (2025). *CCIA Europe Response to AGCOM's Consultation on Content Delivery Networks*. https://ccianet.org/wp-content/uploads/2025/04/CCIA-Europe-response-to-AGCOM-Consultation-on-Resolution.pdf
[551] Office of the U.S. Trade Representative. (2021, October 21). *USTR Welcomes Agreement with Austria, France, Italy, Spain, and the United Kingdom on Digital Services Taxes*. 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.
[552] Fonter, G. (2024, March 20). Italy could extend its web tax if global minimum tax deal fails. *Reuters*. https://www.reuters.com/world/europe/italy-could-extend-its-web-tax-if-global-minimum-tax-deal-fails-2024-03-20/.
[553] CCIA. (2025, July 8). *Status of Key Digital Services Taxes in July 2025*. https://ccianet.org/library/status-of-key-digital-services-taxes-in-july-2025/.
[554] *Act on Improving Transparency and Fairness of Digital Platforms* [Japan] Act No. 38. (2020). https://www.japaneselawtranslation.go.jp/ja/laws/view/4532/en.

USTR should urge Japan to align implementation of the TFDPA with its legislative mandate of "minimum necessary measures," as current practice imposes disproportionate administrative burdens, solely impacting U.S. firms, through opaque oversight mechanisms and prescriptive ministerial evaluations.

On July 5, 2022, METI released a Cabinet Order stipulating that the digital advertising sector would be regulated under the TFDPA.[555] 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 (roughly US$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 (roughly US$345.7 million) each fiscal year in Japan. The 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.[556] In February 2024, METI released[557] its first major review of compliance with the new law, evaluating the practices of six companies, four of which were U.S. multinationals. Based on this review, METI called on the targeted companies to "strive to improve their operations" or face "certain [unspecified] measures," authorized under the TFDPA (e.g., a ministerial recommendation to "promptly cease its disadvantageous treatment" (Article 10). To date, no such recommendations appear to have been issued.

In June 2024, Japan's Diet passed a law proposed by the Digital Market Competition Headquarters (DMCH) to address competition concerns in the mobile market ecosystem. The law, entitled "Act on Promotion of Competition for Specified Software used in Smartphones"[558] (SSCPA) was promulgated on June 19, 2024, and is scheduled to take effect starting December 18, 2025. On March 31, 2025, the Japan Fair Trade Commission (JFTC), the agency tasked with enforcing the law, issued designations for the firms subject to the SSCPA, scoping in just two companies, both U.S. based, while noting that no Japanese or third-country competitors currently meet the legal thresholds for designation, based on a narrow definition of the market that

[555] METI. (2022, July 5). *Cabinet Decision on Improving Transparency and Fairness of Digital Platforms*. https://www.meti.go.jp/english/press/2022/0705_001.html
[556] Secretariat of the Headquarters for Digital Market Competition Cabinet Secretariat. (2021). *Evaluation of Competition in the Digital Advertising Market Final Report : Summary*. https://www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_210427.pdf.
[557] METI. (2024, February 2). *Evaluation on Transparency and Fairness of Specified Digital Platforms Compiled*. https://www.meti.go.jp/english/press/2024/0202_002.html.
[558] *Act on Promotion of Competition Concerning Specified Software Used in Smartphones* [Japan] No. 58. (2020). https://laws.e-gov.go.jp/law/506AC0000000058/20251218_000000000000000.

excluded a major Japanese operator. In July 2025, the JFTC published implementing regulations further detailing the requirements imposed on designated firms.[559]

For designated companies, the SSCPA seeks to prohibit, on an ex ante basis, 13 forms of conduct, almost all of which have parallels with the DMA. Included among prohibitions are practices relating to tying (bundling of services), self-preferencing (providing advantages to self-owned products or services), technical interoperability, use of commercial data, default settings, service portability, and third-party sellers' ability to communicate with their customers. Since these practices are common across many industries, and in many cases have strong consumer welfare effects (e.g. consumer convenience, efficient pricing, protection of privacy and preventing malware), the presumption that they are or are likely to be anticompetitive, and that their use could result in harm, is unjustified. Although the SSCPA provides greater leeway than the DMA for a company to defend practices that might otherwise run afoul of the prohibitions, the presumption against such practices, in addition to having questionable benefits to competition is likely to incur significant compliance costs on U.S. suppliers.

Japan should also reconsider the broader policy of identifying a market so narrowly as to intentionally capture specific U.S. companies while exempting local competitors, both in the mobile ecosystem and in parallel markets. Although one of the stated intents of the law is to create more competitive digital marketplaces, other digital markets in Japan, dominated by Japanese suppliers, have not been similarly regulated although many practices mirror those the SSPCA seeks to prohibit. For example, two companies, Nintendo and Sony, control 99% of the console gaming market In Japan (70 and 2%, respectively).[560] Like U.S. suppliers of mobile apps, these companies also operate a "walled garden" game store, require commissions on games equal to those of app stores, and prohibits the use of alternative payment systems. In addition, both companies are major developers of games they sell in those stores.[561] Since mobile apps often compete against such games, subjecting U.S. firms to onerous prohibitions while exempting a competing Japanese supplier raises concerns about disproportionate impacts on U.S. firms, which could be viewed as inconsistent with Japan's National Treatment and MFN commitments in the WTO with respect to distribution services.

Japan should refrain from imposing prescriptive, discriminatory conduct restrictions based on arbitrary thresholds that exclude Japanese and third-country competitors; ensure designated firms have meaningful defenses where restrictions apply equally to others; and align implementation with the Diet Resolution calling for proportionate measures that do not undermine user convenience. USTR should also stress the need to minimize overly rigid guidelines and reporting

[559] *Mobile Software Competition Act Guidelines* [Japan]. (2025). https://www.jftc.go.jp/file/MSCA_Guidelines_tentative_translation.pdf.
[560] Knezovic, A. (2025, August 29). *Japanese Gaming Market*. Udonis. https://www.blog.udonis.co/mobile-marketing/mobile-games/japanese-gaming-market.
[561] STATISA. (2024). *Sales volume of best-selling video games for consoles in Japan in 2024*. https://www.statista.com/statistics/322746/best-selling-console-games-japan/.

burdens that jeopardize proprietary technologies and innovation, and to fully account for security risks that could arise from requirements opening systems to potentially untrustworthy third parties, which would erode consumer and developer trust.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In May 2022, Japan enacted the Economic Security Promotion Act, a framework intended to strengthen national security by reducing reliance on foreign supply chains and securing essential infrastructure, including AI and cloud computing.[562] Under this framework, METI designated "Cloud Programs" as specified critical products, enabling the government to provide substantial financial support to domestic companies developing critical infrastructure.

In April 2024, Japan launched a major subsidy program for domestic GPU procurement (necessary for AI model training) as part of its broader ¥10 trillion (approximately $65 billion) investment through Fiscal Year 2030 to strengthen its semiconductor and frontier AI capabilities.[563] Led by METI, this program allocates massive public funding to a select group of domestic companies to build sovereign AI infrastructure, largely excluding foreign participation from the most critical projects. Under the program, METI approved up to ¥72.5 billion (approximately $470 million) in subsidies for five Japanese firms, including Sakura Internet Inc. and KDDI Corporation, to develop domestic AI supercomputers, with Sakura Internet alone receiving up to ¥50.1 billion for its GPU cloud service. By directly subsidizing local companies for GPU purchases, the policy strongly favors on-premise and "sovereign cloud" infrastructure, effectively shutting out U.S. hyperscale cloud providers from these strategic AI development initiatives and creating an uneven competitive landscape.

In May 2024, Japan passed the Act on the Protection and Utilization of Important Economic Security Information (CESI Act),[564] establishing a new security clearance framework intended to protect sensitive government information tied to national security. The law, which came into effect in May 2025 focuses on Critical Economic Security Information, which includes data less sensitive than "Specially Designated Secrets" but still vital to national security, such as information related to critical infrastructure, cyber threats, and supply chain vulnerabilities. The system applies to private companies handling this information, including those engaged in international research, defense, and critical infrastructure projects. Operational standards and detailed regulations were finalized in January 2025, but the framework's physical security requirements are structured around outdated, on-premise IT environments, creating a major

[562] *Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures* [Japan] Act No. 43. (2022). https://www.japaneselawtranslation.go.jp/en/laws/view/4523/je.
[563] Japan Ministry of Economy, Trade, and Industry. (2024, April 9). *Approval of Plans for Ensuring a Stable Supply of Cloud Programs under the Economic Security Promotion Act*. https://www.meti.go.jp/english/press/2024/0419_001.html.
[564] *Summary of the Act on the Protection and Utilization of Critical Economic Security Information* [Japan]. (2024). https://www.japaneselawtranslation.go.jp/outline/127/905R626.pdf

barrier for modern, highly secure cloud solutions offered by U.S. providers. These requirements include the use of a dedicated physical space with perimeter security measures such as locks and fences, physical storage for media, and stand-alone systems with no internet connection, which inherently exclude cloud-based offerings. This approach effectively favors legacy systems over advanced security architectures like zero-trust frameworks, real-time monitoring, and encryption that exceed the protection levels of physical controls. A shift toward a risk-based and technology-neutral security model would allow companies to meet security objectives through the most effective means available, enabling the use of modern cloud infrastructure and fostering fair competition in government procurement. Without such reform, Japan risks entrenching barriers that limit the participation of U.S. cloud providers in sensitive public sector projects.

Japan's current information security guidelines for handling restricted and classified information in national security and defense contexts, which remain rooted in legacy physical security mandates, create major barriers for the use of modern cloud infrastructure.[565] These guidelines require the use of stand-alone, air-gapped or non-networked systems for processing sensitive data and mandate the installation of physical security facilities such as dedicated secure rooms and on-site access controls for inspection. This approach effectively excludes the use of hyper-scale public cloud services, including those offered by U.S. providers, whose security model is based on software-defined protections such as encryption, granular access controls, and virtual isolation rather than physical segregation. As a result, the Japanese Ministry of Defense (MOD) and related agencies are forced to rely on expensive, inflexible, and often less secure on-premise systems. This structural bias toward on-premise environments also undermines U.S.–Japan defense and cybersecurity cooperation, as modern allied military operations increasingly rely on shared cloud environments for real-time, secure information sharing across command, control, intelligence, and cyber defense systems. By keeping critical defense workloads isolated on legacy infrastructure, Japan's approach creates interoperability gaps that weaken operational coordination and overall alliance deterrence. While the MOD announced a "hybrid cloud" modernization plan in early 2025, aimed at integrating space and cyber capabilities by Fiscal Year 2029, this initiative only partially addresses the issue.[566] Because the underlying security rules mandating physical controls remain unchanged, hybrid cloud adoption will be limited to non-classified or lower-sensitivity workloads, leaving mission-critical systems trapped in outdated IT environments and perpetuating interoperability challenges with allies.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Japan's Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the

[565] Acquisition, Technology and Logistics Agency (ATLA) Ministry of Defense, Japan. (2023). *Defense Industrial Security Manual*. https://www.mod.go.jp/atla/img/en/dism/dism2023_en.pdf
[566] Japan Ministry of Defense. (2022). *National Defense Strategy*. https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf

Senders (Act No. 137 of 2001) establishes liability protections for internet and telecommunications service providers while creating a framework for rights-holders to address online infringements.[567] It limits providers' responsibility for user-generated content unless they knowingly host infringing material or reasonably should have known of it, and protects providers from liability when they block suspected infringing content under defined procedures. The Act also grants individuals whose rights are infringed the ability to demand disclosure of identifying information about senders from service providers, subject to evidentiary and necessity requirements, with safeguards such as notifying the sender and limiting provider liability for disclosure decisions. In 2021, the Act was amended to create a new special court mechanism, the "Sender Information Disclosure Procedure," designed to streamline rights-holder requests for disclosure of sender information, particularly in cases of online defamation and piracy. In practice, the Act has been invoked by major Japanese rights-holders, including leading domestic publishers, to pursue legal action against U.S.-based internet infrastructure providers, arguing that their content delivery and security services facilitated piracy.[568] While intended to protect creators, such expansive use of the disclosure and liability framework risks placing disproportionate legal and compliance burdens on foreign service providers, potentially functioning as a barrier to U.S. firms by exposing them to heightened litigation risks and regulatory uncertainty in Japan.

Compounding this challenge is that U.S. technology companies with operations in Japan are legally required to register their U.S. entity in the country. This is a requirement under Japan's Corporate Law, designed to facilitate Japan domestic legal proceedings, particularly those related to online abuse and defamation.[569] In 2022, the Japanese government singled out and pressured U.S. technology companies to register their U.S. entities in Japan.[570] CCIA urges USTR to press Japan to ensure that liability standards under this Act are applied through a reasonable notice-and-takedown framework, particularly for content delivery networks, and to encourage legal reforms that shield intermediaries from excessive court-imposed liability, consistent with safe harbor and legal remedies provisions the United States has advanced in trade agreements.[571]

---

[567] *Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders* [Japan] Act No. 137. (2001). https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/H13HO137.pdf.

[568] Sharwood, S. (2022, February 1). Attack on Titan: Four Japanese Manga publishers sue Cloudflare. *The Register*. https://www.theregister.com/2022/02/01/manga_publishers_sue_cloudflare/.

[569] Japan Ministry of Justice. (n.d.). *Do you remember to register a Foreign Company*. https://www.moj.go.jp/EN/MINJI/m_minji07_00002.html.

[570] Nishi, M. (2022, September 19). *Google, Meta and other Big Tech companies required to register headquarters in Japan*. Clifford Chance. https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2022/09/google-meta-and-other-big-tech-companies-required-to-register-h.html.

[571] Office of the United States Trade Representative. (2018, November 30). *Agreement between the United States of America, the United Mexican States, and Canada: Chapter 20 ("Intellectual Property Rights"), Article 20.88* [Text of trade agreement]. https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/20%20Intellectual%20Property%20Rights.pdf#page=58.

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 2021, capturing suppliers even if they lacked a juridical presence in Japan.[572] This change mandates that foreign OTT services, including 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.[573]

The Personal Information Protection Commission, the data protection authority in Japan, has amended the Act on the Protection of Personal Information in May 2020, which came into effect from April 2022.[574] 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.[575]

Taxation of Digital Products and Services

In April 2025, Japan introduced new tax collection obligations requiring certain online platforms to collect and remit consumption taxes on behalf of non-Japanese businesses providing digital services to Japanese consumers, applying a transaction threshold of ¥5 billion (US$32.9 million).[576] This regime is now under discussion for possible expansion to cover additional cross-border e-commerce transactions,[577] which could amplify competitive disparities if the high threshold remains in place. These concerns are further compounded by the broader need for

---

[572] Niwa, D. (2021, May 7). *Japan's efforts to strengthen the effectiveness of enforcement against foreign telecommunications operators*. JD Supra. https://www.jdsupra.com/legalnews/japan-s-efforts-to-strengthen-the-8593184/.
[573] Data Guidance. (2023, June 22). *Japan: Amendments to Telecommunications Business Act enter into effect*. https://www.dataguidance.com/news/japan-amendments-telecommunications-business-act-enter.
[574] *Act on the Protection of Personal Information* [Japan]. (2022). https://www.ppc.go.jp/en/legal/.
[575] Schaetzel, L. & Sulkin, R. (2022, March 15). *Amended Japanese Privacy Law Creates New Categories of Regulated Personal Information and Cross-Border Transfer Requirements*. JD Supra. https://www.jdsupra.com/legalnews/amended-japanese-privacy-law-creates-7847421/.
[576] Japan National Tax Agency. (n.d.). *Platform Taxation of Consumption Tax*. https://www.nta.go.jp/english/taxes/consumption_tax/05.htm.
[577] Masuda, T. (2025, April 22). *Japan considers next steps for VAT on cross-border e-commerce*. International Bar Association. https://www.ibanet.org/Japan-considers-next-steps-for-VAT-on-cross-border-e-commerce.

Japan to accelerate the digitalization and internationalization of its administrative and customs procedures, particularly through full English accessibility, to reduce compliance costs and ensure equitable treatment for U.S. firms.

Kazakhstan

Asymmetric Platform Regulation

Kazakhstan's Antimonopoly Agency (AMA) is considering proposed amendments to the country's competition laws aimed at regulating major digital platforms, closely mirroring the European Union's Digital Markets Act.[578] By adopting these measures, the AMA explicitly seeks to replicate the EU "gatekeeper" model, arguing that large global platforms benefit from entrenched network effects and market power that hinder competition. Non-compliant firms could face restricted access to the Kazakh market. This shift from traditional antitrust enforcement toward ex ante regulation of dominant digital players represents a significant evolution in Kazakhstan's competition policy and could impose substantial compliance and operational burdens on U.S. technology companies active in the market.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Kazakhstan maintains a comprehensive data localization regime that requires most personal and communications data to be stored domestically. The Law on Personal Data and Its Protection (No. 94-V) and its implementing regulations mandate that personal data be stored in databases located within Kazakhstan, affecting both domestic and foreign entities.[579] The Informatization Law (No. 418-V) reinforces this obligation by requiring electronic databases containing personal data to be hosted on servers located in the country.[580] Additionally, Order No. 38/NK requires entities registering domain names in the Kazakhstani internet segment to host their servers and related technical infrastructure within Kazakhstan.[581] The Communications Law (No. 567-II) and subsequent regulations impose similar localization requirements on telecom operators and prohibit the cross-border transfer of subscriber and service information except in narrow circumstances, such as when serving Kazakh subscribers abroad.[582] These measures create significant barriers to digital trade. Mandatory domestic storage raises operational and compliance costs for foreign providers, particularly cloud, communications, and platform services that rely on integrated global infrastructure. The restrictions also limit the ability to provide cross-border services efficiently, undermine economies of scale, and reduce flexibility in

[578] Murphy, R. (2025, March 19). *Mapping the Brussels Effect*. Center for European Policy Analysis. https://cepa.org/comprehensive-reports/the-brussels-effect-goes-global/.
[579] *On Personal Data and their Protection* [Kazakhstan] No. 94-V. (2013). https://adilet.zan.kz/eng/docs/Z1300000094.
[580] *Law No. No. 418-V ЗРК* [Kazakhstan]. (2015). https://adilet.zan.kz/rus/docs/Z1500000418#z36.
[581] *Об утверждении Правил регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета* [Kazakhstan]. (2018). https://adilet.zan.kz/rus/docs/V1800016654.
[582] *Law No. 230-V* [Kazakhstan]. (2014). https://adilet.zan.kz/eng/docs/Z040000567_.

cybersecurity and disaster recovery planning. Furthermore, broad and vague implementation rules increase regulatory uncertainty and expose companies to enforcement risks, which can deter investment and market entry by international service providers.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Kazakhstan's government is moving to adopt a comprehensive Digital Code by the end of 2025. This initiative builds on earlier regulatory mandates, including a 2023 law requiring foreign social media platforms with more than 100,000 daily users to establish local legal representation.[583] While officially framed as a measure to combat "harmful content" and strengthen digital governance, critics view the Digital Code as a potential instrument of political censorship, raising concerns about its chilling effect on online speech and its implications for the open flow of information.

Potential Challenges to the Development of AI

Kazakhstan's draft Law on Artificial Intelligence, approved by the legislature on September 24, 2025 and expected to enter into force in early 2026, establishes a comprehensive risk-based regulatory framework for AI systems.[584] It requires all AI systems to be classified according to their level of risk and autonomy, with high-risk systems designated as critical information and communication infrastructure subject to mandatory audits, logging, documentation requirements, and enhanced state supervision. The law also prohibits AI applications that exploit emotions, manipulate human behavior, conduct social scoring, or collect personal data without consent, mandates the labeling of AI-generated content, and introduces stronger transparency obligations, requiring deployers to explain system operation, provide users with information about automated decisions, and allows users to refuse AI interactions. In addition, the proposed AI Act requires registration of products, an unworkable requirement that poses a considerable compliance burden and makes it difficult for companies to introduce products into the market, particularly given the speed at which AI technologies evolve. Owners and operators of AI systems are held liable for damages, and the legislation signals the possible introduction of mandatory liability insurance in the future. While intended to promote safety and accountability, these measures may impose heavy compliance burdens on foreign AI developers and deployers, as audit and documentation obligations, labeling requirements, product registration, and heightened liability exposure could increase costs and legal uncertainty, while broad regulatory discretion over risk classification may create unpredictable compliance obligations that complicate market entry and operations in Kazakhstan.

---

[583] *Об онлайн-платформах и онлайн-рекламе* [Kazakhstan]. (2023). https://online.zakon.kz/Document/?doc_id=37166153&pos=4;-108#pos=4;-108.

[584] Akhmetkali, A. (2025). Kazakhstan Enacts AI Law, Parliament Weighs Opportunities and Risks. *The Astana Times*. https://astanatimes.com/2025/09/kazakhstan-enacts-ai-law-parliament-weighs-opportunities-and-risks/; Zhexenbekov, A. (2025, September 26). Kazakhstan to launch national AI platform. *Kazinform International News Agency.* https://qazinform.com/news/kazakhstan-to-launch-national-ai-platform-509716. .

Kenya

Asymmetric Platform Regulation

On May 28, 2024, Kenya's Competition Authority published proposed amendments to the Competition Act, seeking to significantly expand its authority to regulate large digital companies operating domestically. The amendments would significantly broaden thresholds for investing digital firms' activity from the existing standard of "abuse of power" to an "abuse of superior bargaining position" standard—allowing the Authority to potentially challenge any transaction, regardless of its effect on market competition or consumer welfare. This overly broad, ambiguous standard therefore risks stifling market access,[585] and USTR should engage with the Kenyan government to encourage a more targeted, clearly defined threshold.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Data Protection Act does not require the localization of personal data generally, but under Section 50 of the Act,[586] the Cabinet Secretary is empowered to decide the types of personal data that must be stored and processed in Kenya due to the protection of strategic interests of the state or revenue. 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.[587] At a minimum, a company must store a copy of data that is categorized under these definitions in a data center located in Kenya.

The Computer Misuse and Cybercrimes Act of 2018,[588] and the Computer Misuse and Cybercrime Regulations of 2024,[589] both impose onerous and restrictive data localization and reporting obligations on providers of "Critical Information Infrastructure," which includes cloud services providers, with increased restrictions for certain categories of data. Operators of 'Critical Information Infrastructure' are obligated to establish a Cybersecurity Operations Center domestically to monitor and report compliance to the Communications Authority.

---

[585] CCIA. (2024, June 18). *CCIA Comments on the Competition Authority of Kenya's Draft Competition (Amendment) Bill, 2024*. https://ccianet.org/library/ccia-comments-on-the-competition-authority-of-kenyas-draft-competition-amendment-bill-2024/.
[586] *The Data Protection Act* [Kenya] Act No. 24. (2019). https://www.kentrade.go.ke/wp-content/uploads/2022/09/Data-Protection-Act-1.pdf.
[587] *The Data Protection (Civil Registration) Regulations* [Kenya]. (2020). https://www.odpc.go.ke/wp-content/uploads/2024/06/THE-DATA-PROTECTION-CIVIL-REGISTRATION-REGULATIONS-final2-1.pdf.
[588] *The Computer Misuse and Cybercrimes Act* [Kenya]. (2018). https://nc4.go.ke/the-computer-misuse-and-cybercrimes-act-2018/.
[589] *The Computer Misuse and Cybercrime (Critical information Infrastructure and Cybercrime management) Regulations* [Kenya]. (2024). https://nc4.go.ke/the-computer-misuse-and-cybercrime-criticalinformation-infrastructure-and-cybercrimemanagement-regulations-2024/.

On May 2, 2025, the Kenya Cloud Policy, 2025 took effect following its publication in the Kenya Gazette.[590] The policy, issued under the Kenya Information and Communication Act, requires all public entities to prioritize cloud-based solutions in new information and communication technology investments, including hardware, software, and infrastructure upgrades. Where applicable, public entities are directed to favor government-approved cloud service providers based in Kenya, provided they meet required standards. While framed as a measure to strengthen national infrastructure, the preference for local providers risks excluding or disadvantaging foreign suppliers, creating discriminatory barriers to market access that conflict with Kenya's trade commitments and undermine the competitiveness of U.S. cloud and digital service providers.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

The Kenyan government imposed widespread restrictions on the internet[591] throughout June and July 2024 in response to ongoing protests, resulting in a 40% drop in connectivity across major networks, and affecting all major telecommunications providers. The shutdowns took place despite explicit legal and verbal commitments by the government not to impose such restrictions and cost the economy approximately US$6.3 million in lost GDP per day.[592] Similar protests in 2025 led to prohibition of live broadcasting of demonstrations, and the temporary shutting down of several stations, an action overturned by the high court.[593]

On September 18, 2024, the government introduced the Computer Misuse and Cybercrime Bill to the National Assembly.[594] Under the proposed Bill, the National Computer and Cybercrimes Coordination Committee would have the authority to block websites and apps for promoting "illegal activities" and "extreme religious and cultic practices." Given the Bill's vague definitions and the government's interest in using cybercrime criminalization to target political opponents,[595] the risk of abuse if the Bill were to pass remains high. The bill remains under consideration.

---

[590] *The Kenya Cloud Policy* [Kenya] GN No. 3389. (2025). https://new.kenyalaw.org/akn/ke/officialGazette/2025-05-02/83/eng@2025-05-02/source.
[591] Kivuva, M. (2024, June 26). Urgent Concerns Regarding Internet Shutdown in Kenya during the #RejectFinanceBill2024 demonstrations. *KICTANet*. https://www.kictanet.or.ke/urgent-concerns-regarding-internet-shutdown-in-kenya-during-the-rejectfinancebill2024-demonstrations/.
[592] *Ibid.*
[593] Otieno, S. (2025, June 25). High Court orders CA to restore signals to three independent TV stations. *Daily Nation*. https://nation.africa/kenya/news/high-court-orders-ca-to-restore-signals-to-three-independent-tv-stations--5095146.
[594] *The Computer Misuse and Cybercrime (Criticalinformation and Cybercrimemanagement) Regulations* [Kenya]. (2024). https://nc4.go.ke/the-computer-misuse-and-cybercrime-criticalinformation-infrastructure-and-cybercrimemanagement-regulations-2024/.
[595] Muia, W. (2024, October 1). Uproar as Kenyan activist in court over cyber-crime. *BBC*. https://www.bbc.com/news/articles/c1wngd0d0n2o.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

In April 2024, the Communication Authority of Kenya published a Programming Code for Broadcasting Services and subsequently issued letters to large digital companies to comply with the code. On July 26, 2024, the Film and Classification Board published four additional regulations targeting OTT service providers. Under existing law, neither body has the legal authority to regulate OTTs, raising serious concerns about the government's intention to regulate OTT service providers as traditional broadcasters, and risking duplicative, costly regulations that would impose barriers on market access.

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. [596] This provision conflicts with the 2019 Data Protection Act, which enables cross-border data transfers subject to conditions set out by the Data Commissioner.

Taxation of Digital Products and Services

Kenya implemented several tax laws in 2020 implicating digital trade. First, a 20% withholding tax on "marketing, sales promotion and advertising services" provided by non-resident persons; second, a 1.5% DST 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, which was initially changed from zero-rated to exempt, but was restored to zero-rated status in July 2023. As a result, services provided by the local entity to overseas entities once again qualify as export services, allowing local firms to claim VAT refunds on their input costs.

In December 2024, Kenya passed the Tax Laws (Amendment) Act, 2024 (Act), and the Tax Procedures (Amendment) (No. 2) Act, 2024.[597] The Acts replaced the existing 1.5% DST with a Significant Economic Presence Tax (SEPT) levied at 3% of gross turnover on non-resident entities operating through digital platforms. In addition, the Act broadens the definition of "royalty" to include nearly all software-related payments, subjecting licensing, development, training, and support fees to withholding tax in a departure from international norms. Non-resident providers must also contend with new obligations, including a 20 percent withholding tax on digital marketplace payments and excise duty on services delivered through digital platforms, adding multiple layers of taxation that increase compliance costs and reduce

[596] Syekei, J. (2020, September 1). *Publication of the National information Communication and Technology Policy Guidelines, 2020*. Bowmans. https://www.bowmanslaw.com/insights/technology-media-and-telecommunications/publication-of-the-national-information-communication-and-technology-policy-guidelines-2020/.
[597] *Tax Laws (Amendment) Act* [Kenya] Act No. 12. (2024). https://new.kenyalaw.org/akn/ke/act/2024/12/eng@2024-12-13.

profitability. While the replacement of the DST is a welcome development, CCIA urges USTR to continue to press the Kenyan government to remove overlapping and burdensome taxation regimes that disproportionally penalize cross-border services providers and, at times, are inconsistent with international tax norms.

Korea

Asymmetric Platform Regulation

In July 2024, Representative Kim Nam-geun and other Assembly members introduced the Online Platform Monopoly Regulation Act, one of several bills imposing sweeping restrictions on a subset of online service providers.[598] The bill sets arbitrary thresholds (KRW 15 trillion market cap, KRW 3 trillion revenue, 10 million users) and bans self-preferencing, tie-in sales, and could mandate data sharing, raising trade secrets and concerns regarding Korea's obligations under the WTO and KORUS. While some Korean firms are covered, the burden would fall disproportionately on U.S. providers, while sparing domestic competitors and leaving many Chinese and Russian companies outside its scope. The legislation would harm Korean businesses and consumers by prohibiting common product integrations (e.g., smartphones combining multiple services) and discouraging innovation. With the inauguration of a new government in June 2025, the Korean Fair Trade Commission (KFTC) Chairman has pledged to renew the push for online platform regulation, and to expand the KFTC with a new, dedicated "Platform Bureau" to target the online platform sector.[599] Following engagement with U.S. officials, the Korean government has indicated that it will suspend these proposed measures indefinitely,[600] but declined to commit not re-introduce them in the future. CCIA urges USTR to exercise continued vigilance in case such discriminatory proposals are revived.

Meanwhile, Korea continues to pursue a related (and overlapping) "platform transaction fairness" bill, with the government casting it as a reasonable alternative to the broader DMA-style proposals under consideration in the National Assembly. The most recent version, introduced in October 2024 by the same Representative Kim Nam-geun,[601] applies to a wide

---

[598] *Online Platform Monopoly Regulation* [Korea]. (2024). https://www.kfcf.or.kr/news/trend/read.do?no=624; and *Online Platform Monopoly Regulation* [Korea]. (2024). https://www.kfcf.or.kr/news/trend/read.do?no=624.

[599] Yong-gap, K. (2025, August 14). 주병기 공정위원장 후보자 "온플법, 한미 협상 이후 방안 마련"(종합). *Yonhap Infomax*. https://news.einfomax.co.kr/news/articleView.html?idxno=4369818; Chan-woo, Y. (2025, June 5). and https://n.news.naver.com/mnews/article/214/0001428922?sid=154. ; Ji-eun, L. (2025, June 8). "공정위 인력 충원"..'경제 검찰' 온라인 플랫폼·재벌 겨누나. *Naver News*. https://n.news.naver.com/mnews/article/214/0001428922?sid=154.

[600] Min-hyung, L. (2025, August 14). FTC to suspend push to regulate US platform firms amid trade risk. *The Korea Times*. https://www.koreatimes.co.kr/business/companies/20250814/ftc-to-suspend-push-to-regulate-us-platform-firms-amid-trade-risk.

[601] Korean National Assembly. (n.d.). *온라인 플랫폼 중개거래의 공정화*. https://opinion.lawmaking.go.kr/gcom/nsmLmSts/out?sortCol=&sortOrder=&sugCd=20&endSugCd=22&sgtCls=&cptOfiOrgCd=&searchStDtNew=&searchEdDtNew=&rslRsltNmL=&rslRsltNmR=&scCptPpostCmt=&scPpsUsr=

range of intermediation services, including app stores, e-commerce platforms, and online booking platforms. As described in detail in a CCIA briefer,[602] the bill targets companies based on relatively modest coverage thresholds (₩100 billion in brokerage fees or ₩1 trillion in domestic sales or US$70 thousand/US$700 thousand)), thereby capturing many large U.S. platforms active in Korea. Obligations under the bill include mandatory use of standardized contracts, advance notice for contractual modifications, and a 10-day payment deadline, which is impractically short for services that must conduct fraud detection and other risk checks before disbursing funds. Platforms deemed to hold a "superior bargaining position" (i.e., likely targeting U.S. firms) would face additional restrictions on common commercial practices such as product integration, promotional arrangements, or bundling, backed by penalties of up to double the value of the disputed transaction. While framed as narrower than DMA-style "gatekeeper" legislation, these bills replicate many of the same *ex-ante* restrictions and discriminatory impact and would significantly limit platform flexibility and innovation.

These proposals raise serious concerns for U.S. providers. The vague and discretionary concept of "superior bargaining position" risks arbitrary or politicized enforcement, particularly given the longstanding focus of Korean regulators and legislators on U.S. firms. Imposing rigid fee caps on marketplaces undermines companies' ability to recover costs or reinvest in new services, while prescriptive contractual requirements reduce their ability to respond quickly to evolving market or security risks. By proscribing conduct that is widespread and often pro-competitive across both digital and traditional industries, these measures would chill innovation, create a two-tier regulatory framework, and place foreign firms at a structural disadvantage vis-à-vis Korean competitors not subject to the same restrictions. Such measures are inconsistent with Korea's commitments to apply transparent, non-discriminatory, and evidence-based regulation, and they risk erecting new barriers to market access for U.S. firms. The United States should urge Korea to reconsider this legislative approach and ensure that any competition-related measures are narrowly tailored, transparent, and grounded in demonstrable evidence of consumer harm.

Barriers to the Deployment and Operation of Network Infrastructure

Under the Telecommunications Business Act, overseas operators, including satellite operators, are prohibited from directly providing telecommunications services in Korea.[603] Instead, they must rely on a domestic telecommunications operator through a cross-border supply agreement, subject to approval by the Minister of Science and ICT. This requirement blocks independent market entry by foreign firms and makes access to the Korean market contingent on partnering

---

&stDtFmt=&edDtFmt=&scBlNm=scBlNm_blNm&scBlNmSct=%EC%98%A8%EB%9D%BC%EC%9D%B8+%ED%94%8C%EB%9E%AB%ED%8F%BC+%EC%A4%91%EA%B0%9C%EA%B1%B0%EB%9E%98%EC%9D%98+%EA%B3%B5%EC%A0%95%ED%99%94.

[602] CCIA. (2025, September 17). *Korean Legislative Proposals on Platform Transaction Fairness*. https://ccianet.org/library/korean-legislative-proposals-on-platform-transaction-fairness/.

[603] *TELECOMMUNICATIONS BUSINESS ACT* [Korea] Act No. 19856. (2023). https://elaw.klri.re.kr/eng_service/lawView.do?hseq=64463&lang=ENG.

with a local operator, reducing competition and creating leverage for domestic incumbents. Given the resurgence of U.S. competitiveness in the satellite sector, the United States should seek to remove this barrier.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Korean government continues to maintain a highly effective protectionist stance to keep global cloud service providers out of the local public sector market. It has accomplished this through numerous measures, including 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. Overlaying this is the National Intelligence Service's categorization of governmental entities by risk level,[604] another tool used to deny U.S. firms market access.

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 separate from those servicing commercial customers; non-recognition of Common Criteria certification of equipment (and international standard), in favor of unique national requirements; 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. The CSAP obligations have resulted in U.S. firms being effectively unable to qualify to bid on the vast majority of public sector cloud computing contracts, despite clear WTO and KORUS FTA commitments that should ensure access, and which prohibit the use of technical requirements as a means of denying market access.

On January 31, 2023, MSIT promulgated a revised version of 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 remain dominated exclusively by Korean national firms.

Burdensome requirements even at the low tier remain (e.g., with respect to encryption), but a small portion of the public sector market is now accessible to global CSPs, by allowing logical versus physical separation of data for this category. Microsoft (November 2024) and AWS (March 2025)[605] have obtained CSAP Low (Group C) certification, but no company has yet

---

[604] Korean National Cyber Security Center. (2025, January 23). *국가 망 보안체계 보안 가이드라인 (Draft)*. https://www.ncsc.go.kr/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=198744&pageI%20ndex=1&searchCnd2=#LINK

[605] Sung, S. (2025, April 2). *AWS achieves Cloud Security Assurance Program (CSAP) low-tier certification in AWS Seoul Region*. AWS. https://aws.amazon.com/blogs/security/aws-achieves-cloud-security-assurance-program-csap-low-tier-certification-in-aws-seoul-region/.

qualified for Medium or High tiers (which represent the bulk of the market). The key burden of requiring physically separate computing facilities these tiers remains.

Recent advancements in AI technology, a specialty of U.S. suppliers, are expected to offer significant benefits to the Moderate tier of the public sector. 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.

The key restrictions that remain for mid- and high-tier data include requirements to:

- physically separate facilities used for servicing the public sector from those servicing commercial customers (which was allowed for low-tier data);
- exclusively use equipment, resources, and personnel located in Korea;
- exclusively store data in Korea;
- exclusively utilize Korea's national encryption algorithms; and
- exclusively rely on NIS certification for key infrastructure.

CSAP restrictions are also beginning to bleed into other sectors: the government requires CSAP-like controls in 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 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.

As a near-term goal, USTR should encourage the Korean government to allow U.S. cloud computing companies to store and process data for the majority of cloud-based workloads of public institutions, covering, at a minimum, the central and sub-central entities covered by Korea's WTO/KORUS government procurement obligations.[606] Detailed steps Korea will need to take to ensure effective market access are described in a recent CCIA briefer.[607]

Also affecting cloud computing market access generally is Korea's implementation of its 2011 Industrial Technology Protection Act, which aims to prevent undue divulgence of industrial

[606] World Trade Organization. (n.d.). *Republic of Korea - Central Government Entities - Annex 1*. https://e-gpa.wto.org/en/GPACoverage/Annex1/54; World Trade Organization. (n.d.). *Republic of Korea - Sub-Central Government Entities - Annex 2*. https://e-gpa.wto.org/en/GPACoverage/Annex2/55.
[607] CCIA. (2025). *Korea's Barriers to U.S. Digital Service Suppliers*. https://ccianet.org/wp-content/uploads/2025/04/CCIA-South-Koreas-Barriers-to-U.S.-Digital-Service-Suppliers-and-Suggested-Commitments.pdf.

technology.[608] The act defines "industrial technology" broadly by reference to multiple statutes and empowers the government to designate "national core technology" (Art. 9) where overseas leakage would significantly harm security or economic interests, alongside comprehensive state-led policies, guidelines, and oversight. Through the Industrial Technology Protection Committee, the Act governs designation and revision of core technologies and regulates their export and foreign M&A (Arts. 11, 11-2), imposes confidentiality and reporting duties, authorizes investigations, and establishes strong criminal and administrative penalties for violations.

Based on this Act, MOTIE restricts the use of foreign cloud service providers for workloads involving national core technologies, citing concerns that U.S. CSPs could export sensitive data overseas. In practice, this restriction prevents Korean companies and research institutions from using global best-in-class cloud infrastructure for critical workloads, forcing reliance on local providers regardless of technical, security, or cost considerations. For cross-border services suppliers, this functions as a market access barrier and undermines the principle of non-discriminatory treatment under Korea's trade commitments. It also raises operational challenges for multinational firms with integrated R&D operations that need consistent infrastructure across jurisdictions. To address these concerns, Korea should ensure that U.S. cloud computing companies are exempt from any requirement for their commercial or governmental customers to obtain pre-approval for using their services in relation to national core technologies.

In February 2025, MSIT announced a National AI Initiative aimed at developing a state-of-the-art LLM and creating a National AI Computing Center, forming the backbone of Korea's national AI capabilities.[609] However, the Request for Proposal released in May 2025 for these projects introduced a restrictive "domestic companies only" clause,[610] effectively excluding U.S.-based cloud service providers from participating in a potential market estimated at ₩1.5 trillion (approximately US$1.1 billion). This exclusionary measure has raised significant concerns among U.S. stakeholders, particularly given that several U.S. CSPs had already made substantial infrastructure investments in anticipation of an open and competitive procurement process based on earlier engagements with MSIT. The abrupt introduction of such restrictive eligibility criteria, without prior consultation, undermines the principles of transparent government procurement and risks setting a harmful precedent for other AI and technology-related government initiatives. Removing the "domestic companies only" requirement would

---

[608] *ACT ON PREVENTION OF DIVULGENCE AND PROTECTION OF INDUSTRIAL TECHNOLOGY* [Korea] Act No. 10962. (2011). https://elaw.klri.re.kr/eng_service/lawView.do?hseq=24351&lang=ENG.

[609] Korea Ministry of Science and ICT. (2025, May 19). *Korea Secures 1.9 Trillion KRW in Supplementary Budget for AI Sector—Laying the Groundwork to Become a Global Top 3 AI Powerhouse*. https://www.korea.net/Government/Briefing-Room/Press-Releases/view?articleId=8025&type=O&insttCode=A110439.

[610] Korea Ministry of Science and ICT. (2025, May 26). *2025년도 「AI컴퓨팅 자원 활용 기반 강화(GPU 임차 지원)」 및 「고성능컴퓨팅 지원사업」공급사 모집 공고.* https://www.msit.go.kr/bbs/view.do?sCode=user&mId=311&mPid=121&pageIndex=1&bbsSeqNo=100&nttSeqNo=3179519&searchOpt=ALL&searchTxt=GPU.

help ensure a level playing field, uphold fair competition, and foster stronger U.S.–Korea cooperation in the rapidly evolving AI sector. As with CSAP noted above, this measure appears inconsistent with Korea's WTO and KORUS government procurement obligations, that USTR should seek to enforce.

Discriminatory Local Content Quotas and Audiovisual Service Mandates

In July 2024, Rep. Jo In-cheol introduced the Partial Amendment Bill to the Framework Act on Broadcasting and Communications Development, which would require "value-added telecommunications providers" meeting certain traffic thresholds to contribute 1% of their revenue to the Broadcasting and Communications Development Fund.[611] The fund is designed to support broadcasting communications, which, under the foundational law,[612] is defined to be used for a range of broadcast transmissions and content development. The bill would implicate a series of trade commitments Korea has made to the United States through KORUS to treat U.S. digital products (Article 15.3)[613]—such as content and programming—equally to Korean digital products, and in the WTO (Telecommunications Services Reference Paper)[614] to ensure that universal service funds are competitively neutral. Value-added telecommunications services providers from the United States are currently unable to access the fund, rendering this regime discriminatory and violative of the spirit, if not the letter, of KORUS. The current status of this bill is unclear.

Government Imposed Content Restrictions and Related Access Barriers

The Act on Promotion of Information and Communications Network Utilization and Information Protection (the Network Act) regulates how information and communications networks are used and policed. Article 44-7(5), added in January 2024, creates new compliance burdens for providers that operate domestic servers of a certain type or scale.[615] These entities must implement measures to (1) identify and restrict access to unlawful information, subject to review by the Korea Communications Standards Commission, (2) request uploaders to halt further

---

[611] In-Cheol, J. (2024, July 12). *조인철 | OTT 방발기금 무임승차 금지법 대표 발의(240712)*. Naver. https://blog.naver.com/iccho19/223510413508; *Partial Amendment to the Framework Act on Broadcasting and Communication Development* [Korea]. (2024). https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_G2H4F0G7E1M1N1L5M2K5L2J3R8S1Q7&ageFrom=22&ageTo=22.

[612] *Framework Act on Broadcasting Communications Development* [Korea]. (2015). https://elaw.klri.re.kr/eng_service/lawView.do?hseq=37358&lang=ENG.

[613] Office of the United States Trade Representative. (2012, March 15). *Free Trade Agreement between the United States of America and the Republic of Korea: Chapter 15 (Electronic Commerce)* [Text of trade agreement]. https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text.

[614] World Trade Organization. (1996, April 24). *Negotiating group on basic telecommunications.* https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm#top.

[615] *ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION* [Korea]. (2024). https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=64717&type=sogan&key=41.

distribution, (3) record and store logs of these enforcement actions, and (4) adopt any additional preventive measures mandated by Presidential Decree. For cross-border service suppliers, this provision poses significant concerns. It could indirectly pressure foreign companies to maintain local servers in Korea, functioning as a de facto data localization requirement. It also expands liability exposure by obligating providers to monitor, restrict, and document user content in ways that may conflict with global business models and international trade commitments. To mitigate these risks, USTR should urge the Korean government to shield CDNs from obligations to block content deemed illegal in Korea when such blocking has already been implemented at the ISP or hosting-provider level. This safeguard would reduce duplicative compliance costs, avoid unnecessary disruption of global CDN operations, and align enforcement with the principle of proportionality.

The Korea Communications Commission (KCC) is advancing further amendments to the Network Act to introduce new digital content censorship measures requiring mainly U.S.-based large online platforms to censor vaguely defined "false manipulated information" under threat of government investigations and substantial fines for non-compliance.[616] Modeled on the European Union's Digital Services Act, these measures would replicate its risks and negative impacts for U.S. industry and free expression.[617] Although no official draft has been released (an informal draft is attached to CCIA analysis footnoted above), the Proposed Measures would create discriminatory burdens by targeting an undefined category of "large-scale" platforms, likely capturing predominantly U.S. firms.[618] They would impose vague and onerous content regulation by obligating companies to act against content produced with "intent to mislead" for "economic or political gain," particularly around elections or matters of public opinion, thereby targeting lawful political speech and entrenching a politically motivated censorship regime. The KCC would be empowered to investigate platforms' censorship systems and impose fines of up to 4% of domestic sales for non-compliance, incentivizing over-censorship of lawful speech and discouraging innovation in content moderation. By mandating rigid, government-overseen systems, the measures would enable the Korean government to pressure platforms into removing politically inconvenient content, effectively deputizing U.S. companies to carry out state-directed censorship.[619] Further, a local agent requirement for platforms without a domestic presence,

---

[616] CCIA. (2025, October 10). *Proposed Korean Content Control Legislation*. https://ccianet.org/library/proposed-korean-content-control-legislation/.
[617] 2025 study by the CCIA Research Center found that the DSA imposes an estimated $750 million annually in direct compliance costs, in addition to their exposure to intrusive investigations and punitive fines. CCIA. (2025, July 28). *New Study Finds EU Digital Regulations Cost U.S. Companies up to $97.6 Billion Annually*. https://ccianet.org/news/2025/07/new-study-finds-eu-digital-regulations-cost-u-s-companies-up-to-97-6-billion-annually.
[618] Min-ho, J. (2025, August 20). Push to punish 'fake news' tests limits of free press in Korea. *The Korea Times*. https://www.koreatimes.co.kr/southkorea/politics/20250820/push-to-punish-fake-news-tests-limits-of-free-press-in-korea; CCIA. (2025, October 10). *Proposed Korean Content Control Legislation*. https://ccianet.org/library/proposed-korean-content-control-legislation/.
[619] United States International Trade Commission. (2022). *Foreign Censorship, Part 1: Policies and Practices Affecting U.S. Businesses*. https://www.usitc.gov/publications/332/pub5244.pdf.

combined with liability provisions, could serve as a non-tariff barrier in potential violation of Korea's obligations under the Korea–U.S. Free Trade Agreement. These measures form part of a broader pattern of discriminatory digital regulation and aggressive enforcement targeting U.S. firms in Korea,[620] and their adoption would mirror the DSA's economic and speech-related harms while undermining shared U.S.–Korea democratic values.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

MSIT has advanced numerous amendments to the 2020 Telecommunications Business Act, imposing obligations on OTT suppliers, including foreign suppliers, for network management issues outside their control, ostensibly to mitigate network congestion.[621] 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 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.

Eight proposals have been made by the Korean National Assembly to explicitly mandate "network usage fee" payments by certain content providers over the past several years. A new legislative proposal from Representative Lee Hae-Min, dubbed the "Bill on Partial Amendment to the Telecommunications Business Act"[622] and which amends the Telecommunications Business Act, was introduced on August 8. The bill prohibits value-added telecommunications service providers that meet certain user and data traffic thresholds from, among other requirements, unjustly delaying or declining to enter into a contract for the use of telecommunications networks or declining to pay a "legitimate" price for the use of telecommunications networks. This contravenes the free-market system based on voluntary negotiation that has allowed the internet to flourish—with vast benefits to online services and telecommunications providers alike—by allowing telecommunications providers to force value-added services providers to pay fees for their traffic. Proponents justify such proposals with the unsupported argument that network fees are necessary to fund the costs of extending and adding

[620] Cory, N. & Holleyman, R. (2025, June 12). *Safeguarding U.S. Companies from Unfair South Korean Competition Policies*. The National Bureau of Asian Research, https://www.nbr.org/publication/safeguarding-u-s-companies-from-unfair-south-korean-competition-policies/.
[621] Eun-jin, K. (2020, September 9). Enforcement Decree of 'Netflix Law' Feared to Hurt Korean Internet Companies. *Business Korea*. http://www.businesskorea.co.kr/news/articleView.html?idxno=51497.
[622] *Partial Amendment to the Telecommunications Business Act* [Korea]. (2024), https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_N2M4K0J7R1R8Q1Q8Z2X4V2U9V4D6C1&ageFrom=22&ageTo=22.

capacity to local broadband markets. However, in reality, such a regime would distort investment incentives and lead to discriminatory treatment of content and application providers.

Such proposals can be traced to years of conflict between U.S. content providers operating in the region and local telecommunication providers,[623] culminating in legislation introduced in 2022 by Rep. Young-chan Yoon, called the "Netflix Free Ride Prevention Act."[624] The legislation would effectively mandate foreign content access providers—namely U.S. firms such as Google, Meta, and Netflix—to enter into paid contracts with internet service providers for the content demanded by ISPs' customers. The bill would directly undermine long-standing global norms and procedures that serve as the foundation of the internet ecosystem[625] and would likely violate Korea's trade obligations to the United States[626] by targeting U.S. content providers and requiring contracts and extractive fees for any company meeting arbitrary data transfer thresholds. In addition, the bill would have a detrimental impact on the domestic content industry by increasing the cost for users to access content and inhibiting the overseas expansion of K-content. 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 (Access to and Use of the Internet for E-Commerce).[627]

Korea's existing Sending Party Network Pays model, adopted in 2016 and applicable to ISPs operating in Korea, demonstrates that these concerns are not merely speculative. Multiple studies have found that Korea's SPNP model has led to higher transit prices, higher latency, and high regulatory costs. Industry observers expect new proposals in the next regular session of the National Assembly. South Korea is one of a handful of markets where "paid peering" is the norm due to this regulatory intervention, acting as a significant trade barrier. The 2016 "Sending Party Network Pays" requirement mandated interconnection fees between the three main South Korean ISPs,[628] which effectively led them to abandon the global norm of settlement-free peering as they no longer needed to compete to cooperate with U.S. Cloud Service Providers. As a result, US

[623] Coldewey, D. (2021, June 28). Korean court sides against Netflix, opening door for streaming bandwidth free from ISPs. *TechCrunch*. https://techcrunch.com/2021/06/28/korean-court-sides-against-netflix-opening-door-for-streaming-bandwidth-fees-from-isps/.
[624] Young-chan, Y. (2022, September 8). *Representative Yoon Young-chan, Lead Proposer of "Netflix Free Riding Prevention Act."* Naver. https://blog.naver.com/yyc8361/222870020115.
[625] Frautschy, D. & Gahnberg, C. (2022, May 25). *Old Rules in New Regulations - Why "Sender Pays" Is a Direct Threat to the Internet*. Internet Society. https://www.internetsociety.org/blog/2022/05/old-rules-in-new-regulations-why-sender-pays-is-a-direct-threat-to-the-internet/.
[626] McHale, J. (2022, September 19). *New Korean legislation undermines Internet norms and raises broad trade concerns*. Disruptive Competition Project. https://www.project-disco.org/21st-century-trade/091922-new-korean-legislation-undermines-internet-norms-and-raises-broad-trade-concerns/.
[627] CCIA. (2022). *Proposal to Mandate Payments by Content and Application Providers (CAPs) Undermines the Future of U.S.-Korea Trade*. https://ccianet.org/wp-content/uploads/2022/09/CCIA-Trade-Analysis-of-Korean-Network-Usage-Fee-Proposals.pdf.
[628] Gahnberg, C., de Guzman, N., Robachevsky, A. & Wan, A. (2022, May 11). *Internet Impact Brief: South Korea's Interconnection Rules*. Internet Society. https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-south-koreas-interconnection-rules/.

companies experiences wholesale bandwidth costs in South Korea that are nearly 30 times the cost of Internet transit in the United States. The high fees demanded by large South Korean ISPs affect the ability of U.S. content providers to serve traffic efficiently, and this network peering overregulation has resulted in major U.S. technology companies reducing or pulling out of the South Korean market.[629]

With respect to extending network usage fees directly to content and applications service suppliers, USTR noted that "such a mandate could be anticompetitive by further strengthening Korea's ISP oligopoly of three major providers to the detriment of the content industry"[630] CCIA appreciates the engagement of USTR and the Department of Commerce on this issue in the past and encourages continued vigilance.

Potential Challenges to the Development of AI

South Korea's AI Basic Act, signed into law on January 21, 2025, and set to take effect in January 2026, establishes a broad regulatory framework for artificial intelligence.[631] Obligations created by this law include requirements relating to transparency, risk assessment, disclosure of mitigation measures, and compliance with fact-finding investigations. However, the law does not clearly distinguish between the various categories of AI entities – such as developers, deployers, and users of AI systems – or their respective obligations and responsibilities, resulting in significant uncertainty and risk particularly to large AI developers who are disproportionately U.S.-based and who could be held liable for downstream uses they cannot control. For cross-border service suppliers, the law poses several major concerns.[632] First, it introduces unsupported compute-based thresholds, rather than capability-based risk assessments, to designate "high-impact" and "high-performance" AI. This risks targeting U.S. firms disproportionately and may conflict with WTO and KORUS commitments. Second, it requires public disclosures and labelling of certain AI outputs and training criteria, which could compromise commercially sensitive information and trade secrets. While intended to promote safety and accountability, these provisions create compliance uncertainty and could duplicate existing industry best practices, such as watermarking standards already widely adopted. Third, it mandates that some foreign providers designate a domestic agent liable for violations, which could function as a disguised local presence mandate, contravening KORUS Article 12.5. Finally, the low threshold

---

[629] Yoon, J. (2023, December 6). Twitch Will Shut Down Its Streaming Platform in South Korea. *The New York Times*. https://www.nytimes.com/2023/12/06/business/media/twitch-korea-shut-down.html.

[630] Office of the U.S. Trade Representative. (2024). *2024 National Trade Estimate Report on Foreign Trade Barriers*. https://ustr.gov/sites/default/files/2024%20NTE%20Report_1.pdf.

[631] *인공지능 발전과 신뢰 기반 조성 등에 관한 기본법안(대안)(과학기술정보방송통신위원장)* [Korea]. (2025). https://likms.assembly.go.kr/bill/bi/billDetailPage.do?billId=PRC_R2V4H1W1T2K5M1O6E4Q9T0V7Q9S0U0&currMenuNo=2600044.

[632] CCIA. (2025). *CCIA Comments on South Korea's AI Law*. https://ccianet.org/wp-content/uploads/2025/03/CCIA-Korea-AI-Act-Explainer.pdf.

for intrusive fact-finding investigations exposes foreign providers to unpredictable enforcement risks. Korea's Basic AI Act risks hindering market access, imposing disproportionate compliance costs, and raising trade law concerns for U.S. and other international AI suppliers.

Restrictions on Cross Border Data Flows

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. Since September 15, 2023, these obligations have been unified across both online and offline service providers, though less stringent requirements still 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.[633]

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 two 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 recommended them to comply with such standards.

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.[634] Beginning March 13, 2025, these reforms introduced the right to data portability. The

[633] Office of the U.S. Trade Representative. (2022). *2022 National Trade Estimate Report on Foreign Trade Barriers.* https://ustr.gov/sites/default/files/2022%20National%20Trade%20Estimate%20Report%20on%20Foreign%20Trade%20Barriers.pdf.

[634] IAPP. (2023, September 6). *South Korea approves PIPA enforcement amendments*. https://iapp.org/news/b/south-korea-cabinet-approves-enforcement-amendments-to-pipa.

amendments also expanded PIPC's penalty powers by allowing fines of up to 3% of a company's global 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.

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 core 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. As of September 2025, applications from Google and Apple remain pending. The deadline for a decision has passed, and there is no indications that Korea is willing to meaningfully liberalize its restrictions, suggesting that protecting its domestic suppliers from foreign competition remains its overriding priority.

Threats to the Security of Devices and Services

In late 2022, in response to a fire at a major data center, the National Assembly passed the amendments to the Broadcasting Communications Development Act, the Telecommunications Business Act, 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.

Other Barriers to Digital Trade

In August 2021, the Korean National Assembly passed legislation that requires mobile application marketplaces to permit users to make in-application purchases through payment mechanisms not controlled by the marketplace itself. The law did not ban app store distribution models, but rather prohibited app stores from forcing developers to use the store's in-app billing system exclusively. Further, policymakers supportive of the bill have made clear their intent to single out specific U.S. companies with the new law.[635] 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, which prohibits a government from treating one set of service suppliers less favorably than competing local or third-country suppliers. Since many services mandate a specific payment mechanism to complete a transaction, banning this practice solely for app stores raises fundamental questions of fairness.

The rules for this legislation were approved by the Korea Communications Commission on March 8, 2022.[636] The agency announced on August 16, 2022, that it was investigating Google, Apple, and SK Group's OneStore over potential violations regarding in-app payments, with a specific warning to Google and Apple: "In addition, the KCC determined that if Google or Apple imposes discriminatory conditions on the payment method (third-party payment) provided by the app developer in an internal payment, or makes the usage process inconvenient, that act may constitute an act of forcing a specific payment method (own company payment)."[637] In October 2023, the KCC proposed a fine of ₩68 billion (approximately US$52 million) on two U.S. companies for allegedly violating these regulations.[638] Both firms contested both the proposed fines and assertion of violation, and the issue remains unresolved.[639]

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

---

[635] *Reason for Proposal and Main Contents, New regulations on prohibited acts of app market operators, etc.* [Korea] Agenda No. 2102524. (2020). https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_B2C0H0N7Z3O0I1Y5X3Q0Z3Y1D1U2L3.

[636] *Enforcement Decree* [Korea]. (2022). https://www.kcc.go.kr/user.do?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=4&boardSeq=52916

[637] Korea Communications Commission. (2022, August 16). *KCC begins fact-finding investigation of three app market operators.* https://www.kcc.go.kr/user.do?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=1&boardSeq=53609.

[638] Korea Communications Commission. (2023). *Press Release.* https://kcc.go.kr/user.do?boardId=1113&page=A05030000&dc=K00000200&boardSeq=57613&mode=view.

[639] Hyun-woo, N. (2024, October 4). Assembly to grill Apple, Google execs over in-app purchase fees. *The Korea Times*. https://www.koreatimes.co.kr/www/tech/2024/10/129_383576.html.

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.

On February 14, 2025, amendments to Korea's 2018 Electronic Commerce Act (E-Commerce Act) were passed. Although motivated by a legitimate interest in addressing consumer complaints relating to imported physical goods, particularly from China, one particular provision is problematic, as described in detail in a CCIA briefer:[640] the requirement (Article 20-4) for local agents present in Korea to resolve disputes and the mandatory assignment of such functions to any subsidiary if present in Korea. This requirement is likely inconsistent with Korea's trade commitments under KORUS. Designating a local agent for information exchange would be consistent with FTA local presence rules (*e.g.*, Article 12.5 of KORUS). However, requiring the agent to fully resolve such disputes and assigning such functions to any existing local subsidiary would be tantamount to requiring establishment, and hiring related personnel, that the trade rules are designed to prevent, in cases a supplier prefers to offer a specific service fully on a cross-border basis. The burden this proposal would place on firms offering digital products and services (apps, videos, cloud computing), as opposed to physical products, is noteworthy: such suppliers typically operate global platforms staffed from various locations specializing in specific functions such as payments, technical support, dispute resolution, etc. While most large U.S. digital firms maintain a local presence in Korea, the personnel there may have no expertise or responsibility for complaint dispute resolution, and saddling such an entity with such functions is neither appropriate nor effective. USTR should work to ensure that, at a minimum, suppliers engaged in wholly digital trade are not subject to these onerous requirements.

Korea's longstanding use of aggressive regulatory enforcement tactics, has created a challenging and unpredictable operating environment for digital service providers—and often appear to disproportionately target U.S. firms.[641] In recent years, the KFTC has emerged as a key actor through which these objectives are pursued, often employing dawn raids and other unannounced on-site inspections, expansive investigations, and threats of criminal prosecution[642] for practices that are not treated as criminal offenses in other jurisdictions. This excessive and unpredictable application of regulatory powers creates significant legal uncertainty,[643] deters investment, and raises the cost of doing business in Korea's digital economy. Although KORUS provides due

[640] CCIA. (2024, September 24). *Comments on Korea's Proposed Amendments to the Electronic Commerce Act*. https://ccianet.org/library/comments-on-koreas-proposed-amendments-to-the-electronic-commerce-act/.
[641] Corey, N. & Holleyman, R. (2025, June 12). *Safeguarding U.S. Companies from Unfair South Korean Competition Policies*. NBER. https://www.nbr.org/publication/safeguarding-u-s-companies-from-unfair-south-korean-competition-policies/.
[642] Kim, H. E. (2012). *Developments in Criminal Enforcement of Competition Law in Korea*. Competition Policy International Inc. https://www.competitionpolicyinternational.com/assets/Uploads/Asia1-22-2013-2.pdf.
[643] Lee, S. (2024, October 30). *Duplicate powers in the criminal referral process and the overlapping enforcement of the competition and criminal authorities in Korea: An analysis through the lens of the redundancy theory*. ASCOLA Asia Annual Regional Workshop 2024. https://ssrn.com/abstract=5004296.

process protections for U.S. firms, Korea's adherence to these standards has been spotty and engendered at least one case of pushback form the Unites States.[644] These practices have broader implications for cross-border digital trade by undermining the regulatory predictability and transparency necessary for foreign firms to compete on a level playing field.

Malaysia

Barriers to the Deployment and Operation of Network Infrastructure

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.[645] The exemption is key in reducing the time required to conduct submarine cable repairs. 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.[646] The revocation was justified by the government as both a means to protect the domestic shipping industry from foreign competition and as a measure to safeguard national security. In May 2022, Malaysia's transport minister Wee Ka Siong said the revocation would remain, and that the requirement for foreign vessels to obtain a Domestic Shipping License is "not a hindrance" to submarine cable projects.[647] While the government reinstated the cabotage exception on June 2, 2024,[648] the situation remains uncertain given the billions of dollars of investment in crucial telecommunications infrastructure being dependent on an exemption that can so easily be rescinded once more upon another government change. Industry would benefit from a permanent revocation of the cabotage policy, or a permanent exemption enshrined in legislation.

---

[644] Palmer, D. (2019, July 7). USTR says Korea competition-related concerns still not resolved. *POLITICO*. https://subscriber.politicopro.com/article/2019/07/ustr-says-korea-competition-related-concerns-still-not-resolved-1574166.

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

[646] Kohlstedt, K. (2017, June 30). *Inside the Cables Carrying 99% of Transoceanic Data Traffic*. 99% INVISIBLE https://99percentinvisible.org/article/underwater-cloud-inside-cables-carrying-99-international-data-traffic/.

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

[648] Wong, A. (2024, June 2). Malaysia finally reinstates cabotage exemption for undersea cable repair ships. *SYOA CINCAU*. https://soyacincau.com/2024/06/02/malaysia-reinstates-undersea-cable-repair-vessel-cabotage-exemption/.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The State of Selangor announced in October 2025 that they will impose a 30% target local content requirement for data centers located in the State of Selangor, which is a key hub for US cloud service providers' data centers.[649] Components in scope are servers, memory, storage, and networking. An enforcement mechanism has not been spelled out, but could be linked to the range of approvals under Selangor's jurisdiction such as land use permits and water access. The federal government and the State of Johor, which is also a data center hub, are reported to be looking to draft similar requirements.

In October 2025, Malaysia's National AI Office (NAIO) unveiled its Sovereign AI Strategy,[650] introducing a tiered approach to AI governance with far-reaching implications for international technology providers. The strategy sets strict requirements for compute infrastructure, data residency, and operational flows, particularly for top-tier (L3) sensitive government workloads.[651] It notably proposes the development of government-owned cloud and compute capabilities for these high-sensitivity workloads and establishes new sovereignty certification requirements, even when engaging with global technology providers. Although NAIO has emphasized an "ecosystem-supportive" posture open to both foreign and local providers, the structure of the policy raises concerns about potential market access barriers and preferential treatment for domestic firms. The introduction of mandatory requirements for handling sensitive government data, combined with new certification and auditability obligations, is expected to increase operational complexity and compliance costs for U.S. companies operating in Malaysia. This evolving regulatory landscape warrants close monitoring, as its implementation could set precedents that significantly affect the ability of international technology firms to participate in Malaysia's growing AI ecosystem. The recent U.S.-Malaysia Reciprocal Trade Agreement (Oct. 2025)[652] directly addresses these concerns. The agreement explicitly prohibits Malaysia discriminating against U.S digital services (Article 3.2.(a)); or from imposing conditions that require U.S. firms to 'purchase, utilize, or accord a preference to a particular technology' (Article 3.4(1)) and commits Malaysia to ensuring cross-border data transfers for business conduct (Article 3.2(b)).

---

[649] Han, N. S. (2025, July 18). *As part of our ongoing efforts to develop a forward-looking and inclusive local content provision for Selangor's data centre* [Facebook Post]. Facebook. https://www.facebook.com/NgSzeHan.dap/posts/as-part-of-our-ongoing-efforts-to-develop-a-forward-looking-and-inclusive-local-/1277778900371030/.

[650] Malaysia Ministry of Digital. (2025, October 11). *Allocations In Belanjawan Madani 2026 Set To Spur Malaysia's Digital Transformation*. https://www.digital.gov.my/en-GB/siaran/Peruntukan-Dalam-Belanjawan-Madani-2026-Akan-Merangsang-Transformasi-Digital-Malaysia.

[651] Digital Policy Alert. (2025, August 13). *Malaysia: Ministry of Digital launched National Cloud Computing Policy*. https://digitalpolicyalert.org/event/32665-ministry-of-digital-launched-national-cloud-computing-policy.

[652] The White House. (2025, October 26). *Agreement Between the United States of America and Malaysia on Reciprocal Trade*. https://www.whitehouse.gov/briefings-statements/2025/10/agreement-between-the-united-states-of-america-and-malaysia-on-recipricol-trade/

Forced Revenue Transfers for Digital News

The Malaysian Communications and Multimedia Commission (MCMC) announced on September 5, 2023 its intent to move forward with a news remuneration proposal.[653] To date, no text has been released. The MCMC announcement suggested an interest in extraction and redistribution of revenues similar to that of Canada, Australia, and Indonesia. 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 between digital platforms and local media to ensure fair compensation for news content creators."[654] Recent initiatives by the Malaysian government appear to suggest that it is moving away from direct intervention in media sustainability. These include the establishment of the Malaysia Media Council (MMC) to promote self-regulation within the industry and which does not have any mandate to require financial contributions from platforms,[655] and a RM 30M (US$7.1 million) media sustainability fund to help media organizations with their digital transformation and adaptation to the evolving media landscape.[656] This legislation warrants careful monitoring, both due to Malaysia's market size and the broad goals of the proposal. These goals include sweeping issues with deep impacts on internet policy, such as addressing the impact of AI and "fair competition, strengthen intellectual property rights, protecting consumers from online harms and privacy," as the government release states.[657]

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Malaysia is navigating a period of regulatory uncertainty in its digital ecosystem for content restrictions, exemplified by new measures like the social media licensing regime implemented on January 1, 2025 under the Communications and Multimedia Act 1998,[658] and the Online Safety Act 2025.[659] These initiatives, while framed around improving online safety, raise significant concerns regarding their potential to curb freedom of expression and impose disproportionate liability on digital platforms. Specifically, any framework that grants authorities excessive content removal power or relies on vague definitions directly threatens free speech and the open

---

[653] MCMC. (2023). *MCMC CONSIDERS REGULATORY FRAMEWORK TO ADDRESS ONLINE HARM AND IMBALANCE MEDIA*. https://www.mcmc.gov.my/skmmgovmy/media/General/PressRelease/MS_MCMC-CONSIDERS-REGULATORY-FRAMEWORK-TO-ADDRESS-ONLINE-HARM-AND-IMBALANCE-MEDIA-ADEX.pdf.
[654] *Ibid*.
[655] Scoop. (2025, July 15). *MMC empowers media to govern without involving government: Fahmi*. https://www.scoop.my/news/264282/mmc-empowers-media-to-govern-without-involving-government-fahmi/.
[656] *Bernama*. (2025, June 14). RM30 Million to Drive Media Organisations' Digital Transformation. https://www.bernama.com/en/news.php?id=2434093.
[657] MCMC. (2023). *MCMC CONSIDERS REGULATORY FRAMEWORK TO ADDRESS ONLINE HARM AND IMBALANCE MEDIA*. https://www.mcmc.gov.my/skmmgovmy/media/General/PressRelease/MS_MCMC-CONSIDERS-REGULATORY-FRAMEWORK-TO-ADDRESS-ONLINE-HARM-AND-IMBALANCE-MEDIA-ADEX.pdf.
[658] *Communications and Multimedia Act* [Malaysia]. (1998). https://www.mcmc.gov.my/en/legal/acts.
[659] *Online Safety Act* [Malaysia] Act 866. (2025). https://www.mcmc.gov.my/en/legal/acts.

digital economy. For major U.S. platforms (such as social media and internet messaging services with over eight million users), these changes not only increase compliance costs and necessitate operational adjustments but also risk forcing a precautionary approach to moderation that potentially leads to the over-removal of lawful content to avoid the severe penalties associated with non-compliance. Therefore, it is critical for the U.S. government to urge the Malaysian government to ensure its overall content moderation framework strictly adheres to international principles of necessity and proportionality, and to engage in open and meaningful consultation with industry and civil society to protect fundamental rights.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

The MCMC crafted rules that subject data centers and cloud service providers to licensing obligations under the Communications and Multimedia Act 1998 (CMA 1998).[660] Traditionally, and pursuant to global best practices, requirements in question 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 comply with the provisions of the Communications and Multimedia Act 1998, including requirements on 1) data access and disclosure requests; 2) the interception of communications subject to the discretion of the Communications and Multimedia Minister; 3) mandatory standards periodically set by MCMC; and 4) make mandatory payments to the Universal Service Provision Fund (USPF). These new rules went into effect on January 1, 2022.[661] While the Malaysian government has publicly stated, in the context of recent negotiations between the U.S. and Malaysia on reciprocal tariffs, that it will abolish the requirement for social media platforms and cloud service providers from the U.S. to make payments to the USPF,[662] this has yet to be formally implemented.

On August 1, 2024, the MCMC adopted the Framework for Internet Safety under the Communications and Multimedia Act, extending new and burdensome obligations to social media and cloud service providers.[663] As of January 1, 2025, social media platforms with more than 8 million users in Malaysia are required to register with the government, apply for a license, and comply with a wide range of obligations, including handing over user data upon request without a warrant, removing content at the government's direction, and contributing 6% of their revenue to the USPF. Of the eight companies subject to this, all are foreign. These measures

---

[660] MCMC. (2021, December 17). *FREQUENTLY ASKED QUESTIONS (FAQ) ON LICENSING CLOUD SERVICE PROVIDERS*. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/FAQ-Regulating-Cloud-Service.pdf.
[661] Baker McKenzie. (2021, November 8). *Malaysia: Cloud Services to Be Licensed From 1 January 2022*. https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/malaysia-cloud-services-to-be-licensed-from-1-january-2022.
[662] Parliament of Malaysia, Dewan Rakyat. (2025, August 4). *Hansard of the Second Meeting, Fourth Term, Fifteenth Parliament of the Dewan Rakyat* (Vol. …, p. 43). https://www.parlimen.gov.my/files/hindex/pdf/DR-04082025.pdf#page=43.
[663] MCMC. (2024, July 27). *New Regulatory Framework for a Safer Internet for Children and Families.* https://www.mcmc.gov.my/skmmgovmy/media/General/PressRelease/MS_NEW-REGULATORY-FRAMEWORK-FOR-A-SAFER-INTERNET-FOR-CHILDREN-AND-FAMILIES.pdf.

significantly expand state control over digital services and introduce discriminatory costs that favor domestic telecom operators. In August 2025, Malaysia's Investment, Trade and Industry Minister announced in Parliament a decision to abolish the 6% revenue contribution requirement as part of trade concessions to the United States.[664] This ministerial announcement was formalized by the U.S.-Malaysia Reciprocal Trade Agreement, signed October 26, 2025. Article 3.1 of the agreement commits Malaysia to not imposing 'digital services taxes, or similar taxes, that discriminate against U.S. companies in law or in fact,' directly addressing the discriminatory 6% USPF revenue contribution. While the international commitment is now secured, the change must still be implemented through formal legislation by the MCMC. Additionally, while the revenue obligation may be lifted, the MCMC remains unlikely to remove its broader licensing requirement, and there is a persistent risk that the Communications Minister could forcibly deem foreign companies as licensees by law. This would expose them to onerous data disclosure and content removal obligations under the Online Safety Act (ONSA), which was gazetted in June 2025. The MCMC has stated its intention to implement regulations under ONSA by Q1 2026 but has yet to publish a draft of the specific obligations or commit to formal consultations, despite sustained pressure from industry stakeholders.

Potential Challenges to the Development of AI

Malaysia is looking to develop a law-based AI framework, with the Digital Minister confirming that an AI bill is being drafted aiming to balance security with investor confidence. However, a concerning "AI Sovereignty" narrative is gaining traction, with advocates pushing for government AI to use exclusively local models and data. This trend was amplified by the launch of the homegrown ILMU model in August 2025[665] and the Prime Minister's announcement of a "sovereign AI cloud" in the 2026 Budget,[666] posing a significant risk that Malaysia's public sector could be restricted from leveraging global AI models. The U.S.-Malaysia Reciprocal Trade Agreement provides new tools to counter this narrative: Article 3.2(a), which bars Malaysia from discriminating against U.S. digital services or U.S. products distributed digitally, and Article 3.4(1), which explicitly bars Malaysia from imposing conditions that require U.S. firms to 'purchase, utilize, or accord a preference to a particular technology' as a condition for doing business.

---

[664] Zalani, A. (2025, August 4). Tengku Zafrul: Malaysia makes trade concessions to US to keep exports flowing, protect 100,000 jobs. *Malay Mail*. https://www.malaymail.com/news/malaysia/2025/08/04/tengku-zafrul-malaysia-makes-trade-concessions-to-us-to-keep-exports-flowing-protect-100000-jobs/186397

[665] *Malay Mail*. (2025, August 12). PM Anwar launches ILMU, Malaysia's first home-grown multimodal AI. https://www.malaymail.com/news/malaysia/2025/08/12/pm-anwar-launches-ilmu-malaysias-first-home-grown-multimodal-ai/187359

[666] Malaysia Ministry of Digital. (2025, October 11). *Allocations In Belanjawan Madani 2026 Set To Spur Malaysia's Digital Transformation*. https://www.digital.gov.my/en-GB/siaran/Peruntukan-Dalam-Belanjawan-Madani-2026-Akan-Merangsang-Transformasi-Digital-Malaysia

Threats to the Security of Devices and Services

Recent amendments to the CMA,[667] passed with minimal consultation, grant law enforcement enhanced powers for data access and interception, which create significant operational and compliance risks for global service providers. The new provisions allow law enforcement authorities to compel the warrantless disclosure of broadly defined "communications data", potentially placing U.S. companies in a position of legal conflict: compliance with this mandate to avoid penalties up to RM 1 million (US$236,000) and/or up to five years in prison could necessitate a breach of strict U.S. legal requirements that limit such disclosures. Furthermore, the amendments empower law enforcement officers to enter any premises without a warrant to install interception devices which would be a red-line critical security risk for U.S. service providers, as it jeopardizes the integrity and security of communications networks; interference with this entry carries potential severe penalties of RM1 million (approx. US$236,000) and/or up to 10 years imprisonment. Given these concerns, the U.S. government should insist that Malaysia use the U.S.-Malaysia Mutual Legal Assistance Treaty as the sole and standard legal mechanism for requesting data from U.S.-based service providers, and concurrently seek the repeal of the intrusive power that permits warrantless entry for interception as it poses a direct threat to service integrity and security.

Malta

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Industry reports that Malta's Gaming Authority (the MGA) enforces data mirroring requirements on gaming providers to mirror what they broadly define as essential or regulatory data, which includes player details, financial transactions and player activity, on a live replication server in Malta when their primary servers are located abroad. The MGA argues these requirements are necessary to access real-time information for audits, regulatory supervision, and compliance checks. These obligations apply to all licensees, regardless of nationality. Companies are obligated to disclose detailed documentation regarding server locations, data replication processes, and data transmission processes. The data replicated in-country must be accessible to the MGA at all times, making it costly for non-EU companies to adhere to the rules. Additionally, operators using U.S. cloud services must demonstrate that essential data held abroad is mirrored in Malta, which adds another layer of operational complexity for U.S. companies. The rules undermine the cross-border flow of data, add high compliance costs for companies, and undermine user security.

[667] *Communications and Multimedia (Amendment) Act* [Malaysia]. (2025). https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/A1743-BI-COMMUNICATIONS-AND-MULTIMEDIA-AMENDMENT-ACT-2025-1.pdf.

Mexico

Customs-Related Restrictions and Import Barriers for Goods

U.S. exporters report sustained challenges at the U.S.-Mexico border, as industry notes that the Mexican government has still not fully implemented its USMCA customs facilitation commitments and has introduced 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 abruptly made to tariff levels. These issues have further lengthened the wait times for crossing the border. Separately, the United States should engage with counterparts in Mexico to fully implement Mexico's commitments in the USMCA Custom Administration and Trade Facilitation Chapter—such as provisions related to expediting the release of goods, improving transparency in customs procedures, facilitating communication with traders, allowing the use of information technology, and adopting and maintaining a single window—which would address these concerns.

In an August 2023 presidential decree, Mexico imposed temporary 5-25% tariff rate increases on a variety of imports that include metals, textiles, chemicals, oil, soap, paper, electronics, and furniture.[668] The government imposed this increase without providing public notice or allowing stakeholders the opportunity to comment on the proposal. The decree also suspended prior plans to reduce tariff rates. Industry reports that the tariff rate changes have raised the cost of importing into Mexico without adequate adjustment time for importers. The decree set a general expiration date of July 31, 2025, with some exceptions. The decree was expanded to additional goods with tariff hikes for 5-50% as of April 23, 2024, and will remain in place until April 23, 2026.[669]

A proposal to amend Mexico's Customs Law would significantly alter the country's customs duty structure by eliminating the simplified tariff classification system for Low-Value Shipments under US$2,500, previously known as "T1".[670] Under the proposed system, the Secretariat of Finance would replace the flat duty rates (tasa global) with variable rates, which would likely increase duties on shipments valued between US$50 and US$2,500 beyond the current 17–19 percent rates, unless an exemption for USMCA partners is introduced. This change would raise

---

[668] Vejar, C. et. Al. (2023, August 21). *Mexico Imposes Temporary Import Duties*. White & Case. https://www.whitecase.com/insight-alert/mexico-imposes-temporary-import-duties-25-more-588-non-fta-tariff-items.

[669] Vejar, C. et. Al. (2024, April 25). *Mexico reinstates tariff hikes ranging from 5% to 50% on over 544 goods*. White & Case. https://www.whitecase.com/insight-alert/mexico-imposes-temporary-import-duties-25-more-588-non-fta-tariff-items.

[670] Loaeaza, J. M. et al. (2025, September 12). *Reforma a Ley Aduanera y Ley de los Impuestos Generales de Importación y Exportación en México*. Holland & Knight. https://www.hklaw.com/es/insights/publications/2025/09/reforma-a-ley-aduanera-y-ley-de-los-impuestos-generales.

operational complexity, increase the risk of tariff misclassification, and subject U.S. e-commerce shipments to heightened regulatory scrutiny. The proposal represents a shift away from a predictable and simplified customs regime, increasing compliance costs and potentially undermining Mexico's commitments to digital trade facilitation under the USMCA.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

On January 28, 2021, new regulations by the Central Bank and the National Banking and Securities Commission came into force, mandating electronic payment companies using third-party cloud providers for data storage to implement backup options.[671] Such options risk incentivizing data localization or reliance on untrusted third vendors and could violate the USMCA's financial services provision prohibiting data localization. It could also lead to U.S. cloud services being disadvantaged in the region compared to local data center firms.

Article 50 of the 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 be subject to a different jurisdiction or risk profile than the first provider, or the IFPE must maintain its own infrastructure. A similar requirement is being imposed on financial service providers that 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 incentivizing or pressuring financial service providers to maintain data locally through approval requirements.

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.

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 (including from the U.S. Congress[672]) that these obligations on cloud services providers and electronic payment fund institutions could hinder U.S. competitiveness in the Mexican market.[673] CCIA urges USTR to continue to press Mexico to remove these requirements, as they serve as a *de facto* requirement for U.S. companies

[671] Baker & McKenzie. (n.d.). *Cloud Compliance Center: Mexico*. https://resourcehub.bakermckenzie.com/en/resources/cloud-compliance-center/na/mexico.
[672] Hurd, W., & Cuellar, H. (2020). *Letter to Robert E. Lighthizer and Steven T. Mnuchin.* https://ustoa.com/r/ustoa-filemanager/source/resources/lighthizer-digital-trades-letter.pdf.
[673] Office of the United States Trade Representative. (2023, January 25). *Readout of Ambassador Jayme White's meeting with Mexico's Under Secretary of Economy Alejandro Encinas*. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/january/readout-ambassador-jayme-whites-meeting-mexicos-under-secretary-economy-alejandro-encinas.

operating in the market to partner with local suppliers or foreign providers such as Huawei, a major investor in cloud services in Mexico.

Government-Imposed Content Restrictions and Related Access Barriers

Mexico made reforms to its Federal Copyright Law in 2020 in an attempt 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 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.

Taxation of Digital Products and Services

On September 8, 2020, the Secretary of Finance & Public Credit, Arturo Herrera, presented to the Mexican Congress a legislative proposal including "kill switch" (e.g., web blocking) for use against non-resident entities that do not pay VAT on digital services consumed by Mexicans. The measure was approved by Congress in October 2020 and published in the Diario Oficial on December 8, 2020.[674] The regulation empowers tax authorities to work with the telecom regulator to block non-resident internet platforms, preventing them from reaching Mexican users. The vast majority of U.S. internet companies have registered and have been complying with these fiscal obligations and there is no indication to date that this enforcement tool has been used. If used, this measure would raise questions with respect to USMCA compliance.

Additionally, industry reports that 2020 legislation mandates that U.S. businesses that store products 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 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 a local Mexican legal representative, who is jointly and severally liable for the firm's tax obligations, to obtain an RFC, while also being subject to VAT obligations on non-resident digital service providers. Income tax (ISR) withholding applies to sellers who are individuals using platforms, not automatically to the foreign platform's own gross revenue absent a permanent establishment. Firms are subjected to an arduous and bureaucratic

[674] *LEY DEL IMPUESTO SOBRE LA RENTA* [Mexico]. (2020). https://www.diputados.gob.mx/LeyesBiblio/ref/cff/CFF_ref57_08dic20.pdf.

registration process that includes apostilling documentation in the United States, using a certified translator to produce all documentation in Spanish, having a Mexican Notary legalize documentation, waiting anywhere from one to four months for an SAT appointment, and registering the RFC in SAT's offices. While the SAT announcement in October 2024 simplified RFC and e.firma processes, including expanded remote and streamlined options, firms still face significant administrative hurdles. These steps can take over five months and impose costs of over US$5,000, not including the costs of complying with other income tax obligations.

In September 2025, a new proposal included in Mexico's Economic Package would significantly expand this enforcement regime by requiring digital service providers to grant SAT permanent, real-time online access to their systems and records related to operations in Mexico.[675] Failure to comply could result in the temporary blocking of digital services, reinforcing the existing "kill-switch" mechanism under the Value-Added Tax Law. Under this proposal, SAT would coordinate with the newly created National Agency for Digital Transformation and Telecommunications to manage the infrastructure and data analysis supporting these obligations. While Mexican authorities have stated that the measure is intended to address tax compliance by Chinese e-commerce companies, its broad language captures all digital service providers, including U.S. firms. This proposal raises serious concerns regarding Mexico's USMCA commitments, including those on nondiscriminatory treatment, cross-border data flows, and digital trade facilitation.

USTR should press the Government of Mexico to simplify the bureaucratic requirements (e.g., local legal representative and apostilled documentation) for foreign SMEs seeking an RFC, which currently acts as a market entry barrier, and to seek assurances that the "kill switch" mechanism will not be activated, as its use would raise immediate USMCA compliance concerns.

Other Barriers to Digital Trade

Mexican policymakers continue to impose regulatory and procedural obstacles for companies pursuing connection to the electricity grid and clean and reliable energy for purchase. These obstacles include new laws and dispatch rules that prioritize CFE's generation over private suppliers, and procedural hurdles in grid connection processes overseen by CENACE (including permitting, grid access, and infrastructure conditions). The government, on the other hand, continues to limit or constrain private and off-grid energy sourcing in certain sectors and circumstances. U.S. companies are therefore unable to sufficiently locate their energy needs in

[675] Rueda, R. (2025, September 9). *Análisis: Paquete Económico para el Ejercicio Fiscal 2026 en México*. Holland & Knight. https://www.hklaw.com/en/insights/publications/2025/09/analisis-paquete-economico-para-el-ejercicio-fiscal-2026-en-mexico.

Mexico, which compromises their clean energy targets. Industry appreciates the United States seeking dispute settlement consultations with Mexico under the USMCA over the matter.

In August 2024, the Constitutional Commission of the Mexican Chamber of Deputies approved a proposal to amend the constitution and eliminate the autonomy of antitrust regulators—the Federal Economic Competition Commission (COFECE) and the Federal Telecommunications Institute (IFT)—along with other independent regulatory bodies.[676] If enacted, COFECE's functions would instead be under the purview of the Secretariat of Economy, and the IFT's functions to the Secretariat of Infrastructure, Communications, and Transport. Given the ruling party's supermajority in both legislative chambers, the party's prominence in local legislative bodies, and the support of the reform from President Claudia Sheinbaum, industry reports that the proposal is likely to move forward. Implementation of the reforms will go through a process, during which the U.S. government should engage with Mexican counterparts to ensure cross-border business operations are not disrupted.

The constitutional reform was approved in December 2024 and published in the Official Gazette, though implementation details have carried into 2025 as Congress continues to review additional constitutional reforms. Key issues in the reforms include:

- Centralizing Authority: the reforms would grant the executive branch greater control over preventing, investigating, and punishing monopolies, anti-competitive practices, and market inefficiencies, while critics warn this could weaken independent study and consultation before imposing remedies;
- Losing the Independent Watchdogs: COFECE and IFT would effectively be dissolved under the reforms, with their current functions consolidated into a new national competition authority, the Comisión Nacional Antimonopolio (CNA), rather than remaining as independent constitutional bodies. The formation of the CNA has entered its final and definitive transition phase with the appointment and ratification of its new commissioners in October 2025. This step is pivotal, as the full constitution of the new five-member CNA Board (Plenum)—down from seven in the former COFECE—marks the imminent and formal dissolution of both COFECE and the IFT. Consequently, all ongoing investigation proceedings that were suspended after the law's publication in July 2025 will resume immediately. The CNA is distinct from its predecessors: it possesses significantly broadened powers, including full authority over the entire telecommunications sector (formerly the IFT's domain), and operates under a much stricter sanctioning regime with higher fines for anticompetitive practices. Despite being granted technical and operational independence, the CNA is structured as a decentralized

[676] *Posicionamiento del IFT sobre la aprobación del Dictamen de la Comisión de Puntos Constitucionales de la Cámara Diputados, a la iniciativa en materia de simplificación orgánica* [Mexico]. (2024). https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/posicionamiento-del-ift-sobre-la-aprobacion-del-dictamen-de-la-comision-de-puntos-constitucionales.

public agency under the Ministry of Economy, a shift that has prompted concerns regarding potential political influence or changes in the overall policy direction;
- Judicial Oversight: The reforms do allow entities the ability to challenge decisions by the new antitrust authority through constitutional appeals, which would be reviewed by specialized judges.

Mexico's ongoing development of technical regulations and conformity assessment procedures for ICT products and devices continues to pose significant challenges for U.S. companies due to short consultation periods, insufficient implementation timelines, and a lack of meaningful consideration of industry input. Under the approach previously used by the telecommunications regulator, new regulations have often entered into force with minimal notice, failing to comply with USMCA TBT Chapter and ICT Annex obligations, including requirements to allow e-labeling options. Compounding these issues, Mexican agencies frequently do not conduct regulatory impact analyses or cost-benefit studies before issuing new rules, a problem that has grown more pronounced with the newly established Digital Transformation and Telecommunications Agency, whose leadership has expressed an intent to deprioritize such analyses. These regulatory practices undermine transparency, increase compliance costs, and create unnecessary market access barriers for foreign firms. The United States should urge Mexico to adopt robust, transparent, and predictable regulatory processes that include adequate consultation periods, evidence-based policymaking, and adherence to USMCA commitments.

Nepal

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In March 2024, the Ministry of Communication and Information Technology introduced the draft Information Technology and Cyber Security Bill 2080 to regulate activities related to information technology and cyber security. As written, the Bill would require data centers and cloud service providers to obtain licenses subject to yearly renewal and would require health and financial organizations to store all data domestically.[677] USTR should continue to track the development of this legislation and its discriminatory impact on foreign data centers and cloud service providers.

Government-Imposed Content Restrictions and Related Access Barriers

In August 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.[678] This measure seeks to implement a government-owned intranet and an internet filtering system—a

[677] Gyawali, R. (2024, April 25). IT Bill requires a serious revision. *The Annapurna Express.* https://theannapurnaexpress.com/story/48543.
[678] Republica. (2024, August 9). *Govt approves National Cyber Security Policy 2023*. https://myrepublica.nagariknetwork.com/news/govt-approves-national-cyber-security-policy-2023/.

national internet gateway—that would restrict what content is visible online in the country. The policy would implement a regime of monitoring what is posted online in the country and restricting what can be seen by internet users.[679] This represents a threat to the internet ecosystem and to the availability of U.S. services in the country, would limit competition and increase operational barriers, and is viewed by industry as an effort to exert tighter control over the internet, ensuring centralized monitoring over all traffic. [680] The broad impact on human rights is described by Digital Rights Nepal and International Center for Not-for-Profit Law detail in a joint brief: "Implementation of the [National Internet Gateway] presents a profound risk of censorship and threatens the fundamental right to freedom of expression. By consolidating all internet traffic through a centralized point, the government gains unprecedented control over the flow of information, enabling them to regulate and censor online content according to their own agenda."[681] As the civil society group Article 19 elaborates, the concern is that "if Nepal's national internet gateway is modeled on others in the region it would mean centralising 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."[682]

In November 2023, Nepal's cabinet adopted the 'Social Media Directive' in an effort to address sectarian violence in the country.[683] The Directive imposes local registration mandates as well as onerous content moderation requirements that lack safe harbor provisions. By 2025, the Ministry of Communication and Information Technology had issued repeated warnings that major platforms must register under the Directive, appoint local liaison officers, and implement complaint and moderation systems, while stating it was assessing the consequences of non-compliance.

On January 28, 2025, Nepal's National Assembly introduced the Social Media Act Bill, aimed at regulating social media platforms and users through mandatory registration, penalties, and expanded content moderation requirements. The bill would require platforms to register with the government in order to operate in Nepal, adopt strict moderation practices, and address a range

---

[679] Digital Rights Nepal. (2024, August 7). *Advocacy Brief on National Cybersecurity Policy 2023.* https://digitalrightsnepal.org/report/advocacy-brief-on-national-cybersecurity-policy-2023/.
[680] Caster, M. (2023, August 30). *Nepal: Revise cybersecurity policy to avoid further internet fragmentation*. Article 19. https://www.article19.org/resources/nepal-revise-cybersecurity-policy-to-avoid-further-internet-fragmentation/.
[681] Digital Rights Nepal. (2024, August 7). *Advocacy Brief on National Cybersecurity Policy 2023*. https://digitalrightsnepal.org/report/advocacy-brief-on-national-cybersecurity-policy-2023/.
[682] Caster, M. (2023, August 30). *Nepal: Revise cybersecurity policy to avoid further internet fragmentation*. ARTICLE 19. https://www.article19.org/resources/nepal-revise-cybersecurity-policy-to-avoid-further-internet-fragmentation/.
[683] The Kathmandu Post. (2023, December 10). *Asia Internet Coalition asks government to rethink Nepal's social media policy*. https://kathmandupost.com/national/2023/12/10/asia-internet-coalition-asks-government-to-rethink-nepal-s-social-media-policy; The Kathmandu Post. (2023, November 21). *Free speech advocates decry social media directive saying it oversteps Electronic Transactions Act*. https://kathmandupost.com/national/2023/11/21/free-speech-advocates-decry-social-media-directive-saying-it-oversteps-electronic-transactions-act.

of online harms including extortion, cyberbullying, phishing, scams, and hacking. More troublingly, the bill grants authorities broad powers to order the removal of content deemed "indecent" or "misleading," criminalizes remarks classified as defamatory, penalizes the sharing of "trolling" images, and prohibits disclosure of "confidential information." It also criminalizes interacting with social media with "malicious intent," creating sweeping and ambiguous liability. Civil society groups have warned that these vague provisions risk abuse, chilling legitimate speech and empowering arbitrary enforcement. It provides for penalties of up to 2.5 million Nepali rupees (approximately US$18,300) and up to five years' imprisonment, with punishments able to accumulate across concurrent charges. The bill poses serious risks to cross-border digital services by imposing discriminatory registration requirements and overbroad liability on foreign platforms, undermining open internet principles and creating new barriers for U.S. firms operating in Nepal's market.

Nepal's E-Commerce Act 2081 (effective April 15, 2025) establishes broad extraterritorial jurisdiction over foreign digital service providers, requiring local registration, licensing, and compliance with Nepali consumer, contract, and data protection laws.[684] It classifies global online platforms as intermediaries, making them potentially liable for third-party activities such as fraudulent listings or misleading advertisements. The Act mandates strict obligations on seller verification, payment transparency, returns and refunds, data privacy, and grievance redress. It also introduces heavy penalties and accountability provisions, increasing operational and legal risks. Overall, the Act represents a major shift toward tighter regulatory control and localized compliance requirements for cross-border e-commerce and digital platforms operating in Nepal.

In September 2025, Nepal ordered the blocking of 26 major social media platforms that had not registered under the existing registration regime, prompting protests and court challenges and the eventual withdrawal of the blocking order. While the future of such enacted and proposed regulations remains uncertain following ongoing political turmoil in Nepal, CCIA urges USTR to remain vigilant.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

In March 2022, Nepal amended its National Broadcasting Rules to require broadcast OTT, video-on-demand (VOD), and online television services in Nepal to obtain broadcast licenses from the Ministry of Information and Communications before being able to serve the local market.[685] Additionally, Broadcast OTT providers will need to maintain local cache servers in Nepal, store user data and program records for at least 60 days, and adopt age-based categorization of Broadcast OTT content.

---

[684] *Electronic Commerce Act, 2081* [Mexico] Act No. 13. (2025). https://giwmscdnone.gov.np/media/files/E-Commerce%20Act%2C%202081_yr7k9o5.pdf

[685] Pradhan & Associates. (2022, March 23). *Amendment to the National Broadcasting Rules 2052 (1995 AD).* https://pradhanlaw.com/publications/amendment-to-the-national-broadcasting-rules-2052-1995-ad.

In April 2023, the Nepal Telecommunications Authority (NTA) released a draft OTT Regulatory Framework to regulate voice/video telephony and messaging OTT services, which would require Communications OTT providers to obtain an authorization from NTA before providing their services in Nepal.[686] To obtain the authorization, Communications OTT providers will need to register a branch office or appoint a local intermediary in Nepal.

These changes to the broadcasting and telecommunications regulatory regime in Nepal create significant regulatory and financial burdens on U.S. and other countries' Broadcast OTT, Communications OTT, VOD, and Online TV providers seeking to serve the market.

Taxation of Digital Products and Services

Nepal introduced a 2% DST through its Finance Act for FY 2022/23, which took effect on July 17, 2022. 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.

New Zealand

Forced Revenue Transfers for Digital News

On December 4, 2022, the government announced a 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.[687] In the announcement, ministers 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.[688] 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 NZ$40-60 million per year could be extracted from registered digital platforms subjected to the law for the benefit of news

[686] *OTT Regulatory Framework (Draft)* [Nepal]. (2023). https://nta.gov.np/uploads/contents/OTT%20Regulatory%20Framework%20(Draft).pdf.
[687] Jackson, W. (2022, December 4). *Big online platforms to pay fair price for local news content*. Beehive. https://www.beehive.govt.nz/release/big-online-platforms-pay-fair-price-local-news-content.
[688] *Fair Digital News Bargaining Bill* [New Zealand] No. 278-1. (2023). https://bills.parliament.nz/v/6/fc7faac0-2ec0-4e47-7ab5-08db9ebb2302?Tab=hansard.

businesses.[689] The bill has been referred to the Parliament's Economic Development, Science and Innovation Committee, and remains under consideration.

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 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. Many have expressed significant concerns about the bill's emphasis on forced revenue transfers between sectors and its implications for news industry innovation.[690] However, the government has officially put the Fair Digital News Bargaining Bill on hold, citing that the legislation is "not ready."

Government-Imposed Restrictions on Internet Content and Related Access Barriers

The government of New Zealand is considering new age restriction rules for social media platforms, closely following measures recently adopted in Australia. The proposed Social Media (Age-Restricted Users) Bill would require social media platforms to take reasonable steps to prevent individuals under the age of 16 from holding accounts on designated age-restricted platforms.[691] Providers that fail to comply could face fines of up to NZ$2 million, enforced through civil proceedings. The Bill also allows the government to designate which platforms are age-restricted, set regulations, and review the law's operation after three years. Such a framework could significantly raise compliance costs and legal risks, particularly for foreign platforms, by mandating costly age-verification systems and adding operational complexity.

Nigeria

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The 2019 Guidelines for Nigerian Content Development in ICT, issued by the National Information Technology Development Agency (NIDTA) require all "sovereign data" to be

[689] New Zealand Ministry for Culture & Heritage. (2022, December 9). *Proactive release of Cabinet Material: Supporting commercial bargaining for online news*. https://mch.govt.nz/sites/default/files/projects/cab-rel-online-news-151222.pdf
[690] Crampton, E. (2024, July 10). *The Fair Digital News Bargaining Bill.* The New Zealand Initiative. https://www.nzinitiative.org.nz/reports-and-media/reports/the-fair-digital-news-bargaining-bill.
[691] *Social Media Age-Restricted Users Bill* [New Zealand]. (2025). https://img.scoop.co.nz/media/pdfs/2505/Social_Media_AgeRestricted_Users_Bill.pdf.

stored locally.[692] The definition of ”sovereign data" in the Guidelines encompasses a broad range of datasets including government data and information management companies, effectively requiring all data to be stores locally.

The previous administration advanced a proposed NITDA Bill and National Shared Services Corporation (NSSC) Bill to the National Assembly earlier in 2023. The NITDA 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 aimed to aggregate the provision of ICT infrastructure and services—including cloud services—to Nigerian federal agencies under a single, state-owned corporation. Neither bill had passed before the subsequent elections, though industry continues to monitor their revival.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

In September 2022, the NITDA issued the Code of Practice for Interactive Computer Service Platforms and Internet Intermediaries.[693] Under the Code, which came into effect on December 26, 2022, digital service platforms with more than one million users must incorporate and maintain a physical presence in Nigeria and appoint a liaison officer, obligations that may limit cross-border operations.[694] The Code also imposes content moderation, notice-and-takedown, transparency, and cooperation with legal requests. Following industry consultation, NITDA reviewed some stringent provisions, including differentiated services, flexible takedown timelines for specific content, and the removal of criminal liability and "stay down" obligations.

Restrictions on Cross Border Data Flows

The Nigeria Data Protection Act outlines strict conditions for transferring data across borders.[695] To ensure an adequate level of protection, such transfers are only permitted if the receiving country's laws, binding corporate rules, contractual agreements, codes of conduct, or certification mechanisms provide sufficient safeguards. Data controllers must thoroughly document all cross-border transfers and the protective measures in place. Furthermore, the Nigeria Data Protection Commission holds the authority to designate specific data categories that are subject to transfer restrictions and may also issue adequacy decisions for various countries or sectors.

---

[692] *National Information Technology Development Agency, Guidelines for Nigerian Content Development in ICT* [Nigeria]. (2019). https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf.
[693] *Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries* [Nigeria]. (2022). https://nitda.gov.ng/wp-content/uploads/2022/10/APPROVED-NITDA-CODE-OF-PRACTIVE-FOR-INTERACTIVE-COMPUTER-SERVICE-PLATFORMS-INTERNET-INTERMEDIARIES-2022-002.pdf.
[694] Elliott, V. (2021, May 14). New laws requiring social media platforms to hire local staff could endanger employees. *Rest of World*. https://restofworld.org/2021/social-media-laws-twitter-facebook/.
[695] *Data Protection Act* [Nigeria]. (2023). https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf.

Nigeria's Guidelines for Content Development in Information and Communication Technology (2023) establish local hosting requirements for government (sovereign), consumer and subscriber data. The Guidelines emphasize localization but do not expressly provide that cross-border transfer is only allowed with NITDA approval. This is in addition to 2011 guidelines from the telecoms regulator requiring local hosting of subscriber data (though such requirements are not comprehensively published in the public domain) and the Central Bank Guidelines requiring domestic routing of card transactions; these rules primarily apply to domestic transactions and do not explicitly prohibit all cross-border transfers.

Taxation of Digital Products and Services

The 2021 Finance Act introduces income tax and digital service obligations for non-resident companies providing digital goods and services in Nigeria.[696] While the law applies to all non-resident companies earning above a certain threshold, extensive media coverage and analysis by experts have repeatedly mentioned the targeting of U.S. multinationals. The law specifically references non-resident companies with a "significant economic presence" in the country which is defined by a number of factors including: a minimum amount of revenue generated from users in Nigeria, transmitting data about Nigerian users, or the availability of local websites or local payment options. Exceptions have been built into the law for companies that are covered by a multilateral agreement to which the Nigerian government is a party.

This policy was eventually signed into law as the Finance Act of 2021 on December 31, 2021,[697] 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.[698] Under Nigeria's SEP regime, non-resident digital services firms may be taxed on a deemed profit basis, often resulting in an effective 6% rate on turnover where SEP criteria are met.

Under a 2022 amendment to existing laws, all advertising must be approved by the Advertising Regulatory Council of Nigeria (ARCON) before exposure. The extension of which requirement, which previously only applied to legacy advertising channels, to online advertising has been problematic, resulting in significant penalties and fines. In October 2022, ARCON 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

[696] KPMG. (2019). *Nigeria: Tax Provisions in Finance Act*. https://home.kpmg/us/en/home/insights/2020/01/tnf-nigeria-tax-provisions-in-finance-act-2020.html.
[697] Uwaegbute, C. et. al. (2024, October 9). *Deduction of Tax at Source (Withholding) Regulations, 2024: Key changes from the official gazette*. PWC. https://www.pwc.com/ng/en/assets/pdf/deduction-of-tax-at-source-withholding-regulations-2024-key-changes-from-the-official-gazette.pdf.
[698] Oyeniyi, A. (2022, March 4). Google, Meta, and Others Raise Nigeria Prices Due to Digital Tax. *QUARTZ*. https://qz.com/africa/2137660/google-meta-and-others-raise-nigeria-prices-due-to-digital-tax/.

streams.[699] ARCON filed a lawsuit against Meta to enforce the fine. However, ARCON ultimately withdrew the matter after about 3 years with little or no progress. ARCON has subsequently issued similar fines to TikTok & Google, although there remains no practical means of enforcement of the fines.

Under a 2022 amendment to existing laws, all advertising in Nigeria must receive prior approval from ARCON before being displayed. This requirement, previously limited to traditional advertising channels, was expanded to cover online advertising, creating significant compliance challenges for digital platforms. In October 2022, ARCON fined Meta US$70 million for allegedly running ads without prior vetting—a process that places unreasonable administrative and operational burdens on online platforms that rely on dynamic, globally integrated advertising systems to reach audiences in a market as large as Nigeria. ARCON also filed a lawsuit to enforce the fine but ultimately withdrew the case after three years with little to no progress.[700] Despite this, ARCON has since issued similar fines against TikTok and Google, underscoring the ongoing legal uncertainty and regulatory risk. Although enforcement mechanisms remain limited in practice, the policy continues to pose significant exposure and compliance risks for online platforms operating in Nigeria.

Norway

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Norwegian government is considering the development of a national cloud solution for a broadly-defined set of critical entities, which would encourage public sector entities to route a substantial portion of data through state-backed frameworks. [701] The government is also campaigning to expand this regime to the energy, telecommunications, and financial services sectors, despite reports showing that a state-owned cloud service would increase costs.[702] The national cloud solution would discriminate against U.S. and other foreign companies, if, as proposed, it would developed exclusively by Norwegian providers within Norway. USTR should investigate whether such a proposal is consistent with Norway's comprehensive commitments to allow cross-border computer services.

---

[699] Asadu, C. (2022, October 5). Nigeria Regulator Seeks $70M Penalty Against Meta. *AP News*. https://apnews.com/article/technology-africa-business-lawsuits-nigeria-f00313679c07f2a56d844d53b7094643.
[700] Adewakun, A. (2024, July 20). ARCON withdraws suit against Meta, restrategises. *The Tribune*. https://tribuneonlineng.com/arcon-withdraws-suit-against-meta-restrategises.
[701] Norway Ministry of Justice and Public Security. (n.d.). *Meld. St. 9 (2022–2023): National control and cyber resilience to safeguard national security*. https://www.regjeringen.no/en/documents/meld.-st.-9-20222023/id2950130/?ch=4.
[702] Anskaffelser. (2023, October 20). *It's probably not economically viable to establish an extensive private state-owned cloud service*, OSLO ECON. https://osloeconomics.no/en/2023/10/20/its-probably-not-economically-viable-to-establish-an-extensive-private-state-owned-cloud-service/.

Pakistan

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Sectoral regulators have already imposed restrictive data localization requirements. For example, the Pakistan Telecommunications Authority requires its licensees to obtain prior approval before transferring any data abroad.[703] In 2024, the Securities and Exchange Commission of Pakistan prohibited licensed digital lenders from storing data on cloud infrastructure located outside the country, effectively mandating local hosting.[704] Similarly, the State Bank of Pakistan requires licensed exchange companies to maintain both their primary and secondary data centers within Pakistan and permits outsourcing of "material workloads" only to local cloud service providers, absent case-by-case approval.[705] These existing measures entrench data localization, restrict the ability of firms to leverage global cloud infrastructure, and raise compliance costs for foreign and domestic companies alike.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

In 2025, Pakistan's Parliament passed amendments to the Prevention of Electronic Crimes Act, 2016, formally approved on January 29, 2025, which established a new regulator, the Social Media Protection and Regulatory Authority (SMPRA), to replace the Pakistan Telecommunication Authority as the primary body overseeing social media platforms.[706] The amended law grants SMPRA broad legislative and enforcement powers, including the authority to require social media platforms to enlist with the Authority, impose fines, degrade or block platforms until compliance is achieved, and issue content removal directions. The scope of content subject to takedown has been significantly expanded to include material that SMPRA deems contrary to the "ideology of Pakistan," that it has "reason to believe" is false, or that contains aspersions against any person, including members of the judiciary, armed forces, or Parliament, with "aspersion" defined broadly as "spreading false and harmful information which damages the reputation of a person." These amendments create sweeping new obligations and risks for social media platforms, increasing the potential for arbitrary enforcement, censorship, and operational uncertainty for foreign firms operating in Pakistan. 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

[703] Ahmed, M. M., Rehman, S. & Khan, S. K. (2021). *Pakistan Law and Practice*. RIAA Barker Gilette. https://www.riaabarkergillette.com/pk/wp-content/uploads/2021/05/015_PAKISTAN.pdf.
[704] *Requirements for NBFCs engaged in Digital Lending* [Pakistan] Circular No. 12. https://www.secp.gov.pk/document/circular-no-12-of-2024-requirements-for-nbfcs-engaged-in-digital-lending/.
[705] *Issuance of Regulatory Framework for Exchange Companies* [Pakistan] FE Circular No. 02 of 2024. https://www.sbp.org.pk/epd/2024/FEC2.htm.
[706] *An Act to further amend the Prevention of Electronic Crimes Act, 2016* [Pakistan] No. F. 9(05). (2025). https://www.na.gov.pk/uploads/documents/679b243193585_457.pdf.

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.[707]

The government has repeatedly deployed internet shutdowns in response to protests and elections, imposing large economic losses and harming human rights.[708] Industry has reported that shutdowns have introduced significant uncertainty and encouraged investment flight.[709] Recent internet shutdowns by the government are estimated to have cost Pakistan between US$892 million and US$1.6 billion. In August 2024, local industry began reporting on the government's implementation of an internet firewall to moderate content – triggering widespread network disruptions. According to local industry groups, the firewall has already cost the economy US$300 million, with further costs and harms to human rights expected to increase.[710]

Restrictions on Cross-Border Data Flows

In May 2023, Pakistan's Ministry of Information Technology and Telecommunications (MoITT) published a draft Personal Data Protection bill.[711] In January 2025, MoITT informally shared an updated draft, but it has yet to be made publicly available. The revised draft bill adopts a broad scope, applying to both digital and non-digital operators and extending to entities outside Pakistan through extraterritorial provisions. While it removes an earlier requirement that "Critical Personal Data" must only be processed on servers located within Pakistan, the bill empowers the federal government under Sections 32(2), 47(1)(f), and 56(2) to restrict the transfer of "certain personal data" to jurisdictions outside Pakistan. This discretionary authority effectively allows the government to block cross-border data transfers for any reason, including vague determinations related to "public interest" or national security, creating significant regulatory uncertainty for foreign companies operating in Pakistan. The bill also requires explicit consent for some cross-border transfers in addition to either adequacy determinations or compliance with further transfer conditions, and it does not provide for internationally recognized transfer mechanisms. Taken together, these provisions are functionally equivalent to data localization, severely restricting the ability of firms to leverage global cloud infrastructure. The draft also grants regulators sweeping powers with few procedural safeguards or

---

[707] Asia Internet Coalition. (2021). *Industry comments on the Amendment - Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules*. https://aicasia.org/policy-advocacy/aic-submits-comments-on-the-amendment-removal-and-blocking-of-unlawful-online-content/.
[708] AccessNow. (2024, December 13). *#KeepItOn: authorities in Pakistan must stop the ongoing suppression of digital* rights. https://www.accessnow.org/press-release/keepiton-authorities-in-pakistan-stop-suppression-of-rights/.
[709] Siddiqui, Z. (2023, June 8). Pakistan's 4-day internet shutdown was the final straw for its tech workers. *Rest of World*. https://restofworld.org/2023/pakistan-internet-outage-tech-workers/.
[710] Shahid, A. (2024, August 15). Pakistan's internet firewall could cost economy $300 million, association says. *Reuters*. https://www.reuters.com/technology/pakistans-internet-firewall-could-cost-economy-300-million-association-says-2024-08-15/.
[711] *Draft Legislation - Personal Protection Bill* [Pakistan]. (2023). https://moitt.gov.pk/Detail/YjVmNzU0MWMtYzBkMC00Yjg5LTk1ODktOTJiODYzZTY5ZWRk.

accountability mechanisms, raising serious concerns about arbitrary or politically motivated enforcement. It allows regulators to define "sensitive personal data" expansively—including financial data—and establishes a more onerous standard for processing such data, requiring both consent and an additional legal basis, a stricter approach than many international benchmark regimes. The bill contains burdensome data processing requirements and broad regulatory powers, with no guarantee of meaningful stakeholder consultation before introduction in Parliament, heightening uncertainty for industry.

Taxation of Digital Products and Services

In 2025, Pakistan introduced a digital services tax applicable to the sale of goods and services by offshore platforms with a "significant digital presence" in Pakistan.[712] However, before the tax came into force, the Federal Board of Revenue issued a blanket exemption on its implementation, leaving uncertainty about its future application.[713] Despite this exemption, Pakistan continues to maintain several overlapping taxation measures on digital products and services. Provincial service tax laws extend their reach to companies without a physical place of business in Pakistan, effectively taxing offshore entities providing services into the country. At the federal level, income tax laws are also applied extraterritorially to offshore companies. In 2023, the definition of "permanent establishment" was also broadened to cover entities with no physical presence in Pakistan but a virtual business presence, including where transactions are carried out through the internet or other electronic means.

Panama

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Resolutions 52 (2021) and 03 (2024) of the Government Innovation Authority AIG require government entities using cloud services for functions that are determined to be critical—relating to state security or involving sensitive institutional data—to be hosted domestically by December 31, 2024. These resolutions undermine the ability of foreign companies to continue serving the government in its functions. The resolutions undermine cross-border data flows, harm Panama's chances of serving as a regional hub, restrict the deployment of new services such as generative AI, and introduce cybersecurity vulnerabilities.

---

[712] *A Bill to give effect to the financial proposals of the Federal Government for the year beginning on the first day of July, 2025 and to amend certain laws* [Pakistan]. (2025). https://fbr.gov.pk/Budget2025-26/FinanceBill/Finance-Bill-2025.pdf; CCIA. (2025). *Pakistan's 'Digital Presence Proceeds' Tax*. https://ccianet.org/wp-content/uploads/2025/07/Pakistans-%E2%80%98Digital-Presence-Proceeds-Tax.pdf.

[713] *Arab News*. (2025, July 31). Pakistan withdraws digital tax on foreign online purchases. https://www.arabnews.com/node/2610121/pakistan.

Papua New Guinea

Government-Imposed Restrictions on Internet Content and Related Access Barriers

On October 2, 2025, the National Executive Council approved the 2025 National Social Media Policy, advancing proposed regulations for social media regulation to Parliament for approval.[714] Under the Policy, users aged 14 and above will be required to register for a SevisPass digital ID before accessing platforms like Facebook, TikTok, Instagram and X. Social media companies must also register locally and comply with domestic laws, and a new national e-Safety Directorate will monitor and enforce rules against harmful content. Such measures could impose significant barriers, particularly for foreign platforms, by adding localization, compliance, and user-verification obligations that raise operational costs and restrict market access.

Peru

Customs-Related Restrictions and Import Barriers for Goods

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 on 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 establish a potential barrier for firms engaging in express delivery shipments to the country.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

In 2025, the Peruvian Congress began debating Bill 10880,[715] which seeks to establish a regulatory framework for the protection of children and adolescents in the digital environment. A key concern for U.S. industry is a proposed amendment within the bill that would modify Peru's Personal Data Protection Law. This amendment would raise the age of consent for the processing of personal data from 14 to 16 years old. This change would have a broad impact on all U.S. digital services operating in Peru, requiring them to implement potentially burdensome age verification mechanisms and obtain parental consent for a larger segment of the teenage population. While the bill references using "reasonable efforts" and "available technology" for age verification, the higher age of consent itself represents a significant shift in the data

[714] *Anadolu*. (2025, October 3). Papua New Guinea mulls age restrictions on social media. https://www.aa.com.tr/en/asia-pacific/papua-new-guinea-mulls-age-restrictions-on-social-media/3706540.
[715] *PROYECTO DE LEY DE PROTECCIÓN DE NIÑOS Y ADOLESCENTES EN ENTORNOS DIGITALES* [Peru] Bill No. 10880. (2025). https://wb2server.congreso.gob.pe/spley-portal/#/expediente/2021/10880.

protection landscape and could create new compliance burdens for a wide range of online services, from social media and gaming to educational platforms.

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 2024 NTE Report.[716] CCIA urges USTR to engage with Peru and push for full implementation of the trade agreement and establish intermediary protections within the parameters of the PTPA.

Restrictions on Cross-Border Data Flows

On January 9, 2020, the Digital Government Secretariat of Peru released Emergency Decree 007 - Digital Trust Framework.[717] The Framework raises significant industry concerns as its text gives preferential treatment to domestic data storage and domestic service providers. Initial analysis of the Decree indicates several potential trade barriers, including: (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.

Since 2020, Peru's Secretariat of Government and Digital Transformation has been developing regulations to implement this Decree. After an initial draft in 2023, a new draft regulation was published for comment in April 2025.[718] This latest draft has provided some clarification and addressed certain industry concerns. Notably, the proposed government cybersecurity certifications ("digital trust seals") are now explicitly applicable only to public entities, not private companies. Furthermore, the scope of mandatory digital security measures for the private sector has been narrowed to specific critical sectors (e.g., finance, health, transport), with the guidelines serving only as reference for other companies.

However, significant concerns remain regarding the Decree's broad definitions. The latest draft regulation of April 2025 maintains a definition of "Digital Service Provider" but explicitly

---

[716] United States Trade Representative. (2024). *2024 National Trade Estimate Report on Foreign Trade Barriers*. https://ustr.gov/sites/default/files/2024%20NTE%20Report_1.pdf.
[717] Olaechea, J. A. (n.d.). *Doing business in Peru: overview*. Thomson Reuters. https://content.next.westlaw.com/practical-law/document/I2ef127e01ed511e38578f7ccc38dcbee/Doing-Business-in-Peru-Overview?viewType=FullText&transitionType=Default&contextData=(sc.Default).
[718] *DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO* [Peru] No. 007-2020. (2020). https://cdn.www.gob.pe/uploads/document/file/7883460/6640808-rgto-du-007-2020_prepublicacion-f-f.pdf?v=1743880329.

excludes "third parties acting as internet intermediaries or providing technical support services (such as cloud, hosting, security, etc.)." While this exclusion is a positive development, the draft regulation still fails to provide a clear legal definition of "internet intermediaries" and uses terms that promote ambiguity. This creates legal uncertainty and potential enforcement risks, for a wide range of US digital service providers, who could be inadvertently captured by obligations not intended for them. To date, the draft regulations have not developed or clarified the provisions from the original Decree concerning cross-border data flows or data localization mandates, but the authority to do so remains in the underlying Decree, creating continued uncertainty for US businesses operating in Peru.

As in all countries, the ability to move data and access information across borders from Peru is essential for businesses regardless of size or sector. To implement safeguards, Peru can 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.

Philippines

Barriers to the Deployment and Operation of Network Infrastructure

While the customs laws related to laying fiber optic cables in the Philippines have remained unchanged for many years, the Bureau of Customs has revised its interpretation of the rules over the past year regarding its treatment of ships. The Bureau has taken the position that foreign-built and specialty-constructed repair vessels entering Philippine waters for subsea cable installation, repair, or survey work should be treated as permanent imports, subject to duties and taxes as high as 12% of the vessel's full value. Given that cable ships are highly specialized assets valued in the hundreds of millions of dollars, these obligations push companies' associated costs into the millions. Instead of a temporary bond to guarantee re-export—long the practice—firms are now forced to pay what amounts to an "insurance premium" of 2% of the import tax, without refund, simply to secure a permit to operate. This marks a clear departure from international norms. No other country imposes such extractive fees, and 76 governments, including the Philippines, have already committed under the Istanbul Convention on Temporary Admission to avoid precisely this treatment for means of transport.[719] The Philippines omitted the relevant annex covering vessels, and now insists on treating subsea repair ships as taxable imports, even though the same treaty's provisions for professional equipment could be applied. The resulting "Marina Special Permits" regime has left companies with the untenable choice of paying exorbitant fees or risking impoundment of vessels, which would delay or prevent urgent cable repairs. The current

[719] *Convention on Temporary Admission (Istanbul Convention)* [World Customs Organization]. (1990, June 26). https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/conventions/pf_tempadmiscon.aspx.

regime threatens to deter investment in subsea cable projects and slow urgent repair work, leaving cables idle for extended periods.

The Philippines allocates and assigns spectrum through the Radio Control Law of 1931 (RA 3846 and its amendment, RA 584), Executive Order No. 546 1979, and the Public Telecommunications Policy Act of 1995 (RA 7925).[720] These laws and directives organize the country's legal framework for spectrum allocation, operation, and permitting. Industry reports that although RA 7925 stipulates that there must be a solicitation for open tenders in allocating spectrum, no public bidding to allocate spectrum, such as through spectrum auctions, has ever taken place. Applications typically require companies to document their spectrum needs in a letter to the National Telecommunications Commission. The framework lacks transparency and effectively results in the government allowing to arbitrarily prioritize certain criteria, such as financial or technical capacity, on a case-by-case basis to choose winners and losers in the market.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Public procurement preferences the Philippines applies to domestic entities extend to the cloud sector, restricting limiting foreign access for firms without a domestic partner. U.S. firms can offer cloud services in the Philippines sector but are subjected to a burdensome licensing process administered by the Securities and Exchange Commission in the country as a condition for providing cloud services to the public sector.[721] Absent an SEC license, entities seeking public sector procurement are forced to work with domestic entities, reflecting a *de facto* obligation.

The Philippines currently requires government agencies to procure cloud computing services exclusively through the Government Cloud, a cloud infrastructure managed by the Department of Information and Communications Technology (DICT).[722] In 2024, CSPs were invited to participate in a new government procurement catalogue, the eMarketplace of the Modernized Philippine Government Electronic Procurement System, operated by the Procurement Service of the Department of Budget and Management. This platform will include cloud services as part of Common-Use Supplies and Equipment. The launch of cloud services on the eMarketplace is expected to go live before the end of 2025. As part of the onboarding process, U.S. cloud service providers are required to submit a Certificate of Reciprocity, confirming that Philippine companies may compete, with limited exceptions, on an equal basis with U.S. suppliers in U.S. government procurement. This additional documentation requirement may pose administrative hurdles and could potentially delay participation by foreign providers. The current approach

[720] *Act Providing for the Regulation of Radio Stations and Radio Communications in the Philippine Islands, and for Other Purposes* [Philippines] Act No. 3846. (1931). https://lawphil.net/statutes/acts/act1931/act_3846_1931.html.
[721] *Government Procurement Policy Board Resolution No. 14-2021* [Philippines]. (2021). https://www.gppb.gov.ph/wp-content/uploads/2023/05/GPPB-Resolution-No.-14-2021.pdf.
[722] *Department Circular No. 002* [Philippines]. (2017). https://www.jetro.go.jp/ext_images/jetro/activities/support/aseanjapan/report/3-6.pdf.

effectively limits flexibility in procurement for government agencies and raises concerns about market access for non-local CSPs, particularly as the Philippine government expands the use of GovCloud as the primary platform for critical digital government services.

The Office of the President has been considering a draft Executive Order dubbed "Policy Guidelines on Data Residency and Data Classification for Government Agencies" with onerous data localization provisions. The original draft of the EO, first drafted in 2023,[723] and updated in 2025, would require all data, including non-sensitive and commercial data, that is in any way connected to government work to be processed and stored in the Philippines. Further, the EO explicitly states that the following entities would be mandated to process data using local infrastructure: "Core operations of Bangko Sentral Supervised Financial Institutions[724] 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."[725] The highly restrictive effect of the EO warrants close monitoring of the issues and engagement by the U.S. government: although the commercial entities subject to a localization mandate are limited, these are major potential customers of cross-border cloud services and thus the impact on U.S. cloud suppliers is likely to be significant. Compounding concerns is the fact that the major beneficiary of this policy is likely to be several large Chinese operators, who have established a large presence in the Philippine market.

The Konektadong Pinoy Act aims to remove the outdated legislative franchise requirement for certain segments of telecommunications infrastructure (middle and last mile for data transmission).[726] Since only Filipino entities can obtain franchises, this requirement has significantly hindered foreign investment, and the liberalization represents a substantial step toward lowering entry barriers, fostering greater competition, and creating meaningful market opportunities for U.S. digital services and technology providers. However, this positive market opening is jeopardized by several provisions—most notably Section 6(j), which grants broad authority to DICT to "formulate policies to safeguard local data, when necessary to advance national security and public interest." The forthcoming Implementing Rules and Regulations currently being drafted could embed discriminatory measures, including mandatory data localization requirements or overly broad national security vetting of foreign entities. Such

[723] *Policy Guidelines on Data Localization of Data Stored on the Cloud* [Philippines]. (2023). https://drive.google.com/file/d/14nFO_hJGH-r7IK2xnEswOoHpN6NKwZsC/view.
[724] World Bank. (2020). *The Philippines: Detailed Assessment of Observance - Basel Core Principles for Effective Banking Supervision.* https://openknowledge.worldbank.org/server/api/core/bitstreams/b9e68ee6-5a5c-50d8-b024-14e61e5a9c53/content#page=9.
[725] Global Data Alliance. (2023, September 26). *GDA Comments on Draft Executive Order of the Republic of the Philippines - Policy Guidelines on Data Localization of Data Store in the Cloud*. https://globaldataalliance.org/wp-content/uploads/2023/09/09262023gsadatalocalcloud.pdf.
[726] *An Act Establishing a Comprehensive and Inclusive Data Transmission and Connectivity Framework for the Philippines* [Philippines] S. No. 2699*. (2025). https://web.senate.gov.ph/lisdata/4436242009%21.pdf.

measures would create an asymmetric regulatory environment that disproportionately disadvantages U.S. digital services providers, introduces heightened uncertainty and compliance burdens, and ultimately undermines the liberalization goals of the Act.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

An Internet Transactions Bill was enacted on December 5, 2023.[727] The Bill requires 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.[728] The proposed legislation would grant the Trade Minister broad powers to issue takedown orders as well as other obligations for online platform 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.

On May 24, 2025 the Department of Trade and Industry announced the implementing rules for the 2023 Internet Transaction Act.[729] The Act establishes obligations for e-commerce transactions and requires digital platforms to verify the identity of persons involved in transactions and provide consumers with transparency and opportunities for redress. The requirements could impinge on consumer privacy and increase compliance costs and burdens on suppliers in the market.

Taxation of Digital Products and Services

The United States and the Philippines are party to the Income Tax Convention of 1976, a treaty that 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."[730] Implementation of this treaty, however, has been challenging. The Bureau of International Revenue (BIR) requires income tax payors to apply for status under this treaty, approval which is governed by complex and burdensome documentation procedures. Failure to adhere to the documentation guidelines can lead to entities being subjected to penalties and criminal liabilities. The BIR has not established standard processing timelines, and businesses are subsequently

---

[727] Senate of the Philippines. (2023, September 26). *Senate OKs Proposed Internet Transactions Act on Third Reading.* https://legacy.senate.gov.ph/press_release/2023/0926_prib1.asp.
[728] Filane, M. C. (2022, August 24). Bill on internet transactions hurdles House panel. *Philippines News Agency*. https://www.pna.gov.ph/articles/1182088; Natividad, M. R. (2020, December 22). *The Proposed Internet Transactions Act and the Uncertainties in Online Retail*. ACCRA. https://accralaw.com/2020/12/22/the-proposed-internet-transactions-act-and-the-uncertainties-in-online-retail/.
[729] *Implementing Rules and Regulations of Republic Act No. 11981 or the Tatak Pinoy* (Proudly Filipino) Act [Philippines]. (2024). https://www.dti.gov.ph/sdm_downloads/implementing-rules-and-regulations-of-the-internet-transactions-act-of-2023/.
[730] United States. Department of the Treasury. (1983). *Income tax convention with the Republic of the Philippines, 3 (1983)*. https://www.irs.gov/pub/irs-trty/philip.pdf.

required to wait indefinitely without any commitment toward 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 and impacts members of all industries seeking to provide their services and goods to the Philippines market.

The BIR's issuance of Revenue Memorandum Circular No. 5-2024[731] in January 2024 added further confusion to income-tax obligations of non-resident suppliers of cross-border services. The RMC appears to depart from established principles of income taxation of cross-border services (using the place where the services are performed to determine if the transaction is income-taxable) and treats the place of receipt of the services as being crucial in determining the taxability of the transaction. The BIR and the Philippines government should engage in comprehensive industry consultation, including with U.S. non-resident service providers, to clarify the income-tax position under Philippine law in line with well-recognized and established international practices.

The Philippines government has adopted a new law (RA 12023) to impose a 12% VAT on digital services consumed in the Philippines and provided by both resident and non-resident digital services providers (DSPs).[732] The digital services included within the scope of this measure are online search engines, online marketplaces or e-marketplaces; cloud services; online media and advertising; online platforms; and digital goods. While this law imposing VAT on DSPs does not discriminate between U.S. non-resident DSPs (or other foreign DSPs) and local DSPs, industry is concerned that implementing rules and regulations, which are currently being developed, could impose unworkable requirements on foreign DSPs similar to what has happened above for income-tax payors.

Other Barriers to Digital Trade

Republic Act No. 12009 (otherwise known as the "New Government Procurement Act")[733] and its implementing rules and regulations[734] contain explicit government procurement preferences for Philippine nationals or firms controlled by Philippine nationals. In particular, the New Government Procurement Act, which was signed into law in July 2024, requires a government body to award a procurement contract to a domestic bidder, even when a foreign entity offers a

[731] Bureau of Internal Revenue. (2024, January 10). *Revenue Memorandum Circular No. 5-2024: Further clarifying the proper tax treatment of cross-border services in light of the Supreme Court En Banc decision in Aces Philippines Cellular Satellite Corp. v. Commissioner of Internal Revenue*, G.R. No. 226680 (Jan. 10, 2024). https://bir-cdn.bir.gov.ph/BIR/pdf/RMC%20No.%205-2024.pdf.
[732] *AN ACT AMENDING SECTIONS 105, 108, 109, 110, 113, 114, 115, 128, 236, AND 288 AND ADDING NEW SECTIONS 108-A AND 108-B OF THE NATIONAL INTERNAL REVENUE CODE OF 1997, AS AMENDED* [Philippines] R EPUBLIC ACT NO. 12023. (2024). https://lawphil.net/statutes/repacts/ra2024/ra_12023_2024.html.
[733] *An Act Revising Republic Act* [Philippines] No. 9184. (2024). https://www.gppb.gov.ph/new-government-procurement-act-republic-act-no-12009/.
[734] *The 2016 Revised Implementing Rules and Regulations of Republic Act* [Philippines] No. 9184. 92024). https://www.gppb.gov.ph/ra-9184-and-2016-revised-irr.

lower bid, if the domestic bidder's offer does not exceed 25% of the foreign bidder's offer.[735] These rules reflect general preference for domestic contractors and therefore hinder foreign entities from gaining access to government procurement work.

Procurement policies in the Philippines have a long history of discrimination, dating back decades. The Philippines is not a signatory to the WTO Government Procurement Agreement. Philippine nationals or Filipino-controlled enterprises are given preferential treatment in the rewarding of procurement contracts, which include Executive Order No. 120 of 1993 and Government Procurement Policy Board Resolution 14-2005. Republic Act No. 9184, or the Government Procurement Reform Act, specifies a minimum Filipino ownership requirement of at least 60 percent in the procurement of goods, consulting services, and infrastructure projects.[736] Domestic goods are also provided preferential treatment at the expense of imported products in the bid evaluation process.

The preferential treatment entities given to entities from the Philippines is compounded by Commonwealth Act. No. 138, which gives government bodies the ability to choose the lowest *domestic* bidder as the winner of a contract even in the instance where a foreign entity offers a lower bid, as long as the domestic bidder's offer represents 15% or less of the foreign bidder's offer. The construction of these rules memorializes an overall preference given to domestic contractors, and taken together, undermines the ability of foreign providers to access government procurement work.

Various laws in the Philippines impose inconsistent and burdensome regulatory requirements on businesses operating in its Special Economic Zones.[737] Specifically, the Business Process Outsourcing and related services industries are often subjected to the same obligations as export manufacturing firms, ignoring the fundamental operational differences between them. This regulatory mismatch, coupled with outdated and uncompetitive incentive packages, creates regulatory risk and uncertainty for foreign investors, making the Philippines a less attractive investment destination.

---

[735] *AN ACT REVISING REPUBLIC ACT NO. 9184. OTHERWISE KNOWN AS THE "GOVERNMENT PROCUREMENT REFORM ACT". AND FOR OTHER PURPOSES* [Philippines] Republic Act No. 12009. (2024). https://ngpa.gppb.gov.ph/New-Government-Procurement-Act-RA-12009.pdf.

[736] *Government Procurement Reform Act* [Philippines] No. 9184. https://www.gppb.gov.ph/wp-content/uploads/2023/06/Republic-Act-No.-9184.pdf.

[737] *Special Economic Zones Act* [Philippines] Republic Act No. 7916. (1995). https://lawphil.net/statutes/repacts/ra1995/ra_7916_1995.html; *Corporate Recovery and Tax Incentives for Enterprises Act* [Philippines] Republic Act No. 11534. https://lawphil.net/statutes/repacts/ra2021/ra_11534_2021.html; *Corporate Recovery and Tax Incentives for Enterprises to Maximize Opportunities for Reinvigorating the Economy Act* [Philippines] Republic Act No. 12066. https://www.bir.gov.ph/create-more.

Poland

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Industry reports a draft law is pending that would update and extend existing cybersecurity regulations in Poland, with a proposed authority for the Minister of Digital Affairs to designate High Risk Vendors (HRV). Designated as an HRV would introduce obligations for companies to remove their equipment or software from the systems of critical entities within a designated time period. The rules are broad, which adds a threat of arbitrary designation and undue burdens of non-EU providers as HRVs. The draft has undergone a public consultation and is now pending further review and adoption, but these controversial provisions are expected to be implemented.

Taxation of Digital Products and Services

In August 2025, Poland's Ministry of Digital Affairs published options for a DST that would disproportionately burden foreign, particularly U.S., digital service providers while carving out domestic competitors.[738] Both "wide" and "narrow" variants of the proposed tax would apply turnover-based levies of 3–7.5% on sectors like e-commerce, search engine marketing, and display advertising, with rates notably higher than those under comparable DST regimes in Europe. Under the wide variant, the government estimates raising US$470–930 million annually, largely from the e-commerce sector, while the narrow variant, focused on search and display advertising, would raise US$130–200 million. Importantly, the narrow option not only applies higher rates but also selectively captures sectors dominated almost entirely by foreign, U.S.-headquartered firms, exempting domestic competitors. The Ministry has explicitly stated that revenues would flow into a discretionary fund under the Minister of Digital Affairs to support Polish technology firms and media, effectively redistributing wealth from foreign providers to local competitors. As a result, the measure is designed not simply to raise revenue, but to tilt the competitive landscape in favor of Polish firms at the expense of international players.

By targeting only digital business models while exempting equivalent offline services such as brick-and-mortar retail or traditional advertising, the proposal enshrines structural discrimination against online providers. Its narrower option intensifies these concerns by scoping in only the search and advertising sectors, areas almost exclusively operated by foreign firms, and then applying a higher rate than the wide variant, making its protectionist intent explicit. This approach mirrors earlier DSTs in France and the UK that were found under U.S. Section 301 investigations to be discriminatory, unreasonable, and burdensome. Moreover, by earmarking revenues specifically for domestic tech and media sectors, the measure is not a neutral tax but a transfer mechanism from U.S. companies to Polish industry. This structure risks contravening

[738] CCIA. (2025). *Poland's Proposed Digital Services Tax*. https://ccianet.org/library/polands-proposed-digital-services-tax/.

Poland's WTO and bilateral treaty obligations. The lack of transparency in how funds would be allocated further raises concerns of politicization and selective favoritism in spending.

Russia

Since Russia's 2022 invasion of Ukraine, the government has taken increasingly hostile actions against U.S. digital firms. These aggressive regulatory actions and discriminatory practices have pushed U.S. firms to exit the market. 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. As the government has seized foreign firms' financial assets,[739] state-affiliated enterprises have bought foreign firms' domestic subsidiaries, leaving the government largely in control of the domestic digital ecosystem.[740]

Asymmetric Platform Regulations

On June 24, Bill No. 654254-8 was introduced in the State Duma, amending the Law on Consumer Protection to regulate app stores. The proposed Bill mandates sideloading, requiring app store owners to allow interoperable access with programs and payment systems available under other app stores. While such requirements would implicitly raise barriers for certain app stores that differentiate their products on the basis of security, the Bill is explicitly aimed at specific U.S. companies as retaliation for their compliance with international sanctions on Russia,[741] and seeks to facilitate the mandatory pre-installation of the RuStore,[742] a unified app store controlled by the government, on all devices, posing further privacy and security risks. If enacted, this provision of preferential access for a Russian distribution service could also be inconsistent with Russia's GATS obligations and merit USTR investigation.

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. The government has enacted several laws to expand its authority over online

---

[739] Deutsch, J. & Levingston, I. (2022, March 10). War Accelerates Russia's Internet Isolation. *Bloomberg*. https://www.bloomberg.com/news/articles/2022-03-10/russia-internet-isolation-accelerates-after-ukraine-invasion; Satariano, A. & Hopkins, V. (2022, March 7). Russia, Blocked from the Global Internet, Plunges Into Digital Isolation. *The New York Times*. https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html; Izadi, E. & Ellison, S. (2022, March 4). Russia's independent media, long under siege, teeters under new Putin crackdown. *Washington Post*. https://www.washingtonpost.com/media/2022/03/04/putin-media-law-russia-news/.

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

[741] Udin, E. (2024, March 3). Russia Plans to Require Apple to Open IOS Third-Party App Store. *Giz China.* https://www.gizchina.com/2024/03/03/apple-open-ios-third-party-app-store/.

[742] Maxwell, A. (2023, October 4). Russia Prepares RuStore VPN Ban After Declaring RuStore Installation Mandatory. *Torrent Freak*. https://torrentfreak.com/russia-prepares-rustore-vpn-ban-after-declaring-rustore-installation-mandatory-231004/.

communications and services, imposing significant obligations on services to comply with government demands. Over the past several years, Russia's telecommunications regulator, Roskomnadzor, has veered away from its primary objective towards a quasi-intelligence agency, orchestrating the Kremlin's censorship and surveillance activities.[743]

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[744] and the Federal Law on Amending the Code of Administrative Violations,[745] establish penalties for "knowingly spreading fake news" and establish a framework for ISPs to block access to websites deemed to be spreading "fake news."

In May 2019, the Russian government enacted the Sovereign Internet Law to extend the government's 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.[746]

In December 2019, Russia adopted a law requiring the pre-installation of Russian software on certain consumer electronic products sold in Russia.[747] The law took effect in early 2021.[748] 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, and software that provides access to e-government infrastructure.

In 2021, Federal laws N482-FZ and N511-FZ came into effect.[749] 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 Russian media entities' content. Federal law N511-FZ imposes fines for services that do not remove banned information, which has included

---

[743] Mozur P. et. Al. (2022, September 22). They Are Watching: Inside Russia's Vast Surveillance State. *The New York Times*. https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html.
[744] *Amendments to Article 15-3 of the Federal Law on Information, Information Technologies and Information Protection* [Russia] No. 31-FZ. (2019). http://publication.pravo.gov.ru/Document/View/0001201903180031.
[745] *On Amendments to the Code of the Russian Federation on Administration Offenses* [Russia] No. 27-FZ. (2019). http://publication.pravo.gov.ru/Document/View/0001201903180021.
[746] Doffman, Z. (2019, May 2). Putin Signs 'Russian Internet Law' to Disconnect Russia From the World Wide Web. *Forbes*. https://www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnectthecountry-from-the-world-wide-web/.
[747] Porter, J. (2019, December 3). Russia Passes Law Forcing Manufacturers to Install Russian-made Software. *The Verge.* https://www.theverge.com/2019/12/3/20977459/russian-law-pre-installed-domestic-software-tvs-smartphones-laptops.
[748] *Reuters*. (2020, April 1). Russian Law Requires Smart Devices to Come Pre-Installed with Domestic Software. https://www.reuters.com/article/us-russia-technology-software/russian-law-requires-smart-devices-to-come- pre-installed-with-domestic-software-idUSKBN2BO4P2.
[749] Rakhmetov, B. (2021, February 22). *The Putin Regime Will Never Tire of Imposing Internet Control: Development in Digital Legislation in Russia*. Council on Foreign Relations. https://www.cfr.org/blog/putin-regime-will-never-tire-imposing-internet-control-developments-digital-legislation-russia.

political protest content. In past years, U.S. firms experienced an increase in demands by Roskomnadzor 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.[750]

Russia imposes restrictions on the use of tools to circumvent censorship methods and access restricted content or services. In early June 2022, Russia began to accelerate its ongoing campaign to block VPNs 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."[751] 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.[752]

Russia's already stringent state-sponsored censorship of content online also dramatically increased, often resulting in massive fines. The censorship of news has blended interference with traditional media outlets as well as news online. In March 2022, the Parliament passed two laws, No.31-FZ and No.32-FZ, to prohibit the publication of what the government determined to be falsehoods about the war in Ukraine—including calling the war an "invasion."[753] 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, resulting in a ₽3 million fine.[754]

Russian authorities have retaliated against U.S. companies that refuse to provide their platforms for Russian state propaganda or for entities under international sanctions. In 2022, Google's local subsidiary was forced to initiate bankruptcy proceedings after the government froze its bank accounts pursuant to court orders compelling the company to restore access to Tsargrad TV's YouTube and Gmail accounts, which had been suspended in July 2020 in compliance with U.S.

---

[750] Roache, M. (2021, April 1). How Russia is Stepping Up Its Campaign to Control the Internet. *TIME*. https://time.com/5951834/russia-control-internet; *Radio Free Europe/Free Liberty*. (2020, November 24). *New Russia Bill Would Expand Internet Censorship, HRW Warns*. https://www.rferl.org/a/hrw-warns-new-russian-bill-would-expandinternet-censorship/30966049.html.

[751] *INTERFAX*. (2022, June 2). Russia Restricting Proton VPN, similar services – Roskomnadzor. https://interfax.com/newsroom/top-stories/79803/.

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

[753] Izadi, E. & Ellison, S. (2022, March 4). Russia's Intendent Media, Long Under Sieges, Teeters Under New Putin Crackdown. *The Washington Post*. https://www.washingtonpost.com/media/2022/03/04/putin-media-law-russia-news/.

[754] *TACC*. (2023, August 7). Google fined 3 million rubles for failing to remove prohibited content and fakes about SVO. 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.

sanctions against the outlet's owner. Russian courts imposed escalating penalties of ₽100,000 (approximately US$1,230) per day, doubling weekly with no cap, until the services were restored. These penalties were later replicated through around 20 additional "copycat" claims filed by other Russian media outlets. By October 2024, the accumulated fines had reached a sum of two undecillion rubles—a figure followed by 36 zeros—illustrating the punitive and coercive nature of Russia's legal strategy against U.S. platforms.[755]

The government has threatened to block websites of outlets for critical commentary or news about its invasion of Ukraine, and throttled or blocked access to numerous websites and platforms hosting online news sources.[756] In 2022, the government began blocking Facebook, X, and Instagram, and in 2024, began throttling access to WhatsApp and YouTube and blocked Signal, and in 2025 throttled WhatsApp and GoogleMeet call functions under the pretext of preventing sabotage activities in the Russian territory.[757]

On December 12, 2023, Law No. 406-FZ came into force, requiring owners of websites, webpages, information systems, and programs operating in Russia to authenticate all domestic users accessing their content.[758] It also requires hosting providers to notify Roskomnadzor before commencing operations involving hosting information on a system permanently connected to the Internet.

On March 11, 2024, Law No. 42-Fz entered into force, amending the country's 2012 Foreign Agent Law to ban advertising on platforms owned by media entities designated as foreign actors and ban Russian entities from accepting advertisements from these entities.[759] In August 2024, Google began shutting down payments to Russian-based websites and content owners monetizing advertisements placed by Google.[760] Such restrictions would expand under Bill No. 652920-8, passed by the State Duma on July 25, 2024. Once enacted, organizations declared as "extremist" or "undesirable" will be prohibited from advertising within Russia, with such prohibitions extending to "information resources" whose access is limited by existing regulations

---

[755] Harkavy, R. (2025, July 9). Strasbourg court finds Russia violated Google's rights over YouTube content. *ICLG*. https://iclg.com/news/22815-strasbourg-court-finds-russia-violated-google-s-rights-over-Youtube-content; Fraser, G. (2024, October 31). Russia fines Google more money than there is in entire world. *BBC*. https://www.bbc.com/news/articles/cdxvnwkl5kgo.

[756] Human Rights Watch. (2022, February 28). *Russia: With War, Censorship Reaches New Heights*. https://www.hrw.org/news/2022/02/28/russia-war-censorship-reaches-new-heights.

[757] Tubridy, M. & Garvey, N. (2025, September 5). Russians Report Widespread Disruptions on Google Meet. *Moscow Times*. https://www.themoscowtimes.com/2025/09/05/russians-report-widespread-disruptions-on-google-meet-a90441.

[758] Digital Policy Alert. (2024, February 1). *Russia: Implemented Law No. 406-FZ including prohibition on providing services if not included in Roskomnadzor register*. https://digitalpolicyalert.org/event/18093-implemented-law-no-406-fz-including-prohibition-on-providing-services-if-not-included-in-roskomnadzor-register.

[759] *Amendment to Article 11 of the Federal Law on Control over the Activities of Persons under Foreign Influence and Certain Legislative Acts of the Russian Federation* [Russia] No. 42-FZ. (2024). http://publication.pravo.gov.ru/document/0001202403110004.

[760] *Reuters*. (2024, August 12). Google says it is deactivating Russia-based AdSense accounts. https://www.reuters.com/technology/google-says-it-is-deactivating-russia-based-adsense-accounts-2024-08-12/.

related to "information technology and protection." Given the broad scope of the Bill and the willingness of the government to label foreign companies as extremist and undesirable, this effort represents a *de facto* ban on digital foreign advertising in the country. The Bill was justified under the premise that Russian users continue to access banned foreign services through VPNs, with the government aiming to eliminate revenue streams between Russian advertisers and foreign platforms.[761]

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 resulted in an estimated US$200,000 in losses,[762] 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.[763]

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.[764] In July 2022, Russian-backed separatists blocked Google due to the purported spread of "disinformation" in a breakaway region of eastern Ukraine.[765] Regional internet outages have occurred throughout Ukraine since Russia began its war campaign in the country,[766] with some areas experiencing blackouts for multiple days—in some cases due to reported Russian cyberattacks.[767] 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.

---

[761] Digital Policy Alert. (n.d.). *Russia: Passed Bill banning advertising on information resources whose activities are recognized as undesirable and platforms banned (Bill No. 652920-8)*.https://digitalpolicyalert.org/event/21737-passed-bill-banning-advertising-on-information-resources-whose-activities-are-recognised-as-undesirable-and-platforms-banned-bill-no-652920-8.

[762] Dan Goodin, *Russia's Twitter Throttling May Given Censors Never Been Seen Capabilities,* ARS TECHNICA (Apr. 6, 2021, 5:20 PM), https://arstechnica.com/gadgets/2021/04/russias-twitter-throttling-may-give-censors-never-before-seen-capabilities/.

[763] United States International Trade Commission. (2022). *Foreign Censorship, Part 2: Trade and Economic Effects on U.S. Businesses*. https://www.usitc.gov/publications/332/pub5334.pdf.

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

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

[766] Collier, K., & Talmazan, Y. (2022, March 9). *Ukraine facing major regional outages as Russian invasion continues. NBC News.* https://www.nbcnews.com/tech/tech-news/ukraine-facing-major-regional-internet-outages-russian-invasion-contin-rcna18973.

[767] FitzGerald, D. (2022, May 1). *Occupied regions of southern Ukraine lose internet services. Wall Street Journal.* https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-04-30/card/occupied-regions-of-southern-ukraine-lose-internet-service-YrGVuhNABIkQzxc099dM.

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 certain companies "land" by establishing a local unit that will represent its interests in Russia and will be liable for its activities.[768] The law applies to foreign companies that 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 government-provided software that 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 2022 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 transferring money and making payments, and potential full or partial blocking or throttling of the noncompliant website or applications. Such local presence requirements, coupled with onerous compliance requirements and harsh penalties, severely constrain the ability of U.S. companies to operate in Russia.

This landing law—previously imposed on foreign technology companies to pressure firms to establish legal entities in Russia for permission to continue operations in the country—has been leveraged by the Kremlin along with throttling websites, fining companies, and jailing individuals as a method of censorship during the war in Ukraine.[769] 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.[770]

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.[771] As Article 19 highlights, establishing

---

[768] Debevoise & Plimpton. (2021, August 23). *New requirements for localisation of major internet companies in Russia*. https://www.debevoise.com/insights/publications/2021/08/new-requirements-for-localisation-of-major.
[769] Satariano, A. (2022, February 26). *Russia intensifies censorship campaign, pressuring tech giants. The New York Times.* https://www.nytimes.com/2022/02/26/technology/russia-censorship-tech.html.
[770] Zakharov, A., & Churmanova, K. (2021, December 16). *How Russia tries to censor Western social media. BBC.* https://www.bbc.com/news/blogs-trending-59687496.
[771] *Reuters.* (2022, July 5). Russian lawmakers approve harsher fines for foreign tech firms. https://www.reuters.com/world/europe/russian-lawmakers-approve-harsher-fines-foreign-tech-firms-without-offices-2022-07-05/.

a local presence in Russia in compliance with the landing law makes it easier for the Russian government to demand the removal of content that 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.[772]

Russia's broader data localization efforts have intensified, as a Russian court levied fines in June 2022 against Google, Airbnb, Pinterest, Twitch, and UPS for allegedly failing to store the personal data of Russians within the country.[773] The court's announcement of the fines on Telegram cites "repeated violations" of the country's data localization laws.[774] In June 2022, a Moscow court fined Google ₽15 million (US$260,000) for being found to have repeatedly declined to adhere to data localization laws.[775] These court cases and fines are likely to continue—Roskomnadzor had also announced that an administrative case against Apple had begun in late May.[776]

On March 1, 2023, amendments were made to Russia's Federal Law on Personal Data.[777] 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.[778]

On December 4, 2023, Bill No. 502113-8 was introduced in the State Duma, amending the Criminal Code to expand criminal penalties for unauthorized handling of personal data. Among its provisions, the Bill would impose penalties for illegal cross-border data transfers in the form of up to eight years in prison and fines of up to ₽2 million (US$22,000).

---

[772] Article 19. (2022, January 21). *Russia: Internet companies must challenge censorship under new law.* https://www.article19.org/resources/russia-internet-companies-must-challenge-censorship-under-new-law/.
[773] *Reuters*. (2022, June 28). Russia fines streaming company Twitch over data storage. https://www.reuters.com/technology/russia-fines-streaming-company-twitch-over-data-storage-2022-06-28/; Wodinsky, S. (2022, June 28). Russia fines Airbnb, Twitch, Pinterest on not storing local data. *Gizmodo*. https://gizmodo.com/russia-fines-airbnb-twitch-pinterest-google-local-data-1849118187.
[774] *Spectrum-2024: Regulation in the field of information and communication technologies* [Russia]. (2024). https://t.me/s/rkn_tg.
[775] *Reuters*. (2022, June 16). Russia Fines Google $260,000 for Breaching Data Rules. https://www.reuters.com/technology/russia-fines-google-260000-breaching-data-localisation-rules-tass-2022-06-16/.
[776] *Front News*. (2022, May 28). Drew Up Administrative Protocols for Airbnb, Pinterest, Apple, Google, Twitch. https://frontnews.eu/en/news/details/31852.
[777] Rumyantsev, S. (n.d.). Russia adopts new rules on cross-border data transfers. *Lexology*. https://www.lexology.com/commentary/tech-data-telecoms-media/russia/gorodissky-partners/russia-adopts-new-rules-on-cross-border-data-transfers.
[778] Data Guidance. (2023, March 12). *Russia: New procedures for data transfers enter into effect*. https://www.dataguidance.com/news/russia-new-procedures-data-transfers-enter-effect.

Rwanda

Taxation of Digital Products and Services

On May 27, 2025, the Government of Rwanda passed a law implementing a 1.5% digital service tax on digital service providers that have significant operations in Rwanda.[779] The details—including the scope of the tax, what constitutes substantial national presence, registration procedures, tax declaration and payment processes, and other criteria for taxing digital services—will be specified in an upcoming Ministerial Order.

Saudi Arabia

Asymmetric Platform Regulation

In July 2022, the Communications, Space, and Technology Commission (CST) published its draft Competition Regulations for Digital Content Platforms with the goal of regulating large online digital services platforms.[780] 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 Saudi market first.[781] 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.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The CST issued the Cloud Computing Regulatory Framework in 2018, with the latest revision released in October 2023.[782] The rules contain a provision on data localization that may restrict access to the Saudi market for foreign internet services. The regulation will also increase ISP

---

[779] *LAW Nº 014/2025 OF 27/05/2025 AMENDING LAW Nº 027/2022 OF 20/10/2022 ESTABLISHING TAXES ON INCOME* [Rwanda]. (2025). https://www.rra.gov.rw/fileadmin/user_upload/Law_amending_the_2022_Income_Tax_May_2025.pdf.

[780] *Competition Regulations for Digital Content Platforms* [Saudi Arabia]. (2022), https://istitlaa.ncc.gov.sa/en/transportation/citc/crdcp/Documents/Competition%20Regulations%20for%20Digital%20Content%20Platforms.pdf.

[781] CCIA. (2022, November 3). *CCIA Comments on the Saudi Arabian CITC's Draft Competition Regulations for Digital Content Platforms*. https://ccianet.org/library/ccia-comments-on-the-saudi-arabian-citcs-draft-competition-regulations-for-digital-content-platforms/.

[782] *Cloud Computing Services Provisioning* [Saudi Arabia]. (2023). https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf.

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. CST 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) has imposed data localization requirements, primarily through the 2018 Essential Cybersecurity Controls[783] and 2020 Cloud Cybersecurity Controls.[784] The ECC framework mandates that data hosted and stored using cloud computing services must be located domestically. This regulation applies to government entities, state-owned enterprises, and critical infrastructure operators, including sectors such as financial services, aviation, and oil and gas. In addition to data storage, the NCA requires that cybersecurity managed services centers for monitoring and operations be completely located inside the country. Furthermore, the 2020 Cloud Cybersecurity Controls require companies offering cloud services in-country (such as systems used for storage processing, disaster recovery centers, and systems used for monitoring and support) to store the data locally. The controls do, however, offer a limited exception: Level 3 and 4 data may be hosted abroad, but entities are required to seek an exemption from the NCA to avoid the general localization mandate.

More recently, and since January 2024, the Saudi Data & AI Authority (SDAIA) has issued four major consultations on data governance, data storage, and data sharing that could significantly shape the regulatory environment for digital services in the Kingdom. First, the National Register of Controllers consultation proposes rules requiring all Controllers to register on the National Data Governance Platform, thereby creating a unified national register and ensuring compliance with the Personal Data Protection Law (PDPL) in line with Article 34 of the PDPL's Implementing Regulation.[785] Second, the Data Sovereignty Public Policy consultation outlines four key principles guiding Saudi Arabia's data sovereignty approach.[786] While this reflects progress toward a more structured data protection regime, industry stakeholders have raised concerns that the framework may introduce protectionist measures or de facto data localization requirements, potentially undermining cross-border data flows. Third, the draft General Rules for Secondary Use of Data clarify how data collected for specific purposes can be reused by government entities, private organizations, and research institutions for public-interest objectives.[787] However, notable gaps remain, including unclear application of the "profit-

[783] *National Cybersecurity Authority, Essential Cybersecurity Controls* [Saudi Arabia]. (2018). https://itig-iraq.iq/wp-content/uploads/2019/08/Essential-Cybersecurity-Controls-2018.pdf.
[784] *Cloud Cybersecurity Controls* [Saudi Arabia] CCC – 1. (2020). https://nca.gov.sa/ar/ccc-en.pdf.
[785] *Rules Governing the National Register of Controllers within the Kingdom* [Saudi Arabia]. (2024). https://istitlaa.ncc.gov.sa/en/Transportation/NDMO/RulesGoverningtheNationalRegister/Pages/default.aspx
[786] *Data Sovereignty Draft Public Policy* [Saudi Arabia]. (2024). https://istitlaa.ncc.gov.sa/en/Transportation/NDMO/DataSovereigntyPolicy/Pages/default.aspx
[787] *Draft General Rules for Secondary Use of Data* [Saudi Arabia]. (2025). https://istitlaa.ncc.gov.sa/en/transportation/ndmo/secondaryuserules/Documents/Draft%20General%20Rules%20for%20Secondary%20Use%20of%20Data.pdf.

oriented" activity prohibition to public-private partnerships or commercial innovation, lack of detail on pre-approval procedures for automated data sharing, absence of guidance on IP provisions for private-sector data access licenses, and ambiguity in the allocation of controller and processor responsibilities between primary and secondary entities. Finally, the Controls for Data Protection Activities consultation seeks to regulate entities providing data protection services such as consultancy, training, awareness, and compliance solutions, but the lack of a clear definition of "technical solutions" creates uncertainty over the scope of the rules.[788] If applied broadly, these controls could significantly increase compliance burdens for industry and introduce new operational complexities.

Government-Imposed Content Restrictions and Related Access Barriers

Saudi Arabia maintains extensive controls over social media, using the expansive provisions under the 2007 Anti-Cyber Crime Law to criminalize political speech online.

In September 2023, the General Authority of Media Regulation proposed a new Media Law. It would impose obligations on media outlets, defined to include social media platforms and individual users, to obtain licenses prior to engaging in "media activity," while reserving the authority to determine if content requires prior approval before publication.[789] While the full impact on digital platforms will not become clear until the implementing regulations are issued and licensing processes are clarified, industry leaders anticipate regulatory hurdles, at least in the near-term. In its current form, the law does not include provisions exempting platforms from intermediary liability, which is of concern, given the Kingdom's focus on digital content moderation.

There is further confusion regarding the responsibilities of digital platforms with regard to content moderation due to the draft CST Global Digital Content Safe Harbor Law, which proposes platform liability exemptions for user-generated content.[790] For example, exemptions are only available for platforms certified by the government, certifications can be revoked and the government can request content removal under conditions detailed in the liability certificate.[791]

---

[788] Saudi Data and AI Authority. (2025). *Draft Controls Governing Commercial, Professional, and Non-Profit Activities Related to Personal Data Protection*. https://istitlaa.ncc.gov.sa/en/transportation/ndmo/rulesgoverningpdplactivities/Documents/Draft%20Controls%20Governing%20Commercial,%20Professional,%20and%20Non-Profit%20Activities%20Related%20to%20Personal%20Data%20Protection.pdf.

[789] Zaghdoudi, A. (2024, February 29). *In Saudi Arabia, no safe harbor for free speech*. AccessNow. https://www.accessnow.org/saudiarabiasafeharbor/.

[790] Saudi Communications, Space, and Technology Commission. (2023, September 12). *Request for public consultation on the Global Digital Content Safe Harbor Law*. https://www.cst.gov.sa/en/regulations-and-licenses/public-consultations/publicconsultation-50.

[791] Zaghdoudi, A. (2024, February 29). *In Saudi Arabia, no safe harbor for free speech*. AccessNow. https://www.accessnow.org/saudiarabiasafeharbor /.

On the creator side, the GMedia issued new guidelines for content creators in September 2025, detailing the types of language and visual content that is prohibited on social media platforms. Details on penalties and fines are yet to be clarified, but individuals and businesses appear likely to be held directly responsible for content posted on their social media accounts.[792]

Deepfake Guidelines issued by the SDAIA in September 2024 instruct platforms - including social media platforms and other intermediaries - to disable access to and prevent the spread of deepfake content deemed misleading or harmful.[793] The Guidelines indicate potential penalties on platforms for failure to comply, including where the misleading content is user-generated. They also reference the potential adaptation of content-identification tools for deepfake detection, signaling heightened expectations for proactive detection and mitigation by platforms. Public consultation closed after the October 2024 deadline, and U.S. stakeholders are monitoring for potential amendments.

The Ministry of Communications and Information Technology (MCIT) opened a public consultation on July 8, 2024 on a proposed amendment to the Telecommunications and Information Technology Act, that would impose severe restrictions on social media companies and other digital content platforms.[794] Under the draft language, platforms would be required to implement internet filtering and prohibit user attempts at circumvention. Platforms that fail to comply risk fines of up to SAR25 million (US$6.6 million), partial or complete service suspension, license deprivation, and the blocking of platform services. At present, MCIT is still reviewing feedback to the consultation, with no confirmation of when the outcome will be announced.

Since the mid-2010s, Saudi Arabia has maintained restrictions on Voice over Internet Protocol services, including voice and video calling features on widely used applications such as WhatsApp and Facebook Messenger, creating a significant barrier to the provision of digital communication services. While text and media functions remain available, encrypted voice and video calling is typically blocked or heavily restricted by local internet service providers under government regulatory direction. These measures are justified by authorities on economic grounds, aimed at protecting the revenue streams of state-licensed telecom operators, and on security and regulatory grounds, citing challenges in monitoring encrypted communications. Only a limited number of government-approved or locally licensed apps are allowed, often tied to paid services, while others face inconsistent enforcement, generating operational uncertainty

[792] Hassan, S. (2024, September 25). Saudi Arabia issues major update to social media rules for businesses. *Caterer*. https://www.caterermiddleeast.com/saudi-arabia/saudi-arabia-issues-major-update-to-social-media-rules-for-businesses.
[793] Saudi Data and AI Authority. (2024). *Deepfake Guidelines*. https://istitlaa.ncc.gov.sa/en/transportation/ndmo/deepfakesguidelines/Documents/SDAIA_Deepfakes%20Guidelines.pdf?trk=public_post_comment-text
[794] *Amendments to the Telecommunications and Information Technology Act* [Saudi Arabia]. (2024). https://istitlaa.ncc.gov.sa/en/Transportation/Mcit/information/Pages/default.aspx.

for providers and users. This policy limits foreign service providers' ability to offer full functionality, distorts competition in favor of domestic telecom operators, and raises compliance and legal risks, ultimately undermining fair market access and reducing consumer choice.

In 2025, the Saudi Central Bank issued a directive prohibiting local banks and financial institutions from using instant messaging applications for official communications with customers, marking a significant shift in how financial institutions are required to engage with clients. The measure, officially justified on security and fraud prevention grounds, reflects concerns over the reliability of third-party messaging apps for sensitive financial communications. Under the directive, institutions must transition to secure, regulated, in-app messaging systems that comply with data protection and financial sector regulations. This effectively excludes major global messaging platforms from the Saudi financial sector, closing off a key channel for business messaging services and increasing compliance and operational barriers for foreign providers.

Potential Challenges to the Development of AI

Saudi Arabia's approach to AI regulation is still evolving, with a stated objective of encouraging innovation while prioritizing safety, accountability, and ethics. To date, the government has favored a light-touch regulatory model, focusing on issuing sector-specific guidelines and policy statements rather than enacting comprehensive legislation. This strategy allows for flexibility and rapid adaptation to technological developments, while also signaling regulatory expectations on issues such as safety, transparency, and responsible AI development. One notable exception is the Global AI Hub Law, drafted by the Communications, Space and Technology Commission (CST) and published in May 2025.[795] This draft law seeks to establish "AI Hubs" or sovereign data zones within the Kingdom, enabling international organizations and foreign governments to operate in a controlled and trusted environment. While the initiative aims to facilitate cross-border data flows and build international confidence, its potential impact is constrained by significant legal and operational uncertainties, including (i) the absence of clear security and data protection standards for Hub Operators, (ii) a lack of defined mechanisms to resolve legal conflicts arising from overlapping jurisdictions, and (iii) ambiguity regarding the scope and triggers for Saudi authorities' intervention in specific scenarios. Consequently, the industry's ability to strengthen cross-border management and R&D capabilities remains contingent on the provision of clear operational guidance and legal safeguards, which could be achieved through more detailed implementing rules. In addition, industry seeks predictable pathways for cross-border data flows, greater transparency around government and data-access requests, and continued risk-based alignment with internationally recognized AI frameworks to ensure legal certainty and foster investment.

[795] Saudi Communications, Space, and Technology Commission. (2025, April 14). *CST Publishes a Public Consultation for the Global AI Hub Law*. https://www.cst.gov.sa/en/media-center/news/N2025041401.

Restrictions on Cross-Border Data Flows

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 SAR 5,000,000 (US$1.3 million).[796] Entities that seek to process personal data are required to register as data controllers through an electronic portal managed by the Saudi Data and Artificial Intelligence Authority, maintain detailed records of processing activities, and, for foreign companies, appoint a local representative responsible for compliance.[797] Some of these restrictions were lifted with amendments implemented on September 14, 2024, that allow for data transfers absent risks to national security and creates a precedent for recognizing personal data protection adequacy in foreign jurisdictions. However, the overall 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. Clarifications from the SDAIA on the "approved list" for jurisdictions to which data flows are allowed is expected in early 2026 and scope of this list will critically affect Cloud operations in Saudi Arabia.

In April 2025, the SDAIA issued a public consultation on Risk Assessment Guidelines for Transferring Personal Data outside the Kingdom, outlining a framework intended to support cross-border data transfers in service of research, innovation, and public interest.[798] Key concerns from industry stakeholders center on the vague definition of "public interest" and the lack of clarity surrounding licensing terms, particularly as they relate to intellectual property protections, confidentiality obligations, and downstream use of data. These gaps could lead to inconsistent interpretations and increase legal and operational uncertainty for foreign digital service providers.

In May 2025, SDAIA followed up with a public consultation on draft amendments to the Implementing Regulation of the PDPL, which, if adopted, would enhance legal clarity, improve operational predictability, and bring the framework into closer alignment with international standards, including the EU GDPR.[799] However, the draft also removes key definitions—such as the definition of "personal data breach"—introducing new legal ambiguities that could complicate compliance obligations and create interpretive uncertainty for both regulators and companies operating in the Kingdom.

---

[796] نظام حماية البيانات الشخصية [Saudi Arabia]. (2021). https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/b7cfae89-828e-4994-b167-adaa00e37188/1.
[797] IAPP. (2022, March 22). *How to Prepare for Saudi Arabia's Personal Data Protection Law*. https://iapp.org/news/a/how-to-prepare-for-saudi-arabias-personal-data-protection-law/.
[798] Saudi Data and AI Authority. (2025). *Draft Risk Assessment Guidelines for Transferring Personal Data Outside the Kingdom.* sdaia.gov.sa/en/SDAIA/about/Documents/RisksTransferringDataOutsideKingdomEn.pdf
[799] Saudi Data and AI Authority. (2025). *Draft Implementing Regulation of PDPL.* https://istitlaa.ncc.gov.sa/en/transportation/ndmo/irofpdplamendments/Documents/Summary%20Draft%20Amendments%20to%20the%20Implementing%20Regulation%20of%20the%20PDPL%20EN.pdf.

Taxation of Digital Products and Services

Saudi Arabia does not currently impose a standalone digital services tax, although recent regulatory activity and international dynamics suggest that the government may explore new avenues to tax foreign digital companies.[800] Currently, non-resident digital service providers must register for VAT if selling to Saudi customers. The VAT, introduced in 2018 at a rate of 5% and raised in 2020 to a rate of 15%, applies broadly. In April 2025, the Zakat, Tax, and Customs Authority approved amendments to the VAT Implementing Regulations, requiring electronic platforms (intermediaries between non-resident suppliers and Saudi customers) to collect VAT, handle compliance documentation, and meet reporting obligations.[801]

Other Barriers to Digital Trade

Saudi Arabia's Regional Headquarters (RHQ) Law, which took effect on January 1, 2024, requires multinational companies seeking to do business with Saudi government entities to establish a regional headquarters in the Kingdom.[802] Companies that fail to obtain an RHQ license from the Ministry of Investment of Saudi Arabia (MISA) risk losing eligibility for government contracts and associated tax incentives. The RHQ program offers extensive incentives to qualifying companies, including a 30-year exemption from corporate income tax and withholding tax on RHQ activities, a 10-year Saudization exemption, visa quota exemptions and accelerated processing, waivers of professional accreditation, and priority in government tendering. RHQs must begin operations within six months of licensing, conduct at least three mandatory strategic management activities, and employ at least 15 full-time staff in the first year, including three senior executives. Importantly, RHQs may not engage in direct commercial activities or revenue generation, which must be carried out through licensed affiliates. As the Saudi government has made local presence a top priority, companies without an RHQ may face reduced access to future government contracts and commercial opportunities, especially as the regulatory and business environment continues to evolve.

---

[800] Organisation for Economic Co-operation and Development. (n.d.). *Base erosion and profit shifting (BEPS). OECD.* https://www.oecd.org/en/topics/base-erosion-and-profit-shifting-beps.html.
[801] Baker McKenzie. (2025, April 18). *Saudi Arabia: Changes to the VAT Implementing Regulations*. https://insightplus.bakermckenzie.com/bm/tax/saudi-arabia-changes-to-the-vat-implementing-regulations-effective-18-april-2025.
[802] KSA Zakat, Tax and Customs Authority. (n.d.). *Guideline KSA in Headquarters Regional for Provisions Zakat and Tax the Clarify to Guideline .Headquarters Regional of Activities the to Applicable*. https://zatca.gov.sa/en/HelpCenter/guidelines/Documents/Guideline%20for%20Regional%20Headquarters%20in%20KSA%20(2).pdf.

Singapore

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

On May 7, the Parliament passed an amendment[803] to the 2018 Cybersecurity Bill to broaden the number of entities subject to reporting obligations and increase potential penalties for non-compliance. The amendment expands covered entities to include Foundational Digital Infrastructure providers, such as cloud computing providers and data center facility services, even when located wholly overseas.

Government-Imposed Content Restrictions and Related Access Barriers

The Protection from Online Falsehoods and Manipulation Bill came into effect on October 2, 2019.[804] 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.[805] The process whereby the government flags content as false or misleading is opaque and lacks an adequate oversight process. Instead of enhancing trust online, these rules could spread more misinformation while restricting platforms' ability to continue to address misinformation issues. Stakeholders have raised concerns with enforcement of these laws since they went into effect,[806] 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.[807] After Singaporean citizens, US social media companies have been the largest target of cases under POFMA, and several have since ceased allowing political ads as a result.[808]

The Foreign Interference (Countermeasures) Act (FICA) was passed on October 4, 2021 and went into effect in July 2022.[809] Similar to the earlier content legislation, 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

---

[803] *Cybersecurity (Amendment) Bill* [Singapore] Act No. 15. (2024). https://www.parliament.gov.sg/docs/default-source/bills-introduced/cybersecurity-(amendment)-bill-15-2024.pdf?sfvrsn=1bb05508_1.
[804] *Protection from Online Falsehoods and Manipulation* [Singapore]. (2019). https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625.
[805] Stelly, R. (2019, April 25). *Singapore's Dangerous Response to Combating Misinformation Online*. Disruptive Competition Project. http://www.project-disco.org/21st-century-trade/042519-singaporesdangerous-response-combating-misinformation-online/.
[806] Human Rights Watch. (2021, January 13). *Singapore Fake News Law Curtails Speech*. https://www.hrw.org/news/2021/01/13/singapore-fake-news-law-curtails-speech.
[807] Freedom House. (2023). *Freedom on the Net 2023: Singapore*. https://freedomhouse.org/country/singapore/freedom-net/2023.
[808] U.S. Department of State. (2024). *2024 Investment Climate Statements: Singapore*. https://www.state.gov/reports/2024-investment-climate-statements/singapore/.
[809] *Straits Times*. (2022, July 6). Measures in Foreign Surveillance Law to Take Effect. https://www.straitstimes.com/singapore/measures-in-spores-foreign-interference-law-to-counter-hostile-information-campaigns-take-effect-from-july-7.

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.[810]

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 (IMDA) 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 as the initial companies named as subject to the Code.[811] 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."[812] 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.[813]

---

[810] Ministry of Foreign Affairs Singapore. (2022, February 24). *Singapore's reply to a joint communication from special procedures mandate holders on the Foreign Interference (Countermeasures) Act.* https://www.mfa.gov.sg/Overseas-Mission/Geneva/Mission-Updates/2022/02/Sgp-reply-to-a-JC-frm-SPMHs-Foreign-Interference; Human Rights Watch. (2021, October 13). *Singapore: Withdraw Foreign Interference (Countermeasures) Bill.* https://www.hrw.org/news/2021/10/13/singapore-withdraw-foreign-interference-countermeasures-bill

[811] Bird & Bird. (2024). *Designated Social Media Services.* https://protect-eu.mimecast.com/s/ORryCDkKMTWvBx5iqySSw?domain=sites-twobirds.vuture.net.

[812] *Broadcasting Act 1994 Guidelines on Categories of Harmful Content* [Singapore]. (1994). 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.

[813] Ang, A. et al. (2022, July 22). *MCI seeks comments on proposed Code of Practice for Online Safety and Content Code for Social Media Services*. Allen & Gledhill. 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.

On November 9, 2022, the Parliament passed legislation imposing new obligations on social media providers in the Online Safety (Miscellaneous Amendments) Bill.[814] The bill took effect in February 2023.[815] The bill requires large "online communications services" ("OCS"), which include social media services, to comply with a Codes of Practice, and empowers the IMDA 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" 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 IMDA 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.[816] The law gives the 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). The Online Criminal Harms Act (OCHA) partially took effect in part on February 1 2024, including "directions to online services to restrict the exposure of Singapore users to criminal activities on their platforms," "orders to limit further exposure to the criminal activities being conducted on platforms of non-compliant online services," and "powers to require information to administer the Act and facilitate investigations and criminal proceedings." The Singapore Police Force has also begun to issue Implementation Directives, pursuant to their

[814] Chia, K., Leck, A. & Lim, R. J. (2022, November 24). *Singapore: Online Safety (Miscellaneous Amendments) Bill passed*. Baker McKenzie. https://www.globalcompliancenews.com/2022/11/24/https-insightplus-bakermckenzie-com-bm-technology-media-telecommunications_1-singapore-online-safety-miscellaneous-amendments-bill-passed-and-expected-to-take-effect-in-2023_11212022; *Online Safety (Miscellaneous Amendments) Bill* [Singapore] Bill No. 28. (2022). https://www.parliament.gov.sg/docs/default-source/default-document-library/online-safety-(miscellaneous-amendments)-bill-28-2022.pdf.

[815] Ang, A. et al. (2023, February 10). *Legislation to tackle harmful content on online serivces accessible to users in Singapore in force*. Allen & Gledhill. https://www.allenandgledhill.com/sg/publication/articles/23174/legislation-to-tackle-harmful-content-on-online-services-accessible-to-users-in-in-force.

[816] Koh, C. L. (2023, August 21). *Singapore passes Online Criminal Harms Act*. Osborne Clark. https://www.osborneclarke.com/insights/singapore-passes-online-criminal-harms-act; *Online Criminal Harms Act*, [Singapore] Bill No. 17. (2023). https://www.parliament.gov.sg/docs/default-source/default-document-library/online-criminal-harms-bill-17-2023.pdf.

powers as the competent authority under OCHA, to require a number of specific and prescriptive measures that they believe is required in order to combat scams.

On 15 October 2025, the Ministry of Digital Development and Information introduced the Online Safety (Relief and Accountability) Act for First Reading in Parliament.[817] The bill, expected to be enacted by the end of 2025 with implementation measures unfolding through 2026, establishes new statutory torts enabling victims of online harms—including online harassment, doxing, stalking, intimate image abuse, and image-based child abuse—to pursue civil action against perpetrators and seek remedies through the courts. To strengthen enforcement, the law will create a new Online Safety Commission (OSC), scheduled to begin operations in the first half of 2026, which will serve as a centralized body to assist victims, particularly those targeted by cyberbullying, deepfakes, and the non-consensual sharing of intimate images. The OSC will be empowered to issue directives to online platforms requiring the prompt removal of harmful content, demand identity information of end-users suspected of causing online harm, or instruct platforms to take further reasonable steps to collect additional identifying information. Together, these measures mark a significant expansion of state authority in content moderation and liability frameworks for online harms and thus warrant close monitoring.

South Africa

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

On May 31, 2024, the Ministry of Communications and Digital Technologies published the National Data and Cloud Policy.[818] The Policy stipulates that "data that incorporates content pertaining to the protection and preservation of national security and sovereignty of the Republic shall be stored only in digital infrastructure located within the borders of the Republic." The scope of covered data remains unclear, and industry is concerned the policy could be interpreted in such a manner that companies are required to locally store wide sets of data to operate in the market[819]

[817] *Online Safety (Relief and Accountability) Bill* [Singapore] Bill No. 18. (2025). https://www.parliament.gov.sg/docs/default-source/bills-introduced/online-safety-(relief-and-accountability)-bill-18-2025.pdf?sfvrsn=4cda5d08_1.
[818] *Electronic Communications Act* [South Africa] Act No. 36. (2005). https://www.gov.za/sites/default/files/gcis_document/202406/50741gen2533.pdf.
[819] iAfrikan. (2023, June 4). *South Africa publishes Data & Cloud Plan to enhance Data Sovereignty*. https://iafrikan.com/sa-published-cloud-plan/.

Forced Revenue Transfer for Digital News

On July 11, 2025, the South African government published an updated draft White Paper on regulating Audio and Audiovisual Media Services and Online Content Safety.[820] The White Paper sets out broad policy proposals and guiding principles intended to inform the development and implementation of a regulatory framework to address existing legislative gaps that have emerged in response to the growth of global streaming platforms, user-generated content, and non-linear media consumption. The White Paper proposed the introduction of a licensing fee for online platforms, the nature of which will be determined by the Independent Communications Authority of South Africa (ICASA) during the first stage of implementation of the White Paper's recommendations. The White Paper also requests ICASA to consider whether to introduce local content quotas.

In February 2025, the South Africa Competition Commission released its provisional report on the Media and Digital Platforms Market Inquiry.[821] The report contains findings and draft remedies, including a 1% copyright levy, mandatory annual payments from American companies to publishers for linking to their news stories, and a 5-10% digital levy on digital advertising revenues, should the covered companies fail to implement the identified remedial actions. Overall, the report significantly distorts the business model of online news and the role digital services play in the online information ecosystem.[822] Given the focus of the report and in anticipation of the release of the finalized proposed remedies, industry remains concerned and urges the U.S. government to continue to push back on the report and future action.

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.[823] The threshold for applicability is global annual sales of €750 million, with a local threshold of €3 million. From 2021 through 2024, Spain has extracted over US$1 billion from

[820] *Invitation for Public Comments on the Draft White Paper on Audio and Audiovisual Media Services and Online Safety* [South Africa] Notice 3369. (2025). https://www.gov.za/sites/default/files/gcis_document/202507/52972gen3369.pdf.
[821] South Africa Competition Commission. (2025). *Media and Digital Platforms Market Inquiry (MDPMI)*. https://www.compcom.co.za/wp-content/uploads/2025/02/CC_MDPMI-Provisional-Report_Non-Confidential-Final.pdf.
[822] CCIA. (2025). *Provisional Report Targets U.S. Companies and Faults Digital Services for Shift in News Consumption*. https://ccianet.org/wp-content/uploads/2025/03/Provisional-Report-Targets-U.S.-Companies-and-Faults-Digital-Services-for-Shift-in-News-Consumption-1.pdf.
[823] Office of the U.S. Trade Representative. (2021). *Section 301 Investigation Report on Spain's Digital Services Tax*. https://ustr.gov/sites/default/files/files/Press/Releases/SpainDSTSection301Report.pdf.

this tax, mostly, it is estimated, from U.S. firms. [824] U.S. companies were cited throughout legislative debate on the legislation making the targets clear.[825] Spain was among the countries that imposed a DST with whom the United States reached an interim agreement premised on progress on the OECD Pillar 1 solution.[826] Given stalled progress on Pillar 1, and the Section 301 finding of discriminatory and unreasonable burdens, USTR should reconsider whether additional steps are necessary to facilitate removal of this tax.

Sri Lanka

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In 2022, Sri Lanka enacted a data protection law modeled on the EU General Data Protection Regulation, though the law has not yet been operationalized.[827] Section 26 of the Act creates significant barriers to the use of cloud services located outside the country by both private companies and government entities, effectively protecting and privileging the country's two expensive Tier 3 data centers (operated by incumbent telcos). Once the Act enters into force, reliance on widely used cloud services will become legally and procedurally complicated for entities domiciled, resident, or incorporated in Sri Lanka, requiring legal reviews and complex approvals for what are currently routine digital operations. Given that cloud services are now the default infrastructure for most applications, requiring legal clearance for such standard actions is both impractical and burdensome. These excessive procedural requirements will drive up costs for data processors and controllers. While large corporations may be able to absorb these costs,

---

[824] CCIA. (2025). *Status of Key Digital Services Taxes in July 2025*. https://ccianet.org/library/status-of-key-digital-services-taxes-in-july-2025/.

[825] Congress of Spain. (2020, June 4). *Daily Sessions of Congress of the Plenary Members and Permanent Membership*, 2020 XIV Legislature No. 26. 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).]).

[826] U.S. Department of the Treasury. (2021, October 21). *Joint Statement form 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*. https://home.treasury.gov/news/press-releases/jy0419.

[827] *PERSONAL DATA PROTECTION ACT* [Sri Lanka] No. 9. (2022). https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf.

often through in-house legal teams, the compliance risks and financial burden will fall disproportionately on startups and MSMEs, for whom legal fees and delays represent a much larger share of overall operating costs. Moreover, unless the planned amendments are adopted, it will be virtually impossible for government entities to use cloud services offered by global providers, undermining efficiency, innovation, and digital transformation efforts across the public sector.

Government-Imposed Content Restrictions and Related Access Barriers

Sri Lanka certified its Online Safety Act on February 1, 2024,[828] a law widely viewed as being introduced with mala fide intent to shield politicians from criticism on online platforms. The Act criminalizes the communication of "false statements" and empowers the yet-to-be-activated Online Safety Commission to determine what is true or false, raising serious concerns about unchecked government authority. Violations are punishable by up to five years in prison and/or a fine of up to five hundred thousand rupees. The law also allows the Commission to order internet service providers and intermediaries to remove posts declared "prohibited statements." Although the Commission has not yet been activated pending amendments to the Act, at least six cases have already been initiated directly with the courts, with only one concluded. The vague definitions of offenses, overly broad information-gathering powers, and impractical procedures heighten the risk of arbitrary enforcement, particularly against U.S. service providers, which are active in the market and are especially vulnerable in a context with a documented history of abuse of process by the government. The law has drawn strong condemnation from industry associations, the UN Office of the High Commissioner for Human Rights, and organizations such as Amnesty International, which called it a "major blow to human rights" and a tool that could be "used to undermine freedom of expression and suppress dissent." Although the government has initiated a reform process, it is being led by the same officials who drafted the original law, making meaningful change unlikely without strong external intervention, including from USTR.

Taxation of Digital Products and Services

Sri Lanka has announced the introduction of an 18 percent VAT on digital services supplied in the country by non-resident entities, scheduled to take effect in April 2026.[829] The tax will apply to a wide range of digital services, including music and video streaming, apps, online gaming, e-learning, search engines, online advertising, SaaS and cloud software, and ride- and home-sharing platforms. The draft implementation framework was developed without adequate industry consultation and lacks clarity on critical issues such as compliance procedures, registration requirements, and alignment with existing tax law. Although the rate mirrors what

[828] *Online Safety Act* [Sri Lanka] No. 9. (2024). https://www.parliament.lk/uploads/acts/gbills/english/6311.pdf.
[829] Kovacs, E. (2025, September 12). *Sri Lanka Imposes 18% VAT on Cross-Border Digital Services Provided via Electronic Platforms*. Fonoa. https://www.fonoa.com/resources/blog/sri-lanka-imposes-vat-cross-border-digital-services.

applies to domestic entities, the absence of clear guidance raises concerns about legal uncertainty and increased administrative burden. Industry stakeholders have called for greater transparency and structured dialogue to ensure the framework supports tax compliance without creating unnecessary market access barriers.

Switzerland

Threats to the Security of Devices and Services

In January 2025, the Swiss Federal Council launched a public consultation on a partial revision of the Telecommunications Surveillance Ordinances to clarify cooperation obligations for telecommunications and communications service providers and to adapt regulatory requirements to evolving technologies.[830] The proposal introduces a three-tier obligation system for "derived communications service providers" (including cloud service providers) based on user volume (starting at 5,000 users) and revenue thresholds (with full obligations applying above CHF 100 million), and would require expanded data retention, user identification capabilities, and technical surveillance interfaces that could undermine encryption protections. The draft has been met with broad opposition in public consultation, including from all major political parties, leading industry associations, and prominent Swiss startups, several of which have threatened to relocate over privacy and compliance concerns. For U.S. cloud providers, the proposed revision would impose significant new operational burdens in Switzerland, including the need to build costly compliance infrastructure, implement expanded data retention measures, and potentially weaken encryption, creating both privacy risks and market access challenges.

Taiwan

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In August 2023, the Financial Supervisory Commission (FSC) published 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.[831] 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

[830] Swiss Federal Chancellery. (2025, February 3). *Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)*. https://www.fedlex.admin.ch/eli/fga/2025/335/de.
[831] Financial Supervisory Commission Republic of China (Taiwan). (2023, August 4). *FSC announces the amendment of Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation.*
https://www.fsc.gov.tw/en/home.jsp?id=54&parentpath=0,2&mcustomize=multimessage_view.jsp&dataserno=202308180003&dtable=News.

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 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.

Industry reports 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 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 must bear over-burdensome documentary requirements that may cause unnecessary compliance costs; even if an institution is willing to bear the burden, the review process is lengthy and unpredictable; and, the institution still needs to maintain a local copy of "important" data.

Regulations have been promulgated in both the financial services and health industries advancing data localization requirements. For financial services, industry reports that regulations require that material financial customer data be stored in Taiwan, unless the regulatory agency grants an exemption. In the healthcare sector, regulations governing Electronic Medical Records Management mandate that medical data remain stored in Taiwan absent an exemption. For both types of data, industry is left with vague and unclear regulations delineating the process for obtaining an exemption.

Through a September 2023 draft amendment to the Cybersecurity Management Act sectoral regulators would be directed to adopt rules delineating the criteria and the procedure behind the labeling 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.

Forced Revenue Transfers for Digital News

Separately, legislators in Taiwan have introduced proposals to the Legislative Yuan to establish a mandatory news bargaining code, with the legislative process advancing without meaningful industry or public consultation.[832] Opposition parties have prioritized the bill, creating a significant risk of enactment of a measure that would impose mandatory revenue transfers from digital service providers to local news businesses. This legislative initiative overlooks the substantial, voluntary contributions and investments that digital platforms have already made to support a sustainable news ecosystem in Taiwan, including multi-year co-prosperity funds, capacity-building initiatives, and digital skills training programs to help local news organizations adapt to the digital environment. Such a law would not only disregard these efforts but also establish a discriminatory and trade-distortive framework, imposing targeted costs on foreign digital services while solely benefiting domestic media interests. This proposal would constitute a discriminatory trade barrier and industry urges the U.S. government to continue opposing its enactment and to encourage Taiwan to pursue collaborative, market-based approaches that strengthen the news ecosystem without undermining digital trade.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

On July 31, 2024 the Fraud Crime Harm Prevention Act was enacted and promulgated into law.[833] Under the Act, four select online advertising platform operators (including two American companies) were designated to be subject to onerous anti-fraud obligations. The Fraud Crime Harm Prevention Act imposes serious compliance burdens on industry, including penalties imposed by the Ministry of Digital Affairs for not complying with content removal requirements, stringent verification and disclosure requirements regarding advertisers on their platforms, and ad transparency requirements such as advertisers' use of generative AI in ads. This rushed legislative process, burdensome requirements and uncertain enforcement could act as a non-tariff trade barrier, discouraging foreign investment and participation in Taiwan's digital economy.

Taiwan's current approach to intermediary liability is creating a significant trade barrier by systematically eroding safe harbor protections, departing from established democratic and international best practices. Instead of adopting a clear, predictable legal framework, the government has taken a sectoral approach that effectively imposes strict liability on platforms for user-generated content. This framework forces digital services to pre-screen and censor user content, producing an untenable operating environment and chilling free expression online. A stark example of this flawed model is the Tobacco Hazards Prevention Act, which aims to regulate illicit sponsored content but fails to assign liability to the actual content creator, the

[832] Shan, S. (2023, May 23). MODA to create model for news media bargaining act. *Taipei Times.* https://www.taipeitimes.com/News/taiwan/archives/2023/05/23/2003800275.
[833] *Fraud Crime Hazard Prevention Act* [Taiwan]. (2024). https://law.moj.gov.tw/ENG/LawClass/LawHistory.aspx?pcode=D0080226.

party responsible for advertising. Instead, it improperly shifts legal responsibility to intermediary platforms, defining sponsored posts as commercial "advertisements" and mandating pre-screening of all user content against an ever-expanding list of keywords, exposing platforms to repeated and severe fines for content they did not create. This approach ignores the critical distinction between paid advertising and organic user-generated content, compelling platforms to implement costly and intrusive censorship systems. As a result, it functions as a non-tariff barrier to trade, normalizes speech-filtering mechanisms that are inconsistent with a free and open internet, undermines cross-border data flows essential to U.S. business interests (including for AI model training), and hinders the growth of a vibrant digital public sphere. Industry urges USTR to press Taiwan to adopt a coherent intermediary liability framework with clear safe harbor provisions that correctly assign liability to the originator of illegal content, rather than the intermediary.

Restrictions on Cross-Border Data Flows

The recent initiative by Taiwan's Personal Data Protection Committee Preparatory Office to develop a unique, domestic set of Standard Contractual Clauses (SCCs) for cross-border data transfers raises serious concerns for U.S. and other foreign investors. By pursuing a bespoke SCC framework that is incompatible with established international standards, Taiwan risks creating a fragmented and legally uncertain data transfer environment, imposing significant compliance burdens on companies operating across borders. Rather than facilitating secure and trusted data flows, such a localized SCC regime would undermine interoperability and fragment the digital economy, forcing multinational companies that rely on globally integrated systems to adopt costly, duplicative contractual arrangements. This would not only deter investment but also create operational inefficiencies that disadvantage both domestic and foreign businesses. The U.S. government should urge Taiwan to adopt flexible and internationally aligned cross-border transfer mechanisms. Prescriptive SCC templates should not be a prerequisite for data transfers where parties already have contractual arrangements or binding corporate policies ensuring that transferees uphold protections comparable to the transferor's jurisdiction. Embracing a flexible, risk-based approach would enable data controllers to operate safely, efficiently, and interoperably across jurisdictions, supporting U.S. investment and promoting sustainable digital trade.

Tanzania

Government-Imposed Content Restrictions and Related Access Barriers

In October 2023, the Communications and Regulations Authority (TCRA) imposed a VPN-ban, requiring firms and individuals using VPNs to declare their use to the government and provide the TCRA with IP addresses, with non-compliance facing fines of US$2,000 and potential prison

sentences.[834] The TCRA imposed the ban under Regulation 16(2) of the Electronic and Postal Communications (Online Content) Regulations of 2020, which prevents Tanzanians from accessing "illegal" content.

The government has escalated blocks on social media platforms and specific accounts. In August 2024, amidst political unrest and following months of pressure by lawmakers of the ruling CCM Party,[835] the government moved to compel ISPs to block access to the platform X across the country.[836] In October 2024, the TCRA compelled social media platforms to suspend the accounts of a local media company for publishing "restricted content" regarding recent political unrest.[837]

In August 2025, widespread and intermittent ISP-based blocking of some social media and sites was detected.[838] This was reportedly linked to ongoing broader government restrictions on speech in the run up to general elections in October 2025.

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.[839] 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.

[834] Namunwa, K. (2023, October 15). *Tanzania Imposes Ban On VPN Usage Without A Permit*. CIO Africa. https://cioafrica.co/tanzania-imposes-ban-on-vpn-usage-without-a-permit/.
[835] The Chanzo Initiative. (2024, June 11). *Political Heat on X (Twitter) Forces Ruling Party Supporters to Call for App Ban in Tanzania, Citing Pornography*. https://thechanzo.com/2024/06/11/political-heat-on-x-twitter-forces-ruling-party-supporters-to-call-for-app-ban-in-tanzania-citing-pornography/.
[836] Sunny, D. (2024, August 30). *Tanzania reportedly blocks access to X amid political tension*. TechPoint. https://techpoint.africa/2024/08/30/tanzania-reportedly-blocks-x/.
[837] *Reuters*. (2024, October 3). Tanzania suspends media company's online platforms for 30 days. https://www.reuters.com/world/africa/tanzania-suspends-media-companys-online-platforms-30-days-2024-10-03/.
[838] Tech & Media Convergancy. (2025, October 9). *Censorship, Surveillance, and Digital Freedoms: Navigating Tanzania's Online Space Ahead of the 2025 General Election*. https://tmc.co.tz/censorship-surveillance-and-digital-freedoms-navigating-tanzanias-online-space-ahead-of-the-29-october-2025-general-election/.
[839] Sinaj, K. (2023). *Will 2023 See Higher Digital Service Subscription Costs?* PwC. https://www.pwc.co.tz/press-room/will-2023-see-higher-digital-service-subscription-costs.html.

Thailand

Asymmetric Platform Regulation

The Royal Decree on Digital Platform Services (B.E. 2565)[840] came into effect on August 20, 2023, and requires relevant services to notify the government prior to starting business operations, with large-scale services subject to additional requirements such as mandatory risk management systems and internal compliance managers. The Decree, inspired by the EU's Digital Services Act, is overly broad beyond the authority of the government and does not recognize different platforms' business models. It also imposes burdensome obligations and liabilities on businesses, such as mandating local representatives with unlimited liability, reporting requirements, and broad authority for the Electronic Transactions Development Agency (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 users' and advertisers' merchant ID verification, but has failed to provide further details, creating uncertainty. Industry reports the government is considering making verification mandatory through the Thai National ID System. On July 9, 2025, the Royal Gazette published a list of 19 digital platforms (including one U.S. firm) required to comply with Section 20 of the Royal Decree on the Operation of Digital Platform Service Business, effective July 10.[841] Under Section 20, designated platforms must conduct business risk assessments and implement risk management frameworks for activities involving the sale or advertisement of products governed by regulatory standards and considered critical to economic and financial stability. Additionally, ETDA has been considering expanding the scope of the Royal Decree by classifying digital platforms as online marketplaces under an overly broad definition of e-commerce. This expanded scope could encompass advertising, social media, and user-generated content, even in cases where no e-commerce transactions occur, significantly exceeding the original intent of the regulation. Such an approach would unfairly impact companies whose business models center on digital advertising or other non-transactional services. U.S. firms brought under this scopew ill face extensive and burdensome compliance obligations, including. for activities that are not considered e-commerce under international best practices. The list of designated platforms will be reviewed annually, creating ongoing regulatory uncertainty for affected services.

Thailand announced its intention to develop a Platform Economy Act in January 2024.[842] The Draft PEA seeks to regulate and standardize digital platform service business operations. If the

---

[840] *ROYAL DECREE ON THE OPERATION OF DIGITAL PLATFORM SERVICE BUSINESSES THAT ARE SUBJECT TO PRIOR NOTIFICATION* [Thailand] B. E. 2565. (2022). https://www.etda.or.th/getattachment/Regulator/DigitalPlatform/law/Clean-Royal-Decree-on-DP-Corrected-1.pdf.aspx?lang=th-TH.

[841] *The Nation*. (2025, July 10). ETDA names 19 online shopping platforms as having risks to cause public damage. https://www.nationthailand.com/business/trade/40052399.

[842] Buranatrevedhya, K. et al. (2024, June 26). Thailand: Impact assessment concerning laws on platform services commissioned by the Electronic Transactions Development Agency. *Baker McKenzie*.

Draft PEA becomes law, it will supersede other existing laws, such as the Royal Decree on the Operation of Digital Platform Service Businesses that are subject to Prior Notification B.E. 2565 of 2022 and the relevant provisions under the Electronic Transactions Act B.E. 2544 of 2001. The Draft PEA reflects strong influences of the EU's Digital Services Act (DSA) and Digital Markets Act (DMA). Stakeholders have identified numerous problematic elements in the draft.[843] Although the draft was officially put on hold by the previous Cabinet on April 8, 2025, the new government announced in Parliament its policy to propose legislation relevant to the digital platform economy on September 29, 2025. As such, industry recommends the U.S. government monitor the relevant legislative developments to ensure any subsequent regulations do not distort digital competition or discriminate against U.S. online service suppliers.

On July 15, 2025, the Trade Competition Commission of Thailand (TCCT) released its draft Guidelines on the Consideration of Unfair Trade Practices and Conduct Constituting Monopoly, Reducing Competition, or Restricting Competition in Multi-Sided Platform Businesses in the Category of Digital Platforms for the Sale of Goods or Services (E-commerce).[844]The draft provides the first detailed framework for how TCCT intends to interpret and enforce the substantive provisions of the Trade Competition Act against digital platforms, acknowledging their unique network effects and the need for complex competition analysis. This development is expected to have a profound impact on the operations of e-commerce platforms, sellers, and associated service providers in Thailand. Affected platforms have already raised concerns regarding the need for proportionate algorithmic transparency aligned with international practice, recognition of legitimate operational requirements (such as logistics and payment solutions), and flexibility in designing transparent and non-discriminatory fee structures. The guidelines are anticipated to be enacted in the near future, signaling a more interventionist regulatory posture toward foreign digital platforms.

On October 6, 2025, the Minister of Digital Economy and Society (MDES), Chaichanok Chidchob, announced the Ministry's urgent policy priorities for addressing perceived economic threats. [845] MDES underscored its role in supporting local SMEs and entrepreneurs, with a particular focus on tackling what it characterized as "monopolization by big platforms" and unfair trade competition. As part of this agenda, the Ministry is considering the introduction of

---

https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/thailand-impact-assessment-concerning-laws-on-platform-services-commissioned-by-the-electronic-transactions-development-agency; Chitranukroh, A. et al. (2024, January 30). *Thailand Issues Draft Platform Economy Act*. Tilleke & Gibbins. https://www.tilleke.com/insights/thailand-issues-draft-platform-economy-act/.

[843] ITIF. (2024). *Comments of ITIF Before the Electronic Transactions Development Agency (EDTA) in the Matter of the Draft Digital Platform Economy Act*. https://www2.itif.org/2024-thailand-pea-english.pdf.

[844] *The Nation*. (2025, September 17). TCCT to introduce new rules to curb e-commerce giants, protect small retailers. https://www.nationthailand.com/business/economy/40055547.

[845] *The Nation*. (2025, September 27). New DES Minister Vows Tech Overhaul to Slash Fees and Fight Disasters. https://www.nationthailand.com/news/policy/40056018.

OTT regulation aimed at imposing tax obligations on international digital platforms operating in Thailand.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In 2025, Thailand's Digital Government Development Agency (DGA) released two draft sets of guidelines, the Government Cloud Usage Guidelines and the Cloud Data Classification Guidelines, intended to direct public agencies toward greater adoption of cloud technology under the national "Go Cloud First" policy.[846] While the policies signal a strategic shift toward higher cloud adoption, the standards outlined impose strict data residency requirements, mandating that most government and regulated data must be stored within Thailand, with only limited cross-border exceptions subject to DGA approval and the construction of a local data center. Similar restrictions are reflected in the National Cybersecurity Agency's Cloud Security Guidelines, which reinforce these localization measures. These obligations risk limiting the ability of U.S. cloud service providers to offer services in Thailand if they are unable to maintain a local presence. Furthermore, the draft "Go Cloud First" policy explicitly states that the top two tiers of government data—Secret and Top Secret—may only be served by a state-owned enterprise, effectively excluding foreign providers from a critical segment of the cloud services market.

Despite the policy intent of increasing cloud adoption and accelerating digital transformation, the proposed guidelines instead create market access barriers for foreign cloud providers by imposing restrictive data localization and sovereignty requirements. The prohibition on storing protected or highly protected government data abroad, except under narrow DGA-approved exemptions, effectively blocks most cross-border cloud services from participating in public sector projects. Even where data in transit or temporary processing outside Thailand may be technically permitted, the default expectation remains domestic storage, leaving international vendors at a disadvantage unless they establish local infrastructure subject to government oversight. Furthermore, the requirement that providers comply with domestic procurement rules, achieve government-mandated certifications, and demonstrate conformity with Thai security standards will raise compliance costs and exclude providers that rely on global or regional data management models. These rules not only restrict competition and deter foreign participation in Thailand's public sector cloud market, but also risk fragmenting the digital ecosystem by forcing data silos and limiting the ability of cross-border services to operate at scale.

[846] Aw, C. & O'Leary, C. (2025, August 18). *Thailand releases draft guidelines on government cloud adoption and data classification*. Hogan Lovells. https://www.hoganlovells.com/en/publications/thailand-releases-draft-guidelines-on-government-cloud-adoption-and-data-classification.

Government-Imposed Content Restrictions and Related Access Barriers

CCIA has previously raised concerns with the Computer Crime Act, amended in 2016.[847] 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.[848] The regulation adopted a broad definition of "National Security" to cover a wide range of content for which the government seeks the power to demand takedowns.

In 2019, Thailand passed a controversial Cybersecurity Law following amendments in 2018. Industry has criticized the law due to provisions that enable government surveillance.[849] Under the new law, officials are granted authority to "search and seize data and equipment in cases that are deemed issues of national emergency."[850]

The Emergency Decree on Cybercrimes, passed in 2025 [851] and now coming into effect, makes Thailand one of the first markets in the Asia-Pacific region to assign liability to digital platforms for online scams. Under the decree, online platforms can be held legally responsible for damages caused by fraudulent activities if they fail to implement regulator-prescribed fraud prevention measures. Current obligations include removing identified fraud and scam content within 24 hours of notification by the Ministry of Digital Economy and Society (MDES) and promptly reporting the outcomes, with the possibility of additional requirements to be introduced in the future. The amount of damages remains undefined and will be determined based on the extent of harm suffered by victims, creating significant legal and compliance uncertainty for affected platforms.

Restrictions on Cross-Border Data Flows

The Personal Data Protection Act went into effect on June 1, 2022.[852] As a general matter, the law applies to *all* entities that collect, use, or otherwise share personal data in Thailand or of

---

[847] CCIA. (2022). *Comments of the Computer & Communications Industry Association Regarding Foreign Trade Barriers to U.S. Exports for 2023 Reporting.* https://ccianet.org/wp-content/uploads/2022/10/CCIA-Comments-2023-National-Trade-Estimate-Reporting.pdf.
[848] Freedom House. (2024). *Freedom on the Net 2023: Thailand*. https://freedomhouse.org/country/thailand/freedom-net/2023; *The Nation*. (2021, December 29). Over a million pieces of fake news posted online in two years. https://www.nationthailand.com/in-focus/40010570.
[849] TechDirt. (2019, March 11). *Thailand Decides To Make Its Terrible Cybersecurity Law Even Worse*. https://www.techdirt.com/2019/03/11/thailand-decides-to-make-terrible-cybersecurity-law-even-worse/.
[850] *TechCrunch*. (2019, February 28). Thailand Passes Controversial Cybersecurity Law. https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/.
[851] Vero. (2025, April 18). *Vero Advocacy Brief: Thailand Enacts New Technology Crime Laws*. https://vero-asean.com/vero-advocacy-brief-thailand-enacts-new-technology-crime-laws.
[852] Phakdeetham, J. (2022, June 1). Explainer: What is PDPA, Thailand's new data law? *Bangok Post.* https://www.bangkokpost.com/business/2319054/explainer-what-is-pdpa-thailands-new-data-law-; PWC. (n.d.). *Thailand's Personal Data Protection Act (PDPA): are companies in Thailand ready?* https://www.pwc.com/th/en/tax/personal-data-protection-act.html; Hunton. (2022, June 1). *Thailand's Personal*

residents of the country, with no restrictions regarding their standing under Thai law or where they 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 they decline to establish a business presence in Thailand but have Thai individuals who use their services.[853]

Other Barriers to Digital Trade

In 2025, the ETDA announced plans to implement a new logistics regulation for e-commerce marketplaces that would require platforms to provide customers and sellers with at least three logistics carrier options for deliveries.[854] ETDA aims to implement the regulation by December 2025, although the draft has not yet been released publicly, and a call for public comments is expected soon. Notably, ETDA has already consulted five local logistics carriers behind closed doors, raising concerns about transparency and the potential for discriminatory market access conditions. If adopted in its current form, the measure could increase operational complexity and compliance costs for international platforms while giving domestic logistics providers a competitive advantage, thereby limiting flexibility in supply chain operations and potentially affecting foreign e-commerce providers' ability to compete effectively in the Thai market.

Türkiye

Asymmetric 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 service providers and intermediary service providers.[855] 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," as defined by their annual gross revenue, number of Turkish users, and qualitative criteria, 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

Data Protection Act Enters into Force. https://www.huntonprivacyblog.com/2022/06/01/thailands-personal-data-protection-act-enters-into-force/.

[853] DLA Piper. (n.d.). *Data protection laws in Thailand.* https://www.dlapiperdataprotection.com/index.html?t=law&c=TH.

[854] *The Nation*. (2025, August 25). Thailand to Force E-commerce Platforms to Offer Choice of Delivery Firms. https://www.nationthailand.com/business/tech/40054468.

[855] Balki, B. et al. (2022, October 25). *A New Age for Digital Markets in Turkey? The Draft Amendment to the Law No. 4054 on the Protection of Competition*. Kluwer Competition Law Blog. https://legalblogs.wolterskluwer.com/competition-blog/a-new-age-for-digital-markets-in-turkey-the-draft-amendment-to-the-law-no-4054-on-the-protection-of-competition/.

obstruct U.S. services suppliers' operations in Türkiye.[856] [857]Türkiye intends to finalize this law by as early as the end of 2025.

Certain obligations included in the draft law 4052 were adopted in the Regulation of E-Commerce Law, which took effect January 1, 2024.[858] The law prohibits e-commerce intermediary service providers from selling their own trademarked goods on their platform. It imposes additional obligations on larger providers, with those with an annual net transaction volume greater than ₺10 billion (US$538.3 million) prohibited from using data collected to compete with other providers, and those with an annual net transaction volume greater than ₺60 billion (US$3.3 billion) prohibited from expanding into industries such as payments, transportation, and delivery as separate business models. Moreover, it imposes new taxes on companies based on their revenues, while providing relief for Turkish-headquartered e-commerce companies.[859] These excessive regulatory requirements, *de facto* preference for Turkish companies, and pressures for localization represent clear barriers for U.S. companies.

Government-Imposed Content Restrictions and Related Access Barriers

Türkiye remains one of the most restrictive markets for internet services and continues to utilize censorship tools to limit online speech.[860] CCIA has previously identified laws that preemptively block websites on vague grounds and specific instances of blocking by Turkish authorities.[861] The Turkish government's aggressive treatment of U.S. digital services imposes economic harms—the U.S. International Trade Commission report estimated that US$14.6 million was lost in Türkiye after it blocked several U.S. services in early 2020.[862]

---

[856] CCIA. (2022). *CCIA Comments on the Draft Amendment to Law No. 4054 of the Protection of Competition in Turkey*. 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.
[857] Doğan, C. (2024, August 15). *Turkish DMA: What's in the Package?* Kluwer Competition Law Blog. https://competitionlawblog.kluwercompetitionlaw.com/2024/08/15/turkish-dma-whats-in-the-package/.
[858] Sozer, C. (2023, January 2). *New E-Commerce Regulation Published*. Esin. https://www.esin.av.tr/2023/01/02/24398/.
[859] U.S. Department of State. (2024). *2024 Investment Climate Statement: Turkey*. https://www.state.gov/reports/2024-investment-climate-statements/turkey/.
[860] Freedom House. (2023). *Freedom on the Net 2023: Türkiye*. https://freedomhouse.org/country/turkey/freedom-net/2023.
[861] de Cramer, A. (2020, September 11). Silence descends on social media in Turkey. *Asia Times*. https://asiatimes.com/2020/09/silence-descends-on-social-media-in-Türkiye/; CCIA. (2018). *CCIA Comments to the U.S. Trade Representative for the 2019 National Trade Estimate*. https://www.ccianet.org/wp-content/uploads/2018/10/CCIA-Comments-to-USTR-for-2019-NTE.pdf;
Reporters Without Borders. (2014, August 28). *Türkiye, Enemy of the Internet.* http://rsf.org/en/Türkiye-enemy-internet; *Wall Street Journal.* (2014, April 1). Google, Others Blast Türkiye Over Internet Clampdown. http://online.wsj.com/articles/SB10001424052702303978304579473190997035788; Türkiye Blocks. (2017, June 5). *Major Internet Access Issues in Türkiye as Cloudflare Knocked Offline*. https://Türkiyeblocks.org/2017/06/05/major-internet-access-issues-Türkiye-cloudflare-knocked-offline/.
[862] United States International Trade Commission. (2022). *Foreign Censorship, Part 2: Trade and Economic Effects on U.S. Businesses*. https://www.usitc.gov/publications/332/pub5334.pdf.

In July 2020, the Turkish Parliament passed Law No. 7253 amending the Law on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications,[863] granting the government sweeping new powers to regulate content on social media.[864] The law requires social network providers with more than one million daily users to establish a domestic representative office, 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 ensure that the data of Turkish users is stored domestically. The law went into effect October 1, 2020, and authorities have since used it to target U.S. firms, imposing fines,[865] advertising bans, and bandwidth restrictions within months.[866]

On October 13, 2022, the Parliament passed the Amendment of Press Law, and Certain Laws, or Law No. 7418, introducing restrictions on social media providers and firms providing messaging services—with stricter requirements for larger companies—and clamping down on freedom of expression in the name of combatting online disinformation.[867] Law No. 7418 requires platforms to disclose algorithms and users' personal data to the government upon demand, a practice recognized by the U.S. government as potentially infringing on trade secrets.[868] It also establishes new criminal liability for spreading disinformation to "create fear and disturb public order," punishable with up to three years in prison. Penalties for non-compliance with the Law include fines of up to 3% of global revenue and bandwidth throttling of up to 9

A decision published by the ICTA in April 2023 regarding procedures and principles for social network providers came into effect on April 1, 2023, without a transition period, and updates the responsibilities and obligations of social network providers in accordance with Article 4 of Law No. 5651.[869] The decision introduces significant new obligations for social network providers,

---

[863] *Regulation of Publications Made on the Internet and Fighting against Crimes Committed Through Publications Law on Amendment of the Law* [Türkiye] No. 7253. (2020, July 29). https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm

[864] Santora, Marc. (2020, July 29). Türkiye Passes Law Extending Sweeping Powers Over Social Media. *The New York Times.* https://www.nytimes.com/2020/07/29/world/europe/Türkiye-social-media-control.html.

[865] Wilks, A. (2020, November 4). Türkiye Fines Social Media Giants for Breaching Online Law. *AP News*. https://apnews.com/article/business-Türkiye-media-social-media-560de2b21d54857c4c6545c1bd20fc25.

[866] Sezer, C & Butler, D. (2021, January 19). Türkiye Slaps Ad Ban in Twitter Under New Social Media Law. *Reuters*. https://www.reuters.com/article/us-Türkiye-twitter/Türkiye-slaps-ad-ban-on-twitter-under-new-social-media-lawidUSKBN29O0CT.

[867] *Amendment of Press Law, and Certain Laws* [Türkiye] Law No. 7418. (2022). https://www.tbmm.gov.tr/Yasama/KanunTeklifi/316898; *BiaNet*. (2022, May 27). AKP MHP Proposes Amendment to Press Law Introducing Prison Sentences for Disinformation. https://m.bianet.org/english/freedom-of-expression/262461-akp-mhp-propose-amendment-to-press-law-introducing-prison-sentences-for-disinformation.

[868] U.S. Department of State. (2024). *2024 Investment Climate Statement: Turkey*. https://www.state.gov/reports/2024-investment-climate-statements/turkey/.

[869] Okumus, B. Y. & Ozturk, S. (n.d.). *New Regulation from ICTA on Social Network Providers*. Lexology. https://www.lexology.com/library/detail.aspx?g=a799c704-d8c6-4235-a0cc-2f40dc78d586; Moroglu, E. S. & Necipoglu, C. (n.d.). *Information Technologies and Communication Authority Published the Regulation Amedning the Regulation on the Procedures and Principles regarding the Registered Electronic Mail System*. Lexology. https://www.lexology.com/library/detail.aspx?g=43c9b557-836e-444a-b86c-56c7bfc5f278.

holding them legally responsible for user-generated content. Any provider accessed more than 1 million times daily from Türkiye must appoint a local representative, respond to content-related applications, report to the ICTA on decisions to remove or block access to content and on applications submitted by individuals, create an advertising library, and store user data domestically in Türkiye. Furthermore, all social network providers are required to: inform judicial authorities about content related to specified crimes; provide separate services for children; protect user rights; establish effective mechanisms for removing unlawful or harmful content; share information with law enforcement regarding content that may endanger life, property, or public safety; submit requested information and documents to the ICTA; and develop a crisis response plan for emergencies affecting public safety and public health. The framework also sets out detailed sanctions for non-compliance, including administrative fines determined by the nature and frequency of the breach, as well as advertising bans for repeated violations.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Turkish government continues to advance laws pressuring companies to localize data, and measures formally aimed at government data and sensitive personal data have been scoped to potentially include all private user data, implicating a wide range of digital companies. As a result, several U.S. firms have left the Turkish market.[870]

In 2019, a Presidential Circular on Information and Communication Security Measures imposed localization requirements on government workloads determined to be "strategic."[871] 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 Türkiye 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.[872] The Regulation establishes a framework for use of cloud services as an outsourced service, but only applies to services located in Türkiye.

---

[870] U.S. Department of State. (2024). *2024 Investment Climate Statement: Turkey*. https://www.state.gov/reports/2024-investment-climate-statements/turkey/.
[871] *Presidential Circular on Information and Communications Security Measures* [Türkiye] No. 2019/12. (2019). https://cbddo.gov.tr/en/presidential-circular-no-2019-12-on-information-security-measures.
[872] Yilmaz, I. et. al. (2020, March 10). *New Regulation on Bank IT Systems and Electronic Banking Services.* Lexology. https://www.lexology.com/library/detail.aspx?g=820f9766-219b-4196-9554-bfc715fd1676.

Turkey's Law No. 6493 ("Law on Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions")[873] establishes a licensing regime for digital payment providers that imposes strict local establishment and data localization requirements, creating a substantial barrier to market entry for foreign providers. To obtain a license from the Central Bank of the Republic of Turkey (CBRT), any provider—domestic or foreign—must establish a local Joint Stock Company (Anonim Şirketi), meet high capital requirements (e.g., at least TRY 20 million for payment service providers), maintain its corporate headquarters in Turkey, and employ qualified local personnel to ensure full traceability of operations by Turkish authorities. Noncompliance with the licensing requirement is treated as a serious offense, carrying potential imprisonment of one to three years and judicial fines. The most restrictive element of this framework is the data localization mandate, which requires that all information systems—including both primary and backup infrastructure—be physically hosted within Turkey's borders. All documents and records related to transactions must be stored domestically for at least ten years, and outsourcing arrangements, including for cloud computing, are only permitted if the outsourced provider also hosts its systems locally. While recent amendments introduce a narrow exception for cross-border data transfers when one party to a transaction is located abroad, these transfers are subject to strict conditions: the data must continue to be stored domestically, and the CBRT retains full oversight and can suspend or limit transfers if it deems them a security risk. This effectively compels foreign digital payment providers to build costly, redundant infrastructure in Turkey and maintain full data residency for their operations, fragmenting global IT systems and creating significant operational and financial burdens. The combination of mandatory legal presence, capital requirements, and stringent data localization rules results in a de facto barrier to entry for U.S. payment service providers and other foreign digital platforms seeking to operate in the Turkish market.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

Law No. 7418 (detailed above) empowers the ICTA to regulate OTT providers for content moderation. This could render OTT providers responsible for informing ICTA of 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

[873] *LAW ON PAYMENT AND SECURITIES SETTLEMENT SYSTEMS, PAYMENT SERVICES AND ELECTRONIC MONEY INSTITUTIONS* [Türkiye] Law No. 6493. (2013). https://faisalkhan.com/wp-content/uploads/2024/02/Turkey-Law-for-EMI-6493.pdf.

₺30 million (US$1.6 million), throttled service up to a 95% restriction on the usual bandwidth capacity, or outright service blockage.[874]

On March 21, 2025, the ICTA released a consultation proposing sweeping regulations on OTT communication providers, with measures that would effectively subject them to the same regime as legacy telecommunications firms.[875] The draft regulations, if adopted, would require OTT providers to incorporate locally as a Turkish joint-stock or limited company, register for authorization under the Electronic Communications Law, and comply with obligations traditionally tied to providers of physical infrastructure such as wireline and spectrum. Providers would also face mandatory contributions to Türkiye's universal service fund, designed to support services like fixed telephony and emergency maritime communications that OTTs do not provide, and be exposed to vague "public order and national security" obligations that could expand into surveillance or content restrictions. Further, ICTA reserves broad authority to impose penalties, including fines, throttling, or outright blocking, for any non-compliance. By defining OTTs as "interpersonal electronic communication services" above a threshold of one million monthly users, these rules extend a century-old telecommunications framework onto services that operate purely at the application layer, creating regulatory requirements mismatched to their technical and business models.

The policy's most damaging element is its localization requirement, obliging OTT providers to establish a Turkish subsidiary in order to operate legally. Such a rule undercuts the very principle of cross-border services that allows internet-based providers to reach users globally without costly and duplicative local incorporation. While large companies may be able to absorb these burdens, smaller and newer entrants would face prohibitive costs and risks, discouraging innovation and competition. The regulation also leaves providers vulnerable to arbitrary blocking or throttling, giving the government unchecked discretion to restrict services under the guise of protecting "public interest." This framework echoes past policies in Türkiye, such as the 2016 decision that drove PayPal from the market, and stands in tension with Türkiye's binding WTO commitments to allow the cross-border provision of voice services. As drafted, the rules create systemic uncertainty and tilt the playing field in favor of domestic providers, who can more easily satisfy incorporation, licensing, and ownership requirements, while international firms face steep compliance hurdles simply to maintain access to Turkish users.

Beyond incorporation and licensing, the draft rules would force OTT providers to fund telecommunications infrastructure through universal service fees, despite having no role in maintaining networks, and open the door to "network usage fees" by redefining OTT services as

[874] Okumus, B. Y. & Talay, Y. U. (2022, July 21). *New Regulations Expected for OTT Service Providers.* Gün + Partners. https://gun.av.tr/insights/articles/new-regulations-expected-for-ott-service-providers.
[875] Çelik, O. F., Yüksel, B. & Yaldır, N. (2025, April 17). *Traditional Communications vs. OTT: Turkish Regulator Opens Draft OT Secondary Legislation For Public Consultation.* Mondaq. https://www.mondaq.com/turkey/telecoms-mobile-cable-communications/1612592/traditional-communications-vs-ott-turkish-regulator-opens-draft-ot-secondary-legislation-for-public-consultation.

telecom operators subject to interconnection obligations. This not only amounts to a transfer of revenue from international digital service providers to Turkish incumbents, but also threatens to undermine the open internet model, where consumers already pay operators for connectivity. Such a regime risks higher costs, degraded performance, and diminished service availability, as seen in other markets where similar frameworks have been attempted. By compelling OTT services to subsidize infrastructure they do not use, while simultaneously exposing them to surveillance demands, content controls, and the threat of service blocking, Türkiye's proposal would chill investment, weaken consumer choice, and fragment the global digital economy. In short, the draft regulations represent a significant barrier to market access for U.S. and other foreign OTT providers, imposing disproportionate obligations that would curtail competition, innovation, and the open flow of digital services.

Restrictions on Cross-Border Data Flows

The Law on the Protection of Personal Data (Law No. 6698) governs the international transfer of data, which is permitted under the following conditions: (1) when transferring personal data to a country with an 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.[876] Türkiye has still not yet announced a list of countries that meet the standard of adequate level of protection as of 2023.[877] Further, the Data Protection Board has yet to grant approval to companies that have sought the ad-hoc approval. Although industry reports this marks progress regarding cross-border data transfers, full compliance with the EU framework remains incomplete.

Taxation of Digital Products and Services

Türkiye enacted a 7.5% DST that went into effect on March 1, 2020—the highest rate of any major country implementing DSTs. The global revenue threshold for this tax is €750 million, with a local threshold of €20 million. 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 other."[878] Digital service providers that provide the covered services, but

[876] *Law on the Protection of Personal Data* [Türkiye] No. 6698. (2016). https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aea97a33-089b-4e7d-85cb-694adb57bed3.pdf.
[877] Kinikoglu, B. (2023). Implementing a new data protection law: Lessons from the Turkish experience. *International Data Privacy Law, 13*(1), 25–36.
[878] Office of the U.S. Trade Representative. (2021). *Section 301 Investigation Report on Turkey's Digital Services Tax*. https://ustr.gov/sites/default/files/enforcement/301Investigations/Report%20on%20Turkey%E2%80%99s%20Digital%20Services%20Tax.pdf.

whose revenue does not make them subject to the tax, still must certify that they are exempt.[879] In November 2021, Türkiye struck a deal with the United States on DSTs grandfathering this tax premised on successful resolution of the OECD's Pillar 1 solution. Given stalled progress on Pillar 1, and USTR's 301 finding of the tax's unreasonable and discriminatory burden on U.S. firms, USTR should reconsider steps necessary to remove this barrier.

In 2024, Türkiye amended Law No. 6563,[880] which would impose burdensome withholding tax requirements for non-resident companies that operate e-commerce platforms, depending on how the law is implemented. There is significant uncertainty in the scope and base of the tax, and industry urges vigilance to ensure companies can operate with fair access in the market. The new requirements took effect January 1, 2025.

Other Barriers to Digital Trade

A new collection of regulations on e-commerce went into effect on January 1, 2023.[881] They define procedures and principles for e-commerce operations and supervision and address 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.

Uganda

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Computer Misuse Act allows the government to compel domestic and foreign service providers to collect or record data in real time. While the Act does not explicitly subject companies to data localization requirements, the Bank of Uganda has interpreted it to require

[879] KPMG. (2020). *Türkiye: Digital Services Tax, A Primer*. https://kpmgvergi.com/Content//Service/Pdf/DijitalHizmetVergisiDanismanligi16112020_081732365687.pdf.
[880] Inal Law Office. (n.d.). *Turkey: New Era On Turkish E-Commerce Law*. https://www.inal-law.com/new-era-on-turkish-e-commerce-law/.
[881] Arseven, M. (n.d.). The Violations of Industrial and Intellectual Property Rights on E-Commerce Platforms Have Been Regulated For The First Time. *Lexology.* https://www.lexology.com/library/detail.aspx?g=c4af283b-27e1-447e-abc3-e26b0532ee65.

financial institutions operating in the country to store data on domestic data centers in order to be able to provide the government with access to customers' digital financial information.[882]

Taxation of Digital Products and Services

The Ugandan government adopted a DST imposing 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.[883] U.S. digital services providers are subject to the DST after the first dollar of revenue it earns, as the law does not include thresholds for in-market activity.

Ukraine

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Ukraine's Martial Law, a special legal framework introduced in February 2022 following Russia's invasion,[884] temporarily lifted restrictions on the use of public cloud services by the public sector and certain private sector entities, such as banks. This permitted Ukrainian Government entities to work U.S. cloud services providers to host its data. However, Ukraine may reinstate restrictions once martial law is withdrawn or expires, as the prior legal regime raised obstacles for U.S. cloud providers and Ukrainian customers of those companies. Key concerns regarding Ukraine's former legislation include: 1) non-alignment of international cybersecurity standards (such as the ISO) obtained by cloud providers coupled with a preference for local technical requirements; 2) exclusive application of Ukrainian law to govern cloud service agreements, which industry reports renders it difficult given the inherent cross-border nature of cloud services; 3) limitations on non-Ukrainian providers offering services to public institutions for personal data processing; 4) obligations to re-localize certain categories of data to Ukraine that have been temporarily permitted to be stored abroad under martial law; and 5) and inadequate and confusing data classification regulations.

[882] U.S. Department of State. (2024). *2024 Investment Climate Statement: Uganda*. https://www.state.gov/reports/2024-investment-climate-statements/uganda/.
[883] Oduti, B. (2023, October 17). *A Look Into Uganda's Digital Services Tax*. Global Voices. https://globalvoices.org/2023/10/17/a-look-into-ugandas-digital-services-tax/.
[884] Radio Svoboda. (2023, November 9). *Zelensky signed laws on the continuation of martial law and mobilization*. https://www.radiosvoboda.org/a/news-zelenskyi-mobilizatsia/32678009.html.

United Arab Emirates (UAE)

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The UAE Cybersecurity Council mandates that data workloads at the federal and Emirate-level are hosted in servers in the UAE.[885] 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 financial services and the healthcare sector. 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 Healthcare Information and Cyber Security Standard disallows hosting information sharing systems on cloud services.

Additionally, industry reports that the UAE Government has adopted strict sovereignty controls that mandate cloud services providers that serve the public sector and certain regulated industries to be solely subject to UAE law; not be subject to foreign jurisdiction and foreign laws; and physically localize data centers as well as engineering, security, maintenance, and support operations and respective personnel. These controls, which have been shared privately with cloud providers by the UAE Cyber Security Council, have been connected to concerns over U.S. law enforcement access under the CLOUD Act. These restrictions undermine U.S. providers from serving government and regulated customers and serve as a barrier to market entry. In practice, the government may certify U.S. providers that provide local ring-fenced infrastructure or work through government-linked technology companies such as G42, which still inherently obligate U.S. companies to localize infrastructure or partner with domestic entities.

In September 2025, the UAE Cyber Security Council published the National Cloud Security Policy, marking a significant evolution in the government's approach to data sovereignty for CSPs serving the public sector and regulated industries. The new policy allows foreign CSPs with infrastructure located in the UAE to host and process most government and regulated workloads, while requiring that Secret and Top Secret classified data be stored in fully sovereign infrastructure (such as Gov Cloud) under exclusive UAE jurisdiction, with UAE-based Hardware Security Modules and denial by default of all foreign access requests. This framework offers clearer compliance pathways for foreign CSPs seeking to serve government customers and regulated sectors. However, informal preferences for local technology champions such as G42 remain a key market access concern, potentially distorting competition and limiting commercial opportunities for U.S. and other foreign providers despite the more structured regulatory environment.

[885] U.S.-UAE Business Council. (n.d.). *Promoting Free and Secure Data Flows Data Privacy and Localization*. https://usuaebusiness.org/focusareas/promoting-free-and-secure-data-flows-data-privacy-and-localization/.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Since the early 2000s, the UAE has maintained longstanding regulatory restrictions on unlicensed Voice over Internet Protocol services, enforced by the Telecommunications and Digital Government Regulatory Authority (TDRA), which selectively block the voice and video calling features of popular OTT platforms such as WhatsApp, FaceTime, Skype, and Viber, while leaving text and media functions available. Only the two state-licensed telecom operators, Etisalat (e&) and Du, are authorized to provide VoIP services, effectively creating a duopoly. This policy is motivated by both economic and security considerations: it protects the substantial revenue streams generated by local operators from international calls and preserves government income from licensing fees, while also allowing the state to maintain regulatory and surveillance control over communications that would otherwise be encrypted and unmonitored. These restrictions limit foreign service providers' ability to offer full functionality, distort competition in favor of domestic telecom companies, and reduce consumer choice, creating a significant non-tariff barrier to digital trade and market entry.

The 2018 National Media Council Content Creators law applies to UAE residents and influencers operating in the UAE, including all social media influencers who promote and/or sell products as well as those that have paid associations with brands or foundations.[886] 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 influencers, particularly those based outside of the UAE, from promoting their services to the UAE market. Though industry reports that the law has not been widely enforced, it could be enforced on a highly selective basis to target certain influencers at will.

United Kingdom

Asymmetric Platform Regulation

On May 24, 2024, the Digital Marks, Competition, and Consumer Act (DMCC) came into law, creating a new competition law framework for large digital services providers, and expanding the Competition and Markets Authority's (CMA) oversight of the digital economy. Alongside changes to consumer protection and merger rules, the law allows the CMA to designate providers as having strategic market status, imposing more intrusive obligations on a small set of firms, overwhelmingly U.S. headquartered. The resulting interventions include firm-specific conduct requirements which can include regulation of prices and other commercial terms allowing CMA to create transfers to domestic vested interests (including a final offer mechanism

[886] Elhais, H. (n.d.). *License Requirements for Social Media Influencers in UAE*. HG. https://www.hg.org/legal-articles/license-requirements-for-social-media-influencers-in-uae-57336.

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 Act also allows for pro-competition interventions that function similarly to existing market investigations but are intended to move faster for those SMS firms. These powers are backed up with large potential fines (up to 10% of global turnover) and novel investigatory powers (e.g., being able to require firms to conduct experimental changes in their services). The potential for firms to challenge CMA decisions is constrained with a shift from full-merits appeal to the Competition Appeals Tribunal to judicial review only and while, in 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 defense after a finding that a code of conduct has been breached, versus at the outset).

While the implementation of the Act is still in its early stages, the CMA has launched three SMS investigations so far, all of which have concerned services provided by American companies (Google Search and the Apple and Google mobile ecosystems). They have also published "roadmaps" with potential conduct requirements. These would include many of the potential measures described above including regulation of commercial terms, interoperability requirements, data sharing, regulation of choices offered to consumers and speculative interventions regarding the integration of AI services. The breadth and potential impact of these measures has created considerable uncertainty for the services affected. USTR should encourage the UK to make sensible changes to the regulatory regime, including making compliance simplifications, undertaking a formal economic assessment and only intervening when it finds clear evidence of economic or competitive harm, base fines and fees on UK turnover (not global).

Taxation of Digital Products and Services

The 2020 Finance Budget, presented on March 11, 2020, included legislation introducing a digital services tax of 2%. The tax is 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." While the government did not identify which companies were impacted, it did acknowledge that 90% of the tax was paid by five large digital services companies likely headquartered in the United States,[887] findings later confirmed by USTR.[888] There is no indication that this burden has changed. From 2021 through

[887] UK Parliament. (2023). *The Digital Services Tax*. https://publications.parliament.uk/pa/cm5803/cmselect/cmpubacc/732/report.html.
[888] Office of the U.S. Trade Representative. (2021). *Report on the United Kingdom's Digital Services Tax*. https://ustr.gov/sites/default/files/files/Press/Releases/UKDSTSection301Report.pdf.

2024, the tax is estimated to have extracted over $3 billion from affected firms.[889] This burden could grow. In 2024, a UK political party called for raising the DST from 2% to 6% in its election platform,[890] highlighting the continued salience of this issue. The UK was among the countries that imposed a DST with whom the United States reached an interim agreement premised on progress in the OECD's Pillar 1 solution.[891] Given stalled progress on Pillar 1, and USTR's 301 finding that the tax was unreasonably discriminatory and burdensome for U.S. firms, USTR should reconsider alternative steps to encourage removal of this tax, including resumption of its suspended 301 action.

Threats to Encryption and Security of Devices

The UK has pursued policies undermining secured communications by mandating law enforcement access to encrypted communications. Passed in 2016, the Investigatory Powers Act allows authorities to require the removal of "electronic protections" applied to communications data.[892] More recent revisions have created a "notification notices" regime which industry warned could give the UK Home Office an effective veto on changes to digital services around the world, with the potential to create significant conflicts of law. Reports of such an order impairing encryption on Apple services led to criticism from the Administration and Congress. Further reports suggest the order was rescinded, but the case remains poorly understood and the underlying laws and guidance that led to the order have not been addressed. Government efforts to target digital security in this manner are damaging to U.S. digital exports and the future of online communications.

On October 26, 2023, the Online Safety Act became law, imposing new obligations on online service providers to remove illegal and harmful content, with non-compliance resulting in fines of £18 million or 10 percent of global annual revenue.[893] Under the Act's Section 122, the Office of Communications (Ofcom) can provide notice to companies to scan their data, including user messages, to proactively identify and prevent illegal content. Such requirements are incompatible with end-to-end encryption on messaging apps and would require companies to install client-side scanning software that would undermine encryption, increasing risks to privacy and security. While the government has partially walked back this requirement in response to pressure by civil

[889] CCIA. (2025). *Status of Key Digital Services Taxes in July 2025*. https://ccianet.org/library/status-of-key-digital-services-taxes-in-july-2025/.
[890] Liberal Democrats. (2023, September 27). *Triple tax on social media giants to boost mental health in schools*. https://www.libdems.org.uk/press/release/triple-tax-on-social-media-giants-to-boost-mental-health-in-schools.
[891] U.S. Department of the Treasury. (2021, October 21). *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*. https://home.treasury.gov/news/press-releases/jy0419.
[892] *Investigatory Powers Act* [UK]. (2016). https://www.legislation.gov.uk/ukpga/2016/25.
[893] *Online Safety Act* [UK] Bill C. 50. [2023]. https://bills.parliament.uk/bills/3137.

society and industry,[894] stating that Section 122 will not be invoked until "appropriate technology" exists,[895] it remains in the Act.

Uzbekistan

Asymmetric Platform Regulation

In May 2024, Uzbekistan published a regulation designating digital platforms with either a dominant position or superior bargaining power ("Resolution N256").[896] The rules include ex-ante obligations for digital suppliers in the same manner as the EU's DMA. The list of regulated platforms and ex-ante obligations is more extensive than those in the DMA and include new categories such as AI-based platforms that could undermine the growth of digital services, the development of local AI systems, and the ability of companies generally to "operate fairly." Industry reports a concerning lack of transparency in Uzbekistan's lawmaking process, offering companies insufficient opportunity to provide feedback. The lack of transparency and consultation with the business community for this set of rules reflects the broader challenges observed by the U.S. government in documents such as the State Department's Investment Climate Statement for Uzbekistan.[897] Industry urges engagement with Uzbekistan to redirect the government's approach away from discriminatory measures and towards non-discrimination ideals that would improve business conditions and cross-border trade.

Restrictions on Cross-Border Data Flows

Uzbekistan Law No. ZRU-666,[898] which amended the 2019 Law on Personal Data,[899] entered into force on April 16, 2021, and establishes strict data localization requirements. The law mandates that owners and/or operators must process the personal data of Uzbek citizens using technical means physically located within Uzbekistan. It applies to both foreign and local entities that collect personal data of Uzbek citizens through information technologies, including the internet, without setting a minimum user threshold. Its applicability is triggered simply by the act of processing Uzbek citizens' personal data. Among other requirements, the servers used to store

---

[894] Global Encryption Coalition. (2023, September 20). *Steering Committee Statement on the UK's Online Safety Bill*. https://www.globalencryption.org/2023/09/steering-committee-statement-on-the-uks-online-safety-bill/; Linares, M. (2023, December 12). *Online dangers of UK government assault on encryption*. Open Democracy. https://www.opendemocracy.net/en/digitaliberties/online-safety-act-bill-uk-government-encryption-privacy-ofcom/; Internet Society. (2023, December 1). *Safety Should Not Cost People Their Privacy*. https://www.internetsociety.org/resources/internet-fragmentation/uk-online-safety-act/.
[895] Chin-Rothmann, C. et. al. (2023, October 18). *A New Chapter in Content Moderation: Unpacking the UK Online Safety Bill*. CSIS. https://www.csis.org/analysis/new-chapter-content-moderation-unpacking-uk-online-safety-bill.
[896] Kosta Legal. (2024). *Uzbekistan Legal Newsletter for May 2024*. https://kostalegal.com/newsletters/uzbekistan-legal-newsletter-for-may-2024.
[897] U.S. Department of State. (2024). *2024 Investment Climate Statements: Uzbekistan*. https://www.state.gov/reports/2024-investment-climate-statements/uzbekistan/.
[898] *Law No. ZRU-666* [Uzbekistan]. https://lex.uz/docs/5220748.
[899] *Law on Personal Data* [Uzbekistan] No. LRU-547. (2019). https://lex.uz/docs/4831939.

and process this data must be registered in the State Register of Personal Databases, further entrenching data localization obligations. Failure to comply can lead to Uzkomnazorat, the state regulator, restricting access to the non-compliant online resource, and may also result in administrative fines and criminal liability for the entity's officials. Although there is some momentum to amend the localization provisions, the process has been slow and lacks transparency, leaving uncertainty as to what the eventual reform will entail. Industry has submitted input through AmCham, but stronger advocacy will be needed to secure meaningful change. This legislation creates a major barrier to entry for U.S. businesses, particularly those offering AI and cloud services, and effectively favors local, Russian, and Chinese vendors while undermining user security and safety. Local experts estimate that these data localization requirements cost the Uzbek economy between $3.2 and $4.5 billion annually, equivalent to 4–5.7% of GDP, illustrating their broad and damaging economic impact.[900]

Vietnam

Asymmetric Platform Regulation

Vietnam has proposed a new Digital Transformation Law that would impose ex ante competition prohibitions modeled on the EU Digital Markets Act and the UK's Digital Markets, Competition and Consumers Act, alongside digital safety obligations inspired by the EU Digital Services Act.[901] The draft law is expected to negatively and disproportionately impact U.S. technology companies. It seeks to regulate "very large-scale digital platforms" (VLDPs) through extensive obligations and prohibitions, including on self-preferencing, tying and bundling, certain data uses, app store linkouts, and interoperability requirements (Articles 41-44). VLDPs would be designated based on broad criteria, such as exceeding an average monthly user count of 10% of Vietnam's population or holding a dominant market position, defined as substantial market power or a market share above 30%, which would overwhelmingly capture U.S.-based platforms. The draft also imposes additional responsibilities on VLDP owners and operators, including algorithmic transparency requirements, and applies across multiple product areas within a single company. Moreover, it directs state agencies and state-owned enterprises to prioritize procurement of digital technology products and services that are produced and technologically mastered in Vietnam, effectively creating a market access barrier for foreign providers. It further grants Vietnamese authorities broad powers to exercise content control and impose removal or blocking obligations on digital platforms at their request. The law's structure will likely lead to the designation of primarily U.S. firms as VLDPs, undermining their ability to compete fairly and creating unjustified non-tariff barriers that advantage non-U.S. competitors in the Vietnamese market. Given Vietnam's broad commitments in both its bilateral agreement

[900] *Daryo.* (2025, July 17). Uzbekistan loses up to $4.5bn annually due to data localization law, report finds. https://daryo.uz/en/2025/07/16/uzbekistan-loses-up-to-45bn-annually-due-to-data-localization-law-report-finds/.
[901] *Lấy ý kiến Hồ sơ dự án Luật Chuyển đổi số* [Vietnam]. (2025). https://mst.gov.vn/van-ban-phap-luat/du-thao/2255.htm.

with the United States and in the WTO, a measure that puts U.S. firms at a material disadvantage in the market, in sectors as wide ranging as distribution, advertising and computer services, could constitute actionable discrimination. USTR is urged to engage with the Vietnamese government to urge reconsideration of an unecessary and unjustified measure.

Customs-Related Restrictions and Import Barriers for Goods

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,[902] 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.

The draft revised Law on Tax Administration published in September 2024 added the requirement for cross-border e-commerce platforms to be responsible for declaring and paying taxes on behalf of the household and individual businesses which creates an extraterritorial scope and uncertainty for enforcement.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

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 on January 1,

[902] *PROMULGATION OF THE "NATIONAL TECHNICAL REGULATION ON CRYPTOGRAPHIC TECHNICAL SPECIFICATION USED IN CIVIL CRYPTOGRAPHY PRODUCTS UNDER IP SECURITY PRODUCTS GROUP WITH IPSEC AND TLS"* (Vietnam) Circular 23. (2022). 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.

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, domestic companies, including foreign-invested subsidiaries, are required to store a copy of Vietnamese user data on domestic servers, and to establish a physical presence subject to the jurisdiction of Vietnamese law enforcement. While foreign firms' foreign operations are exempt from these requirements, if the foreign firms' services are used in violation of the law, the foreign firms can be mandated to localize their data.[903]

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.[904] CCIA appreciates USTR citing the problematic nature of the Decree in the 2024 NTE Report,[905] and welcomes further language specifying the harmful nature of data localization requirements. The Decree was issued without Vietnam conducting any consultation regarding the final drafts, which were kept confidential by the government, contravening Vietnam's obligations under in Article 14.13 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("CPTPP"). 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.[906] 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 CPTPP—implicating the many U.S. companies that are incorporated in CPTPP member countries and that do business in Vietnam.

The Ministry of Public Security is currently revising the Law on Cybersecurity.[907] The latest draft of the revised Cybersecurity Law retains data localization requirements. The U.S. should continue to advocate for the removal of these requirements given their effect as a de facto market access barrier, preventing U.S. and other foreign firms from providing services unless all data

---

[903] U.S. Department of State. (2024). *2024 Investment Climate Statements: Vietnam*. https://www.state.gov/reports/2024-investment-climate-statements/vietnam/.
[904] *Elaborating a Number of Articles of the Law on Cybersecurity of Vietnam* [Vietnam] No. 53/2022/ND-CP. (2022). https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Decree-53-2022-ND-CP-elaborating-the-Law-on-cybersecurity-of-Vietnam-527750.aspx; Ministry of Science and Technology. (2022, August 22). *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; Vu, Y. (2022, August 19). *Vietnam: Cybersecurity Law Decree Issued*. Rouse. https://rouse.com/insights/news/2022/vietnam-cybersecurity-law-decree-issued.
[905] Office of the United States Trade Representative. (2024). *2024 National Trade Estimate Report on Foreign Trade Barriers*. https://ustr.gov/sites/default/files/2024%20NTE%20Report_1.pdf.
[906] Phạm, M. C. (2022, September 9). *Joint industry letter on Law on Cybersecurity.* https://aicasia.org/wp-content/uploads/2022/09/Industry-Letter-Regarding-Decree-53-LOCS.pdf.
[907] Vu, Y. & Nguyen, H. (2025, June 30). *Vietnam's Draft Cybersecurity Law 2025*. Rouse. https://rouse.com/insights/news/2025/vietnam-s-draft-cybersecurity-law-2025-key-changes-businesses-need-to-know.

remains onshore. This requirement (implemented through Decree 53/2022/ND-CP)[908] creates significant technical and regulatory barriers, favoring local telecommunications and cloud providers in Vietnam, and limiting competition and innovation. The requirements also increase operational costs for both local and foreign businesses, forcing them to build local data centers even when secure global infrastructure already exists. Moreover, mandating local storage centralizes data in less secure facilities increases risks by diluting resources, limiting services, and undermining global cooperation essential for robust cybersecurity.

On June 3, 2020, Vietnam's Prime Minister signed Decision 749/QD-TTg, announcing the country's National Digital Transformation Strategy by 2025.[909] The Decree calls for the creation of technical and non-technical measures to control cross-border digital platforms.

The Ministry of Science and Technology (MST) has subsequently issued Official Letters No.1145/BTTTT-CATTT[910] and No. 783/THH-HTDLS[911] which include a local cloud standard and cloud framework, respectively, and set forward technical standards and considerations for state agencies and smart cities projects that offer preferential treatment to local private cloud providers.[912] Such preferential treatment is 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.[913] While the standards are technically voluntary, in practice, they are expected to be adopted by the Vietnamese public sector.

The Vietnamese government finalized its Personal Data Protection Decree (PDP), which was issued as Decree No. 13/2023/ND-CP in April 2023 (Decree 13) and went into effect on July 1, 2023.[914] The Decree prescribes de facto data localization conditions including maintenance of

---

[908] International Trade Administration. (2022, September 19). *Vietnam: Cybersecurity Data Localization Requirements*. https://www.trade.gov/market-intelligence/vietnam-cybersecurity-data-localization-requirements.
[909] *National Digital Transformation Strategy* [Vietnam] Decision No. 749/QD-TTg. (2020). https://english.luatvietnam.vn/decision-no-749-qd-ttg-on-approving-the-national-digital-transformation-program-until-2025-with-a-vision-184241-doc1.html.
[910] *BỘ TIÊU CHÍ, CHỈ TIÊU KỸ THUẬT ĐỂ ĐÁNH GIÁ VÀ LỰA CHỌN NỀN TẢNG ĐIỆN TOÁN ĐÁM MÂY PHỤC VỤ CHÍNH PHỦ ĐIỆN TỬ/CHÍNH QUYỀN ĐIỆN TỬ* [Vietnam] Số: 1145/BTTTT-CATTT. (2020). https://thuvienphapluat.vn/cong-van/Cong-nghe-thong-tin/Cong-van-1145-BTTTT-CATTT-2020-tieu-chi-chi-tieu-ky-thuat-danh-gia-Chinh-phu-dien-tu-439232.aspx.
[911] *ỨNG DỤNG DỊCH VỤ ĐIỆN TOÁN ĐÁM MÂY VÀ THUÊ DỊCH VỤ ĐIỆN TOÁN ĐÁM MÂY TRONG CƠ QUAN NHÀ NƯỚC* [Vietnam] Số: 783/THH-HTDLS. (2020). https://thuvienphapluat.vn/cong-van/Cong-nghe-thong-tin/Cong-van-783-THH-HTDLS-2020-Tai-lieu-huong-dan-ung-dung-dich-vu-dien-toan-dam-may-487024.aspx.
[912] Tran, G. T. H. (2020, April 15). Vietnam issues guidelines on cloud computing for e-government deployment. *Lexology.* https://www.lexology.com/library/detail.aspx?g=e567a057-5b54-4760-bcd9-937ca888773f.
[913] *Vietnam Net*. (2020, May 23). Ministry launches digital transformation campaign. https://vietnamnet.vn/en/sci-tech-environment/ministry-launches-digital-transformation-campaign-643379.html.
[914] *Decree No. 13/2023/ND-CP on personal data protection* [Vietnam]. (2023). https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx; Tran, M. H. (2024, October 14). Vietnam personal data protection decree is now officialized. *Lexology.* https://www.lexology.com/library/detail.aspx?g=678126ac-2536-4947-91a5-7328d8764309; Piemwichai, W. (2024,

extensive records relating to each individual data transfer and 'registration' of transfer of data of Vietnamese citizens overseas, impacting cross-border data flows. CCIA appreciates USTR detailing Decree 13 as a barrier in its 2024 National Trade Estimates Report.[915] 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, as they put U.S. cross-border suppliers at a significant competitive disadvantage vis-a-vis domestic suppliers.

On June 26, 2025, Vietnam adopted the Law on Personal Data Protection (PDP Law / Law No. 91/2025/QH15),[916] which will take effect on January 1, 2026, replacing the existing Personal Data Protection Decree (Decree No. 13/2023/ND-CP). The law establishes a comprehensive legal framework for personal data protection, introducing extensive compliance obligations, stringent cross-border data transfer restrictions, and significant enforcement powers. It preserves the existing transfer regime, including the requirement to submit an Overseas Transfer Impact Assessment within 60 days of the initial transfer, while granting authorities broad discretion to review and suspend transfers deemed to pose risks to national defense or security. Companies must also maintain detailed records for each individual transfer, creating heightened administrative burdens and uncertainty for international service providers. The law imposes sector-specific obligations in sensitive areas such as child data protection, digital advertising, social media, online communications, banking and finance, healthcare, and emerging technologies including artificial intelligence, cloud computing, and the metaverse. It also requires organizations to appoint data protection personnel and departments, restricts the collection of identity documents for account verification, limits legal bases for processing by relying heavily on consent (including for advertising), and prohibits the buying or selling of personal data. Violations can result in severe penalties, including fines of up to 10 times the revenue from unlawful data sales, 5% of annual revenue for unauthorized cross-border transfers, fines of up to 3 billion VND for other infractions, and potential criminal prosecution. The implementing decree, currently in its final drafting stages and expected to enter into force alongside the law, introduces new licensing and local entity requirements for personal data processing service providers. These go beyond the primary law's provisions and risk exceeding delegated authority, further increasing legal uncertainty. While these measures are framed as privacy protections, they are expected to create substantial compliance burdens and act as barriers to entry for foreign companies, particularly those offering digital and AI-driven services.

October 14). Vietnam issues landmark personal data protection decree. *Lexology.* https://www.lexology.com/library/detail.aspx?g=cc6cccb6-f317-4d54-963b-babaf71db4b1.

[915] United States Trade Representative. (2024). *2024 National Trade Estimate report on foreign trade barriers*. https://ustr.gov/sites/default/files/2024%20NTE%20Report_1.pdf.

[916] Tilleke & Gibbins. (2025, August 27). *Vietnam's New Personal Data Protection Law: A Closer Look*. https://www.tilleke.com/insights/vietnams-new-personal-data-protection-law-a-closer-look/.

CCIA encourages USTR to engage with Vietnam on the PDP Law's implementation and seek to mitigate its regulatory overreach and restrictive approach to cross-border data flows.

The revised Telecom Law went into effect in July 2024 and adopted a more liberalized regime for OTT services, data centers, and cloud services. On 24 December 2024, the government issued Decree No. 163/2024/ND-CP ("Decree 163"), detailing several articles and measures for implementing the 2023 Telecommunications Law. Decree 163 clarifies that OTT communication services, data centers, and cloud services are classified as value-added telecom services, alongside traditional categories such as email and internet access. Unlike traditional telecom services, these newly regulated services may be provided cross-border without the obligation to contract with a licensed Vietnamese telecom operator. However, offshore providers must notify the Vietnam Telecommunications Authority before offering services, disclose corporate and service information, designate a contact point, and comply with obligations including user verification, data retention, and service quality disclosure. Offshore cloud and data center providers must refrain from accessing or using service-user data without consent, and if contracting with Vietnamese state authorities, must store government data exclusively in Vietnam, effectively requiring local facilities. While Decree 163 excludes cloud, data center, and OTT services from the strictest cross-border licensing requirements, it introduces new compliance burdens, such as mandatory notifications, user data retention, and government-only local storage, severely limit the value of the liberalization. These developments are especially important as foreign companies, including U.S. firms relocating operations from China, evaluate Vietnam as a key regional hub, and will seek to support their operations in Vietnam through cloud-based services.

Vietnam's newly enacted Law on Data (No. 60/2024/QH15, or the Data Law), which took effect on July 1, 2025, introduces sweeping restrictions on the classification, transfer, and processing of data, backed by draft implementing measures now under consideration. The Data Law defines "important" and "core" data expansively, covering fields such as defense, banking, insurance, health, and even internet behavioral data, and requires burdensome preapproval procedures before such data can be transferred abroad. Important data may be transferred only after a review period without objection from regulators, while core data requires affirmative authorization before transfer. These rules, together with overlapping consent requirements in the draft implementing decree, effectively impose broad data localization obligations, and effectively discriminate against foreign service suppliers. The draft framework further introduces impractical obligations that will hinder U.S. firms' ability to operate in Vietnam. These include requirements for repeated impact assessments and reporting, onerous restrictions on data intermediaries and managers who may not control the datasets they host, and sweeping government powers to requisition private-sector data under vaguely defined "national interest" or "public interest" grounds, without clear due process safeguards. The effect on foreign cloud service suppliers is likely to be significant: while they are not directly subject to these regulations, their customers based in Vietnam would be, and the increased liability they face with

respect to cross-border transfers is a powerful disincentive to using foreign-based cloud computing services. Given the competitive disadvantage this imposes on foreign-based suppliers, this measure implicates Vietnam's WTO Commitments with respect to computer and related services, as well as commitments Vietnam undertook in the CPTPP (several members of which host major U.S. cloud computing companies and thus should be beneficiaries of this agreement).

Government-Imposed Content Restrictions and Related Access Barriers

The Law on Cybersecurity 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 service providers 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, *inter alia,* is critical or disparaging of the Vietnamese government. Companies have already been fined under this provision.[917]

Besides regulatory roadblocks, U.S. companies face challenges from technical interventions 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. companies' competitiveness in the marketplace.

On November 9, 2024, the Vietnamese government issued Decree No. 147/2024/ND-CP on the Management, Provision, and Use of Internet Services and Online Information (Decree 147), which took effect on December 25, 2024, with no grace period, replacing Decree 72/2013 and its amendments.[918] The decree imposes broad obligations on foreign enterprises deemed "Regulated Cross-Border Services," defined as providers with more than 100,000 monthly visits from Vietnam for six consecutive months or those leasing local data center space. Such entities must notify the Ministry of Culture, Sport and Tourism (MCST) of a local contact point, store and hand over user data upon request, take down flagged content within 24 hours, temporarily block content within 48 hours of user complaints, and enter into "cooperation agreements" with Vietnamese press agencies. They must also provide content scanning tools, implement child-protection measures, and submit on-demand and periodic reports. Social networks, app stores, and game providers face additional obligations. Foreign social networks above the traffic thresholds must verify accounts, restrict certain interactive features to verified users, and lock or remove accounts and channels repeatedly posting infringing content. App stores must comply

[917] Vu, K. (2019, January 8). Vietnam says Facebook violated controversial cybersecurity law. *Reuters.* https://www.reuters.com/article/us-vietnam-facebook/vietnam-says-facebook-violated-controversial-cybersecuritylaw-idUSKCN1P30AJ; Olson, J., & Nguyen, M. P. (2019, March 6). Vietnam quick to enforce new cybersecurity law. *Hogan Lovells Chronicle of Data Protection.* https://www.engage.hoganlovells.com/knowledgeservices/news/vietnam-quick-to-enforce-new-cybersecurity-law.

[918] *MANAGEMENT, PROVISION, AND USE OF INTERNET SERVICES AND CYBER INFORMATION* [Vietnam] No. 147/2024/ND-CP. (2024). https://www.qtsc.com.vn/uploads/files/2024/12/30/147_2024_ND-CP_636187-eng.pdf.

with domestic payment laws, remove applications on government request, and require publishers to present licenses before distributing games. The decree also maintains the prohibition on cross-border provision of online games, forcing foreign publishers to establish a domestic entity to operate in Vietnam, while introducing a new 16+ age rating system. These requirements create significant barriers to entry and effectively compel foreign suppliers to rely on local partners. The decree also mandates intrusive data and identity verification requirements, including the collection and storage of mobile phone numbers and, in some cases, national identity numbers. These rules expand state surveillance, impose disproportionate compliance costs, and conflict with data minimization principles by requiring sensitive data storage beyond business necessity. Taken together, Decree 147 imposes sweeping, onerous, and trade-restrictive obligations that disproportionately impact cross-border digital service providers. CCIA welcomed USTR's acknowledgment of these risks in the 2025 National Trade Estimates Report and urges continued U.S. engagement to press back against measures that undermine digital trade, user rights, and market access.

On June 22, 2025, Vietnam's Ministry of Industry and Trade (MOIT) introduced the draft Law on E-Commerce (2025 Draft E-Commerce Law) for public consultation.[919] The legislation would mandate that online platforms verify domestic sellers via VNeID and foreign sellers through legal documents, and extend regulatory oversight to livestream sales, affiliate marketing, and social-media commerce. The draft law is nearing completion and is expected to be submitted for approval by the National Assembly before the end of the year, with effectiveness slated for 2026. Under the draft, foreign platforms must establish a local entity or representative, deposit funds with a Vietnamese bank, and comply with transparency and consumer-compensation rules. The draft also assigns obligations to logistics, payments, and infrastructure providers, requiring them to work only with compliant platforms. These changes raise major operational and compliance risks for foreign platforms: the expanded scope, deeper local-entity requirements, and cross-sector obligations could impose significant new costs and reduce flexibility in Vietnam's digital market.

Imposing Legacy Comms Regs

On October 1, 2022, the Authority of Broadcasting and Electronic Information issued Decree 71/2022/ND-CP (Decree 71),[920] amending Decree No. 06/2016/ND-CP on the Management, Provision, and Use of Radio and Television Services by extending broadcast television regulations to video-on-demand services. Decree 71 continues a long-running effort to regulate

[919] Shang, Y. (2025, August 29). *Vietnam's Draft E-Commerce Law 2025: Key Provisions and Business Implications*. Vietnam Briefing. https://www.vietnam-briefing.com/news/vietnams-draft-e-commerce-law-2025-key-provisions-and-business-implications.html/.

[920] *Decree No. 71/2022/ND-CP on amendments to some articles of Government's Decree No. 06/2016/ND-CP on management, provision, and use of radio and television services* [Vietnam]. (2022). 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/.

internet-enabled subscription video services provided on a cross-border basis and requires such services to be made only through websites or applications with domain names and IP addresses managed by Vietnam. 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.

Potential Challenges to the Development of Artificial Intelligence

In July 2024, the government of Vietnam released the draft Digital Technology Industry Law (DTI Law), which contains troubling provisions relating to AI.[921] The draft DTI Law includes concerning mandates such as access and portability obligations that are technically impossible, without providing any safeguards. Additionally, AI developers would be required to monitor the downstream use of their technology and services, for which company compliance would be extremely difficult. The DTI Law also includes an overly broad and vague provision that details what could be viewed as prohibitions on the development or deployment of any AI technology (e.g. Article. 7). For example, the broad definition of "digital technology" could include diverse and rapidly evolving technologies such as AI, big data, and blockchain, which industry is concerned could lead to overly-prescriptive regulations. This is in part due to the draft DTI Law's focus on prioritizing investment, lease, and procurement of domestically produced digital technology products and services, which could result in unfair treatment of foreign competitors, and U.S. businesses in particular that are leaders in this space. Overall, the draft DTI Law gives the regulator is given sweeping oversight authority with inadequate guardrails that could empower undue and subjective interpretation (such as defining what constitutes an activity that "violates morality" or "causes adverse effects on social security of individuals in Vietnam") and could result in unpredictable or unfair enforcement for companies. This might also result in the potential censorship of speech and expression on the internet relating to what systems can be used to train services and what consumers can enter as prompts, while also furthering biases in the outputs of generative AI services.

The government of Vietnam has separated the AI provisions from the PDP framework into a standalone Law on Artificial Intelligence (AI Law),[922] which is scheduled for National Assembly approval in December 2025 and entry into force on January 1, 2026, following a transition period. The draft AI Law establishes a comprehensive regulatory framework governing the research, development, provision, and use of AI systems in Vietnam, applying to both domestic and foreign entities. It adopts a pre-market, risk-based management approach, classifying AI

[921] Hai, G. H., & Nguyen, T. N. (2024, August 22). Vietnam: A new chapter for digital technology industry. *Lexology.* https://www.lexology.com/library/detail.aspx?g=b0d22a3f-52d6-4d12-b20d-0586de47dc98; Baker McKenzie. (2024, July 9). Vietnam: New draft Law on Digital Technology Industry and draft Data Law. *Baker McKenzie.* https://insightplus.bakermckenzie.com/bm/data-technology/vietnam-new-draft-law-on-digital-technology-industry-and-draft-data-law.

[922] Nguyen, H.T. & Do, A. (2025, October 15). *Vietnam's draft AI Law: Racing toward regulation with EU inspirations*. IAPP. https://iapp.org/news/a/vietnam-s-draft-ai-law-racing-toward-regulation-with-eu-inspirations.

systems into "unacceptable" (prohibited), "high," "medium," and "low" risk categories, with high-risk systems subject to conformity assessments, detailed logging requirements, and mandatory human oversight. The draft further emphasizes transparency, accountability, and compliance with Vietnam's National AI Ethics Framework, while promoting technological sovereignty and innovation through regulatory sandboxes. In addition to these obligations, the law introduces local establishment and registration requirements for providers of high-risk AI systems, including appointing a legal representative in Vietnam, registering with a national system, and conducting pre-launch impact assessments. It also includes obligations around intellectual property protection, privacy, and transparency. While framed as a trust-building measure, this highly prescriptive "regulate-first" approach is ill-suited to the fast-evolving nature of AI, where models and applications develop continuously. It risks locking Vietnam into a rigid framework that stifles innovation and competitiveness, imposes excessive compliance burdens, and creates barriers for market entry—particularly for foreign AI developers and smaller innovators. The extensive technical documentation and complex pre-market approval processes could delay testing and product launches, slowing the development-to-market cycle and deterring investment. Furthermore, the stringent obligations for high-risk systems—covering risk management, data governance, human oversight, and post-market monitoring—are resource-intensive and would disproportionately disadvantage smaller players, raising concerns among foreign stakeholders about the law's potential trade and innovation impacts.

The draft Personal Data Protection Decree, expected to be adopted and enter into force alongside the new Personal Data Protection Law in January 2026, contains AI-related provisions, and language potentially affecting emerging digital environments such as the virtual reality that have raised significant industry concerns. Mandating consent as the sole legal basis for automated data processing and AI model training will restrict technological innovation and deviate from international best practices as well as existing Vietnamese laws. In addition, granting government agencies the authority to order the destruction of AI algorithms is viewed as an extreme measure that could significantly undermine investor confidence and deter market entry. These overlapping and inconsistent regulatory frameworks create legal uncertainty and risk hindering the development of Vietnam's AI sector. Industry strongly recommends removing these AI-related requirements from the Personal Data Protection Decree and deferring them to the dedicated AI regulatory framework under the DTI Law and forthcoming AI Law instead.

Taxation of Digital Products and Services

The Tax Administration Law, effective July 1, 2020, taxes cross-border e-commerce and other digital services.[923] The Ministry of Finance issued Circular 80 providing guidance on the Law

[923] Vettoretti, A. (2020, August 7). Vietnam's Tax Administration Law takes effect. *IR Global.* https://www.irglobal.com/article/vietnams-tax-administration-law-takes-effect-in-july-2020-0f67/.

and its Decree 126 in September 2021. [924] The Circular added a requirement for foreign digital service and e-commerce suppliers without a permanent establishment in Vietnam to directly register and pay taxes. 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 law allows digital suppliers to seek exemptions under bilateral tax treaties but the process for obtaining such benefits remains unclear. The FCT is a discriminatory tax that burdens US commerce in Vietnam. It specifically targets foreign companies and industries operating in the digital economy, where US firms are highly successful. Similar to digital services taxes enacted in other countries, the FCT is applied on gross revenues, imposes a significant financial burden on US commerce in Vietnam, and enables Vietnam to assert first right to tax over the US tax base. The law allows digital suppliers to seek exemptions under bilateral tax treaties but Vietnam's administration of double tax relief applications effectively discriminates against US industries. US companies face significant barriers in their applications for double tax relief under the relevant bilateral tax treaties entered into by the Vietnamese government with other governments. Despite complying with domestic tax law, regulations and procedures in Vietnam, these US companies face long delays by the Tax Department in reviewing their applications, onerous and voluminous informational requests, and unjustified rejections of their tax refund applications that are not only inconsistent with Vietnam's obligations under the relevant bilateral tax treaty, but also run counter to the spirit and principles of bilateral tax treaties. The additional tax burden created by the deemed tax rates (Corporate Income Tax and Value Added Tax) will result in further complications and costs for cross-border service providers and conflict with international taxation rules.

Other Barriers to Digital Trade

Vietnam allows for foreign participation in the telecommunications sector, with varying equity limitations depending on the specific industry. The Law on Telecommunications (Telecom Law) 41/2009/QH12 stipulates that domestic companies providing basic telecommunication services with infrastructure can only have 49% foreign ownership, while companies that supply telecommunications services without infrastructure can go up to 65% foreign ownership. Vietnam's regime permits up to 70% foreign ownership for virtual private network (VPN) services suppliers. Facilities-based operators are mandated to be state-controlled firms, which in practice means that the state (through the relevant line ministry) would be required to have at least 51% equity. For CPTPP countries, Vietnam committed to offering more lenient treatment, but the implementation of this promised liberalization, and whether countries can benefit from this change, is unclear.

[924] Nguyen, T. H., & Duong, C. T. (2021, October 9). Circular 80/2021/TT-BTC guiding the Law on Tax Administration, Decree 126/2020. *Thu Vien Phap Luat.* 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.

On September 25, 2021, the government issued Decree 85/2021/ND-CP (Decree 85),[925] broadening the scope of existing e-commerce regulations 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 January 1, 2022.

Vietnam is developing an E-commerce Law to replace Decree 85. The draft law is expected to be passed in before the end of 2025 and take effect in July 2026 without a grace period. While the Government has made an effort to categorize various types of e-commerce platforms, some definitions are still not clear which could lead to misinterpretations and incorrect assignment of responsibilities. The draft law also imposes irrelevant and overly burdensome responsibilities on social networks that do not have online ordering functions, such as verifying all sellers, proactive monitoring of livestreaming content or onerous mandatory record retention requirements. Finally, the localization requirements (local entity or local representative) are considered onerous and uniform across all platform types, potentially hindering foreign businesses. Given the overarching potential impact of the new E-commerce Law on U.S companies, the U.S. should advocate for a delay of the law for further consultation with the business community, or at the very least, adding an implementation grace period of 12 months for foreign companies in line with the current Decree 85 to allow businesses sufficient time to adapt to the new regulations.

Vietnam has recently revised its Advertising Law (No. 75/2025/QH15), retaining the longstanding requirement from the 2012 law that foreign advertisers must use local advertising agencies to run advertisements targeting the Vietnamese market.[926] With the rapid growth of digital advertising, particularly on social media platforms since the Covid-19 pandemic, this requirement creates significant operational and cost challenges for U.S. companies. Vietnam's digital advertising market is projected to reach $2.94 billion in 2025, with digital ads accounting for over 60% of total ad spend, underscoring the economic significance of this restriction for both international and local businesses. The measure is inconsistent with Vietnam's WTO and trade agreement commitments (which specifically provide for non-discriminatory treatment of cross-border advertising), creates unnecessary barriers for U.S. digital advertising companies, and undermines the efficiency of cross-border platforms. It also raises costs, discourages investment, and limits access to world-class advertising tools, contradicting Vietnam's stated digital economy objectives. More effective and less trade-restrictive alternatives, such as

[925] Samuel, P. (2021, October 12). Vietnam passes regulation on e-commerce: Decree 85. *Vietnam Briefing.* https://www.vietnam-briefing.com/news/vietnams-passes-regulation-e-commerce-decree-85.html/.
[926] *AMENDMENTS TO CERTAIN ARTICLES OF THE LAW ON ADVERTISING* [Vietnam] Law No. 75/2025/QH15. (2025). https://thuvienphapluat.vn/van-ban/EN/Thuong-mai/Law-75-2025-QH15-amendments-to-certain-Articles-of-the-Law-on-Advertising/671036/tieng-anh.aspx.

transparency requirements or appointing a local point of contact, could provide regulatory oversight without imposing discriminatory market access restrictions. U.S. advocacy to remove or suspend enforcement of this clause pending a regulatory impact assessment is critical to protect U.S. companies, uphold international trade norms, and maintain strategic competitiveness in the Indo-Pacific's fast-growing digital economy. Given its significant impact on U.S. suppliers, USTR is urged to prioritize efforts to address this egregious barrier.

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.