

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

In re Request for Comments on Significant
Foreign Trade Barriers for the 2027 National
Trade Estimate Report

Docket No. USTR-2026-0498

COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION
REGARDING FOREIGN TRADE BARRIERS TO U.S. EXPORTS
FOR 2027 REPORTING

October 28, 2026

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 91 Fed. Reg. 58,247 (Sept. 14, 2026),¹ the Computer & Communications Industry Association (CCIA) submits the following comments for consideration for USTR's 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 regulations and policy frameworks that restrict market access in the digital economy.

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\$283.5 billion for the United States in 2025.³

Notwithstanding this success, U.S. firms' export potential is undermined by persistent threats from countries that continue to adopt discriminatory or unbalanced regulations, or regulations designed primarily to extract value from cross-border suppliers and thus impede market access. For the 2027 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) imposition of legacy telecommunications rules on internet-enabled services, (9) challenges to the development of AI, (10) restrictions on cross-border data flows, (11) taxation on digital products and services, and (12) threats to the security of devices and services.

¹ U.S. Trade Representative, (2026, September 14), *Request for Comments on Significant Foreign Trade Barriers for the 2027 National Trade Estimate Report*, Federal Register, <https://www.federalregister.gov/documents/2026/09/14/2026-18775/request-for-comments-on-significant-foreign-trade-barriers-for-the-2027-national-trade-estimate>.

² For more, visit www.ccianet.org.

³ U.S. Bureau of Economic Analysis, (2026, July 7), *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>.

Table of Contents

EXECUTIVE SUMMARY	2
I. INTRODUCTION	5
II. KEY CATEGORIES OF DIGITAL TRADE-RELATED BARRIERS	8
A. Asymmetric Platform Regulation	8
B. Customs-Related Restrictions and Import Barriers for Goods	8
C. Barriers to the Deployment and Operation of Network Infrastructure	8
D. Data and Infrastructure Localization Mandates and Restrictions on Cloud Services	9
E. Discriminatory Local Content Quotas and Audiovisual Service Mandates	9
F. Forced Revenue Transfers for Digital News	9
G. Government-Imposed Restrictions on Internet Content and Related Access Barriers	10
H. Imposing Legacy Telecommunications Rules on Internet-Enabled Services	10
I. Challenges to the Development of AI	11
J. Restrictions on Cross-Border Data Flows	12
K. Taxation of Digital Products and Services	12
L. Threats to the Security of Devices and Services	12
III. COUNTRY-SPECIFIC CONCERNS	12
Argentina	12
Australia	15
Austria	28
Azerbaijan	30
Bangladesh	31
Belgium	34
Bhutan	36
Bolivia	36
Brazil	37
Cambodia	53
Cameroon	55
Canada	55
Chile	67
China	71
Colombia	79
Cote d'Ivoire	83
Croatia	83
Cuba	85
Cyprus	86
Czech Republic	87
Democratic Republic of the Congo	88
Denmark	89
Dominican Republic	91

Ecuador.....	92
Egypt.....	95
Ethiopia.....	98
European Union.....	98
France.....	124
Germany.....	134
Ghana.....	141
Greece.....	141
Guinea.....	142
Hong Kong.....	142
Hungary.....	146
India.....	146
Indonesia.....	162
Iraq.....	180
Ireland.....	180
Italy.....	183
Japan.....	187
Jordan.....	193
Kazakhstan.....	194
Kenya.....	196
Korea.....	200
Malaysia.....	214
Malta.....	222
Mexico.....	222
Morocco.....	232
Nepal.....	233
Netherlands.....	236
New Zealand.....	236
Nigeria.....	238
Norway.....	241
Pakistan.....	242
Panama.....	245
Papua New Guinea.....	246
Peru.....	247
Philippines.....	250
Poland.....	254
Russia.....	256
Rwanda.....	263
Saudi Arabia.....	264
Singapore.....	270
South Africa.....	274
Spain.....	278
Sri Lanka.....	279
Switzerland.....	281

Taiwan.....	282
Tanzania.....	285
Thailand.....	287
Türkiye.....	295
Uganda.....	303
Ukraine.....	305
United Arab Emirates (UAE).....	306
United Kingdom.....	308
Uzbekistan.....	313
Vietnam.....	314
IV. CONCLUSION.....	324

I. INTRODUCTION

Given the centrality of internet-enabled commerce, to both the United States and the global economy, failure to address barriers and keep markets open threatens the prosperity of all participants. For the United States, the threat is to many of its most successful and innovative companies who provide a source of the country's long-term growth, its ability to generate high-quality jobs, and its technological leadership.

The real value added of the digital economy in the U.S. grew at an average annual rate of 7.1% between 2017 and 2022, over triple that of the overall economy.⁴ According to the 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 compensation consistently increasing from 2006 (\$85,595) to 2021 (\$154,427). Digital trade supported 3 million jobs in the United States in 2022.⁶ U.S. companies generated \$813.4 billion in digitally-deliverable services exports globally in 2025, with a trade surplus of \$283.5 billion.⁷ Digitally-deliverable services represented 66% of all U.S. services exports in 2025 reflecting

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, (2026), *Table 3.3. U.S. Trade in ICT Services and Digitally Deliverable Services, by Country or Affiliation*, <https://apps.bea.gov/iTable/?reqid=62&step=6&isuri=1&tablelist=359&product=4>.

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>.

their 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, primarily in data center buildout, reached \$285.9 billion in 2025.⁹

International markets continue to present some of the most significant growth opportunities for U.S. companies, both large and small. For transformative technologies like AI, access to these markets is critical to achieving scale and recouping the substantial investments required for its 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, but also the widely-articulated but inchoate goal of “AI sovereignty”—a slogan that could be benign or a pretext for protectionist policies. 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 2024 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 advancing U.S. economic interests.

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, (2026), *2026 AI Index Report, Economy*, <https://hai.stanford.edu/ai-index/2026-ai-index-report>.

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.

II. KEY CATEGORIES OF DIGITAL TRADE-RELATED BARRIERS

Digital trade barriers identified in CCIA's comments fall into 12 broad categories:

A. Asymmetric Platform Regulation

Led by the EU's Digital Markets Act, *ex-ante* platform regulations are spreading globally. Typically introduced without concrete evidence of consumer harm intended to be addressed, they often function as industrial policy to advantage local competitors—specifically targeting leading U.S. services, impeding legitimate business models while threatening higher prices and reduced innovation. The effectiveness of such proposals in promoting innovation in the tech sector is highly questionable,¹² and a growing body of evidence points to concrete consumer harms that have resulted.¹³

B. Customs-Related Restrictions and Import Barriers for Goods

Goods exporters face low or uncertain de minimis thresholds, opaque licensing and quota schemes, and mandatory pre-shipment inspections. These non-tariff barriers cause border delays, increase working capital needs, and disproportionately burden small e-commerce exporters. Such barriers impede the export of U.S. ICT goods abroad, as well as the components U.S. firms need to expand digital infrastructure in key foreign markets

C. Barriers to the Deployment and Operation of Network Infrastructure

Key impediments to global infrastructure deployment include barriers on:

Subsea Cables: While U.S. hyperscalers are investing tens of billions of dollars to maintain and expand networks to connect their global data centers,¹⁴ they face impediments to cable laying and repair. Carrying over 95% of global internet traffic and \$10 trillion in annual economic activity,¹⁵ subsea cable deployment faces restrictive

¹² MacCarthy, M., (2019, October 22), *To Regulate Digital Platforms, Focus on Specific Business Sectors* <https://www.brookings.edu/articles/to-regulate-digital-platforms-focus-on-specific-business-sectors/>.

¹³ Nextrade (2025), *The impact of the Digital Markets Act on Consumers*, https://www.nextradegroupllc.com/files/ugd/478c1a_9d7c98475ce8404188d2f8dbb1c9d2ff.pdf; and Wagener, (2025), *Europe's Digital Markets Act is Failing Users*, <https://ccianet.org/articles/europes-digital-markets-act-is-failing-users/>.

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 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., Hounghonon, 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/>.

cabotage rules, mandatory local partnerships, route restrictions, and import taxes on repair vessels.

LEO Satellites: Powering a SATCOM market projected at \$40 billion by 2030,¹⁶ low Earth orbit constellations face local incorporation mandates, denied interference protections, mandatory content decryption, and discriminatory registration regimes. 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.

D. Data Localization & Cloud Restrictions

Forced data storage and corporate presence requirements serve protectionist "digital sovereignty" goals, increasing cyber risks by centralizing sensitive data¹⁷ and eroding U.S. cloud leadership.¹⁸ For companies leveraging cloud services to access markets on a cross-border basis, such policies can mean abandoning markets altogether. For investors, complementary regulations discriminate against foreign cloud providers through tailored certification schemes, VPN restrictions, and forced decryption. These policies directly target U.S. companies, who lead in the global cloud services market, supporting billions of dollars in economic activity and thousands of high-paying U.S. jobs.¹⁹

E. Local Content Quotas & Audiovisual Mandates

Mandatory, revenue-based local production funding, cultural levies, and interface manipulation ("discoverability" and "prominence" rules) discriminate against U.S. streaming providers and U.S. content. 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.

¹⁶ 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>.

¹⁷ 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 .

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>.

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-Hit-US-1-614-1-Billion-by-2030.html>.

F. Forced Revenue Transfers for Digital News

Laws like Australia's News Media Bargaining Code and complementary Incentive Tax, and Canada's Online News Act compel platforms to pay publishers for displaying news snippets, headlines, or links. Bypassing traditional copyright norms, these measures extract billions from U.S. firms, distort internet economics, and increase media concentration.²⁰ Other 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 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.

G. Government Restrictions on Internet Content and Related Access Barriers

Censorship, throttling, and 313 internet shutdowns across 52 countries in 2025²² cost the global economy nearly \$8 billion.²³ Simultaneously, the erosion of safe harbor intermediary liability protections forces platforms to perform burdensome monitoring, disclose proprietary algorithms, or face local criminal liability. National firewalls and state-controlled network gateways further disadvantage foreign services by degrading their performance relative to domestic competitors, if not outright blocking access.

H. Imposing Legacy Telecommunications Rules on Internet-Enabled Services

Sender-Pays Fees: Proposals requiring content providers to pay ISPs for user-requested traffic degrade network performance and tax digital exports. 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

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 millions of ad-revenue 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 Access Now. (2025). *When repression meets resistance: internet shutdowns in 2025*. <https://www.accessnow.org/internet-shutdowns-2026/>

²³ 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/>.

charges.²⁴ Similar proposals are under discussion in the EU, Australia, Brazil, and the Caribbean, sometimes with arbitrary traffic thresholds to target large U.S. providers.

OTT Regulation: Subjecting over-the-top messaging and cloud services to telecom-style licensing ignores fundamental differences between network infrastructure and application-layer services.

I. Challenges to AI Development

According to the WTO, AI could boost global trade by 37% by 2040, and increase global GDP by 13% by 2040.²⁵ However, inconsistent legal regimes and the growing proliferation of AI laws and regulations threaten this future: adversely affecting investment in, or the cross-border supply of, AI-enabled services and technologies.

One major near-term challenge is changes to or interpretations of copyright law that threaten access to open web datasets required for model training. Most other countries do not have the innovation-friendly doctrine of fair use but 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 or text-and-data-mining exceptions to copyright should be a priority.²⁶ Other threats to the cross-border supply of AI services include a range of enacted or proposed laws and regulations prematurely constraining AI deployment before standards and best practices have fully evolved.²⁷ 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 unduly restrict U.S. firms' AI offerings.

J. Restrictions on Cross-Border Data Flows

Despite the fact that cross-border data transfers underpin \$4.25 trillion in digitally deliverable services in 2023, non-interoperable privacy rules and restrictive data export conditions reduce productivity, disrupt supply chains and cross-border trade and lower GDP.

²⁴Wagener. (2023). *Myths Surrounding Network Usage Fees: South Korea*.
<https://ccianet.org/library/network-usage-fee-myths-korea/>

²⁵ 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.

²⁶ CCIA. (2026). *International Copyright Frameworks for AI Training*.
<https://ccianet.org/library/international-copyright-frameworks-for-ai-training-2/>.

²⁷ 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.

K. Taxation of Digital Products and Services

Digital Services Taxes (DSTs): Unilateral DSTs in key European countries extracted over \$13 billion from 2020 to 2025, singling out U.S. firms and causing double taxation.²⁸ Policymakers in Washington, across administrations and parties, have consistently condemned these measures,²⁹ and the United States should continue to respond forcefully, using all available trade tools, to prevent their proliferation and to protect U.S. exporters from being singled out for discriminatory treatment in foreign markets.³⁰

E-Commerce Customs Duties: Expiration of the WTO moratorium on electronic transmission tariffs increases the risk that countries will seek to impose such taxes and introduce severe compliance burdens on cross-border data. Between 1998 and 2026, WTO members 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. This moratorium has now expired, based on a failure to reach consensus on renewal at the 2026 WTO Ministerial in Cameroon. 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.

L. Threats to the Security of Devices and Services

Mandatory government access to encrypted communications (such as the UK Online Safety Act, Australia's Assistance and Access Act, and Canada's Bill C-22) weakens end-to-end security and user privacy. Additional mandates compel pre-installed government software, unverified third-party app stores, or forced interoperability that expose devices to malicious actors. Various countries' consideration of such measures warrant continued vigilance.

²⁸ CCIA. (2026). *Status of Key Digital Service Taxes*.

<https://ccianet.org/library/2026-status-of-key-digital-services-taxes/>.

²⁹ 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.

³⁰ 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-Service-s-Taxes-.pdf>.

III. COUNTRY-SPECIFIC CONCERNS

Argentina

Customs-related Customs-Related Restrictions and Import Barriers for Goods

Argentina has reduced customs clearance burdens through successive reforms, including the October 2024 repeal of precautionary import reference values and the May 2025 removal of rules permitting industry representatives to observe red-channel inspections.³¹ Under the U.S.–Argentina Agreement on Reciprocal Trade and Investment (ARTI), signed in February 2026, Argentina committed to paperless processing and pre-arrival clearance of low-risk U.S. shipments.³² CCIA encourages USTR to monitor implementation and address any remaining duplicative documentation requirements or disproportionate inspection delays affecting U.S. technology imports.

Resolution 16/2025 revised Argentina’s electrical-equipment safety requirements and expanded acceptance of foreign certificates.³³ Decree 892/2025, published in December 2025, subsequently established broader recognition of qualifying foreign certifications, with its principal provisions taking effect in February 2026.³⁴ Compliance requirements nevertheless vary by product and certification route. Certain professional electronic, audio, and video equipment qualify for a declaration-of-conformity procedure supported by technical documentation. CCIA encourages Argentina to clarify that equipment imported for companies’ own use qualifies for streamlined treatment and ensure that implementation of these reforms eliminates duplicative testing and unnecessary certification requirements.

Argentina operates two distinct express shipments regimes, each designed to accommodate different types of shipments with varying requirements and restrictions on weight, value, item count, and frequency of use. The coexistence of the two models and the count and value limitations create constant friction at customs clearance, increasing processing times and imposing disproportionate compliance burdens on U.S. companies. Under the Small Shipments Regime, individuals are limited to five duty-exempt shipments per calendar year, each capped at three units of the same commodity, a maximum weight of 50 kg, and a value not exceeding

³¹ Gobierno de Argentina. (2025, May 9). *El Gobierno eliminó viejas trabas aduaneras para agilizar el comercio exterior*.
<https://www.argentina.gob.ar/noticias/el-gobierno-elimino-viejas-trabas-aduaneras-para-agilizar-el-comercio-exterior>

³² Office of the United States Trade Representative. (2026, February 5). *Agreement between the United States of America and the Argentine Republic on Reciprocal Trade and Investment*, Article 3.1.
<https://ustr.gov/sites/default/files/files/Press/Releases/2026/US%20Argentina%20ARTI%20English%20Final%20February%202026.pdf>

³³ Secretaría de Industria y Comercio. (2025, February 25). *Resolución 16/2025*.
<https://www.argentina.gob.ar/normativa/nacional/resolución-16-2025-410052/texto>

³⁴ Poder Ejecutivo Nacional. (2025, December 17). *Decreto 892/2025*.
<https://www.boletinoficial.gob.ar/detalleAviso/primera/336319/20251217>

\$3,000 FOB. Shipments valued below \$400 FOB are exempt from customs duties and the statistical fee; shipments exceeding the five-shipment annual quota are subject to full customs duties (averaging 40%+) on the entire value, including the portion below \$400. This quota-based system creates significant operational challenges for U.S. companies, as they cannot access information to track quotas. The U.S.–Argentina Agreement on Reciprocal Trade and Investment (ARTI), signed on February 5, 2026, directly addresses these barriers: Article 1.22 commits Argentina to removing limitations on weight, value, item count, and frequency of use for simplified procedures applicable to express shipments, while Article 1.24 requires all border agencies to complete pre-arrival data processing to enable immediate release of low-risk shipments without diversion to bonded facilities. Despite these commitments, Argentina has not yet implemented any changes to the express shipments aligned with the provisions of the ARTI.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Argentina’s public sector lacks a standardized framework for cloud service procurement, creating a market access barrier through lengthy, inefficient processes that deter cloud adoption and burden providers, particularly affecting U.S. technology companies serving public sector entities. The Secretaría de Innovación, Ciencia y Tecnología has been developing a public-sector cloud framework agreement (*acuerdo marco*) to standardize and streamline procurement from qualified providers, including international cloud service providers. Argentina should finalize this framework with flexible resource allocation and streamlined approval procedures to facilitate market access and efficient cloud adoption.

On May 13, 2026, Argentina’s Centro Nacional de Ciberseguridad (CNC) issued Disposition 01/2026, mandating that all National Public Sector entities maintain a backup/disaster-recovery data center within Argentine territory, located at least 1,500 km from the primary site and holding Tier 3 certification. These requirements have no precedent in OECD or G20 frameworks and cannot be met by internationally competitive U.S. cloud providers. The measure functions as a data localization mandate that forces entities away from modern cloud architectures toward inferior on-premises infrastructure and risks entrenching the state-owned operator (ARSAT) as the sole compliant provider. It was issued without public consultation and is in tension with Argentina’s non-discrimination commitments (Article 3.2) under the U.S.–Argentina Digital Trade and Innovation Agreement (ARTI). Argentina should adopt technology-neutral, outcome-based disaster-recovery requirements that recognize cloud multi-region resilience as compliant, and remove the in-country residency, fixed-distance, and physical-building certification mandates.

Restrictions on Cross-Border Data Flows

Argentina's published adequacy framework does not include the United States, requiring companies transferring personal data to the United States to rely on contractual safeguards or another permitted legal basis. This creates additional compliance costs for U.S. suppliers. In the February 2026 ARTI, Argentina committed to recognize the United States as providing adequate data protection (Annex III, Section 2). CCIA welcomes this commitment and urges USTR to seek prompt implementation through the necessary domestic measures, providing businesses with clear and reliable conditions for transferring personal data to the United States.

While ARTI has not yet been ratified by Argentina's Congress, the government could nonetheless advance this recognition. A resolution would require modification of Disposition E60/2016 AAIP to include the United States as an adequate jurisdiction, or recognition of U.S. Data Privacy Framework (DPF) certified companies as meeting adequacy requirements.³⁵

Taxation of Digital Products and Services

Argentina's Impuesto PAIS, a temporary surtax on cross-border payments, expired in December 2024. However, General Resolution 5617/2024 retains a separate 30% advance collection toward income or personal assets tax on certain foreign purchases, including covered card payments for services supplied by non-residents, when settled in pesos and requiring access to the foreign exchange market.³⁶ April 2025 amendments exempted foreign-currency purchases by individuals and undivided estates, as well as payments through specified online platforms.³⁷ For transactions still covered, the advance collection increases upfront costs for Argentine customers purchasing foreign services, even where subsequently creditable or refundable. It should be rescinded.

In 2018, Argentina's tax agency ruled that foreign advertising services were exempt from local income tax.³⁸ However, it reversed course in 2021, imposing an effective 17.5% withholding tax on foreign digital ads (such as videos, banners, audio, and text).³⁹ Under the ARTI, Argentina

³⁵ Office of the United States Trade Representative. (2026, February 5). *Agreement between the United States of America and the Argentine Republic on Reciprocal Trade and Investment*, Annex III, Section 2, paragraph 1. <https://ustr.gov/sites/default/files/files/Press/Releases/2026/US%20Argentina%20ARTI%20English%20Final%20February%202026.pdf>

³⁶ Agencia de Recaudación y Control Aduanero. (2024, December 19). *Resolución General 5617/2024 (texto actualizado)*, Articles 1, 6, and 7.

<https://www.argentina.gob.ar/normativa/nacional/resolución-5617-2024-407430/actualizacion>
³⁷ Agencia de Recaudación y Control Aduanero. (2024, December 19). *Resolución General 5617/2024 (texto actualizado)*, Article 2(e)–(f), as amended by General Resolutions 5672/2025 and 5677/2025.

<https://www.argentina.gob.ar/normativa/nacional/resolución-5617-2024-407430/actualizacion>

³⁸ Administración Federal de Ingresos Públicos. (2018, November 9). *Consulta Vinculante 54/2018*. https://biblioteca.afip.gob.ar/dcp/VIN_101_000054_2018_11_09

³⁹ Martín, J. (2021, November 3). *Servicios de publicidad pagados al exterior: Impuesto a las ganancias*. *Consulta Vinculante N° 39/2021. Cambio de postura de AFIP*. <https://abogados.com.ar/servicios-de-publicidad-pagados-al-exterior-impuesto-a-las-ganancias-consulta-vinculante-n-392021-cambio-de-postura-de-afip/29356>

pledged not to target U.S. companies with discriminatory digital taxes (Article 3.1). CCIA urges the U.S. Trade Representative to examine the treatment of cross-border online advertising in implementing this commitment and seek clarification of the applicable withholding rules.

Australia

Asymmetric Platform Regulation

In December 2024, AU Treasury launched its long-anticipated consultation on a new *ex-ante* regime for digital services. The proposed framework adopted aspects of both the EU DMA and the UK DMCCA, which would allow the AU Government to designate digital platform services to broad obligations on matters such as self-preferencing and data use, as well as ‘service-specific obligations.’ The initial proposal would trigger new compliance obligations around preventing self-preferencing, ensuring interoperability, and prohibiting manipulative design practices. The proposal identifies ‘priority services’ for designation as app marketplaces, ad-tech services and social media, although a wide range of digital services were flagged for future consideration, including general online marketplaces, virtual assistants and, potentially, cloud. Designation would also give the ACCC to recommend service-specific (platform-specific) obligations.

The scheme would raise similar trade-related concerns to the DMA, particularly if only US-headquartered companies meet the criteria for designation (which is possible given the initial sectors identified). On June 23, 2025, the ACCC released its final Digital Platform Services Inquiry report, dated March 2025.⁴⁰ The report maintained its recommendation for a new digital competition regime and called for continued monitoring of emerging digital markets. The proposal remains a significant concern for U.S. suppliers because of the breadth of the contemplated obligations and likely targeting of U.S. firms with significant compliance burdens, exacerbated by the ACCC’s stated intent to use the regime to arbitrarily force product changes without clear procedural safeguards.

A February 2025 study published by the CCIA Research Center modeled potential reductions in digital-services investment of up to 17.4% and GDP losses of up to A\$21.1 billion under its assessed scenarios.⁴¹ These figures are prospective estimates dependent on the study’s assumptions, rather than observed effects of Australia’s proposed regime. By targeting specific firms through prescriptive obligations rather than adopting principle-based, evidence-driven

⁴⁰ Australian Competition and Consumer Commission. (2025, June 23). 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>.

⁴¹ Taylor, W., & Feyler, E. (2025, February 25). A New Digital Competition Regime: Insights into Economic Risks. CCIA Research Center.

https://ccianet.org/wp-content/uploads/2025/02/CCIA_New-Digital-Competition-Regime-Insights-into-Economic-Risks_report.pdf

enforcement, the proposal threatens to distort competition and undermine U.S. market access in Australia.

In late 2026, Australia signaled a partial retreat from broad-based EU-style regulation to a narrower, more limited regulatory posture. A “position paper” outlining a narrower scope has been expected since April 2026, but it still has not been released.

In September 2026, the Australian Government released an exposure draft of an Online Safety ‘Digital Duty of Care’ Bill⁴² that would introduce a broad statutory obligation requiring providers of online services to ensure, so far as is reasonably practicable, a safe online environment. The duty would apply to social media platforms, search engines, hosting services, app distribution services and AI content generation tools, and would require providers to conduct annual risk assessments covering content, algorithmic recommendation systems and product design features. The regime would grant the Minister broad power to determine conduct and material that should not be available for adults and children, as well as wide latitude to determine platform design features, an authority that should reside with parliament given their remit. The Duty of Care would be enforced, with civil penalties of up to approximately AUD 109 million (US 78 million) for non-compliance. The Australian Government has indicated that AI companies, including providers of generative AI services, would be captured by the duty. Legislation is expected to be introduced to Parliament in 2027. The scope of this legislation should be monitored to ensure the definition of regulated online services does not disproportionately capture U.S. technology companies or impose unreasonable compliance obligations that function as barriers to market access.

In September 2025, Parliament amended the Payment Systems (Regulation) Act 1998 to expand the Reserve Bank of Australia’s regulatory remit to a broader range of payment systems and participants, including services outside the traditional card-payment framework.⁴³ The RBA subsequently identified mobile wallets, buy-now-pay-later services, three-party card schemes, and e-commerce platforms as areas for further consultation.⁴⁴ The expansion creates potential exposure for U.S. digital payment providers to additional oversight and compliance requirements that may not be appropriate for innovative new services. USTR should monitor subsequent designations and rules to ensure that obligations are proportionate and do not discriminate against foreign suppliers.

⁴² Government of Australia. (2026). *Digital Duty of Care Bill (2026)*. <https://www.infrastructure.gov.au/media-communications/internet/online-safety/online-safety-amendment-digital-duty-care-bill-2026-exposure-draft> .

⁴³ Parliament of Australia. (2025, September 19). *Treasury Laws Amendment (Payments System Modernisation) Act 2025 (No. 46, 2025)*. <https://www.legislation.gov.au/C2025A00046/asmade/text>

⁴⁴ Reserve Bank of Australia. (2026, June 25). *Review of Payments System Regulation – Issues Paper*. <https://www.rba.gov.au/payments-and-infrastructure/regulatory-reviews/review-of-payments-system-regulation-2026/2026-06/pdf/issues-paper.pdf>

Data and Infrastructure Measures and Restrictions on Cloud Services

In 2019, the Australian Government released the Hosting Strategy,⁴⁵ 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.⁴⁶

Certification requires hosting providers, data center operators, and cloud service providers to allow the government to specify ownership and control conditions. The framework has the effect of imposing data localization, data residency, and personnel requirements on all protected-level data and data from government systems. The policy functions of this framework were transferred to the Department of Home Affairs in May 2023⁴⁷ and it is now undergoing reform. Effective November 3, 2025, the government paused applications from new providers and supplementary assessments pending completion of that process, while stating that existing certified providers would not be affected.⁴⁸ The published pause creates a potential additional market-entry obstacle for suppliers seeking certification to serve Australian government customers. USTR should monitor both the duration of the pause and any revised ownership, control, personnel, or data-location conditions, with a view to ensuring that practices are consistent with Australia's obligations under both WTO and AUSFTA government procurement rules.

On March 23, 2026, the government published expectations for new and expanded data centers and AI infrastructure.⁴⁹ The policy links alignment with these expectations to prioritization of Commonwealth regulatory assessments. Expectations include investment in Australian supply chains and skills, deployment of engineers and researchers in Australia, and favorable access to computing capacity for Australian startups, smaller businesses, researchers, and nonprofit organizations, alongside energy, water, and security commitments. The expectations operate alongside existing laws and fall short of a standalone statutory localization mandate. Nevertheless, linking regulatory priority to domestic investment and preferential access commitments creates potential market-access concerns for U.S. cloud and AI infrastructure suppliers. CCIA urges USTR to seek transparent, proportionate assessment criteria and clarity concerning how these expectations affect investment approvals, with a view to ensuring consistency with AUSFTA investment rules.

⁴⁵ 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>

⁴⁶ Digital Transformation Agency. (2021, March). *Whole of Government Hosting Strategy: Hosting Certification Framework*.

<https://www.hostingcertification.gov.au/sites/default/files/2021-11/Hosting%20Certification%20Framework%20-%20March%202021.v2.pdf>

⁴⁷ Department of Home Affairs. *Safeguarding Australian Government data*. <https://www.hostingcertification.gov.au/>

⁴⁸ Department of Home Affairs. *Hosting Certification Framework*. <https://www.hostingcertification.gov.au/>

⁴⁹ Department of Industry, Science and Resources. (2026, March 23). *Expectations of data centres and AI infrastructure developers*.

<https://www.industry.gov.au/publications/expectations-data-centres-and-ai-infrastructure-developers>

Following data center policy frameworks issued by New South Wales and Victoria in August and September 2026, the Australian Government released a consultation paper⁵⁰ proposing mandatory national minimum standards for large data centers, based on legislation expected in early 2027. The proposed standards include requirements to demonstrate meaningful community engagement, draw on local suppliers, and actively support workforce training. It separately proposes conditions requiring entities undertaking frontier AI training in Australia to contribute to local research, innovation and capability—including by making computing capacity available to Australian start-ups, researchers and small businesses on favorable terms. The development of these aspects should be monitored to ensure they do not operate as *de facto* local content requirements or impose disproportionate costs on U.S. cloud service providers.

Discriminatory Local Content Quotas and Audiovisual Service Mandates

Following Parliament’s passage of legislation in November 2025, Australia introduced mandatory Australian-content expenditure requirements for subscription video-on-demand services for the 2026 calendar year.⁵¹ In-scope services carrying qualifying programming become subject to the expenditure obligation when they reach at least one million Australian “paying subscribers” at any time during the reporting year. The statutory subscriber calculation can include activated free trials and subscriptions supplied through bundles. Separate notification obligations apply to in-scope services reaching at least 250,000 Australian paying subscribers, including services below the expenditure threshold. The regime therefore affects major U.S. exporters as well as Australian services. ACMA administers the requirements, with the first annual compliance reports due on February 15, 2027.

Covered services must ordinarily devote an amount equal to 10% of their total program expenditure for Australia to eligible Australian programs or elect an alternative requirement equal to 7.5% of Australian revenue. The program-expenditure calculation includes the Australian value of eligible global content, requiring services to allocate costs associated with internationally commissioned or licensed programming. Eligible genres include drama, children’s programming, documentaries, arts, and education.

Qualifying expenditure can include production, commissioning, investment, and acquisition of eligible Australian programs, subject to timing and other requirements. It generally must be incurred before the program becomes publicly available in Australia outside cinemas. The Australian-program rules impose conditions concerning creative personnel and production, while also recognizing qualifying New Zealand programs and official co-productions. The framework

⁵⁰ Australian Government. (2026). *Building AI infrastructure that works for Australia*. <https://www.pmc.gov.au/resources/getting-it-right-building-ai-infrastructure-works-australia> .

⁵¹ Burke, T., & Wells, A. (2025). *Backing local stories for Australian audiences*. <https://minister.infrastructure.gov.au/burke/media-release/backing-local-stories-australian-audiences>; Australian Communications and Media Authority. (2026, August 20). *Australian content requirement for subscription video on demand services: reporting to the ACMA*. <https://www.acma.gov.au/australian-content-requirement-subscription-video-demand-services-reporting-acma>

allows expenditure to be managed over a three-year compliance cycle, but still constrains services' choices about the content and timing of investment. CCIA has estimated that the cost to U.S. suppliers of these requirements could surpass \$1 billion by 2030.

These requirements divert resources from programming selected in response to consumer demand and impose additional valuation, reporting, and compliance burdens on U.S. streaming services. Domestic-content eligibility conditions also disadvantage investment in productions that do not meet the prescribed criteria, even where those productions appeal to Australian audiences or involve substantial international collaboration.

The measures appear to contravene AUSFTA's digital-product nondiscrimination provisions and Article 11.9.1(b), concerning domestic-content performance requirements.⁵² Australia's relevant Annex II reservation is conditional: it addresses circumstances in which Australian content or genres are not readily available and includes requirements concerning objective criteria, transparency, and the burden of intervention. CCIA urges USTR to examine whether Australia has satisfied those conditions and whether the expenditure mandate is consistent with its commitments. If, as expected, Australia is judged as not having met these conditions, CCIA urges USTR to take appropriate action to redress any breach.

Australia has also implemented a separate television prominence framework applying to regulated devices manufactured and supplied on or after January 10, 2026.⁵³ Manufacturers must provide prescribed access and visibility for Australian free-to-air broadcasting services, including preinstallation and prominent placement of relevant applications, subject to statutory conditions. The rules cover certain connected television devices as well as smart televisions. CCIA is concerned that mandated preferential placement restricts interface design and disadvantages competing digital services seeking access to Australian audiences. USTR should investigate whether such preferences are consistent with Australia's obligation to provide non-discriminatory access to digital products (Article 16.4).

Forced Revenue Transfers for Digital News

In February 2021, the Australian Government passed the News Media and Digital Platforms Mandatory Bargaining Code.⁵⁴ The Code requires designated platforms to negotiate with and pay Australian news publishers for online content, including content that news publishers voluntarily

⁵² Office of the United States Trade Representative. *Australia–United States Free Trade Agreement: Final text*, Articles 11.9.1(b) and 16.4, and Australia's Annex II broadcasting and audiovisual services reservation. <https://ustr.gov/trade-agreements/free-trade-agreements/australian-fta/final-text>

⁵³ Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts.

Prominence for connected TV devices.

<https://www.infrastructure.gov.au/media-communications-arts/television/prominence-connected-tv-devices>

⁵⁴ Australian Competition and Consumer Commission. *News media bargaining code.*

<https://www.accc.gov.au/by-industry/digital-platforms-and-services/news-media-bargaining-code/news-media-bargaining-code>

share on digital platforms.⁵⁵ 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 Treasurer 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,⁵⁶ competition,⁵⁷ trade,⁵⁸ and intellectual property⁵⁹ 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.⁶⁰ A Treasury report in November 2022 found that at least 30 such agreements were reached, though their contents remain confidential.⁶¹ The report recommended expanded investigatory powers, compulsory information sharing, and a full review in 2025.

Australia has now enacted the News Bargaining Incentive, substantially escalating its policy of compelling digital services to finance Australian news businesses.⁶² The implementing legislation received Royal Assent on August 26, 2026, and came into force the following day. The final legislation imposes a fee of 2.75% covered revenue (advertising revenue generated in Australia).⁶³ Liability applies to qualifying reporting periods beginning on or after July 1, 2025, creating retrospective exposure.

⁵⁵ 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/>.

⁵⁶ 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/>.

⁵⁷ 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/>.

⁵⁸ 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/>.

⁵⁹ 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/>.

⁶⁰ 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

⁶¹ 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>.

⁶² Australian Government. (2026, August 26). *News Media Bargaining (Administration) Act 2026 (No. 77, 2026)*. <https://www.legislation.gov.au/C2026A00077/asmade/text>; Australian Government. (2026, August 26). *News Media Bargaining Charge Act 2026 (No. 78, 2026)*. <https://www.legislation.gov.au/C2026A00078/asmade/text>

⁶³ Computer & Communications Industry Association. (2026, August 28). *Australia’s Final News Bargaining Tax Revisions Fail to Address Fundamental Concerns*. <https://ccianet.org/library/australias-final-news-bargaining-tax-revisions-fail-to-address-fundamental-concerns/>

The regime covers social media or search services whose relevant Australian digital advertising revenue exceeds A\$250 million and meet Australia audience thresholds of five million average monthly for social media services and ten million for search services. The final revisions increased the rate but narrowed the revenue base to relevant digital advertising revenue and removed the express professional-networking exclusion. These changes do not resolve CCIA's concern that the measure's thresholds and service definitions concentrate its burdens on major U.S. suppliers and appear inconsistent with several AUSFTA provisions barring discriminatory treatment.

Targeted suppliers can avoid or reduce the tax by purchasing or otherwise funding Australian news content according to highly prescriptive rules: access to this offset requires new eligible expenditures involving at least eight separate news business corporate groups in the relevant year. Eligible payments receive a 150% offset, increased to 200% for qualifying smaller news businesses, subject to a cap on the contribution from any individual news group. CCIA considers the measure a discriminatory revenue-transfer mechanism. Liability does not depend on a platform carrying news content, weakening any asserted connection between the charge and compensation for the use of journalism. Conditioning relief on expenditure benefiting Australian news businesses appears inconsistent with Australia's trade commitments guaranteeing national treatment and proscribing performance requirements.⁶⁴ CCIA urges USTR to prioritize engagement on the measure, including its retrospective application, discriminatory effects, and conditions for obtaining offsets. If Australia is unwilling to exempt U.S. suppliers from these requirements USTR should consider initiating a Section 301 investigation and/or dispute settlement under AUSFTA.

Government-Imposed Content Restrictions and Related Access Barriers

The Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 commenced on April 6, 2019.⁶⁵ It imposes reporting obligations concerning specified Australia-linked abhorrent violent material on relevant service providers and requires content and hosting providers to expeditiously remove or cease hosting covered material.⁶⁶ Criticism of the legislation was widespread, with particular concern about the rushed nature of the drafting and legislative process, precluding meaningful stakeholder consultation. 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. Although the law assigns different reporting and removal obligations to different categories of providers, CCIA remains

⁶⁴ Office of the United States Trade Representative. (n.d.). *Australia–United States Free Trade Agreement: Chapter Eleven—Investment*, Articles 11.3 (National Treatment) and 11.9 (Performance Requirements).

https://ustr.gov/sites/default/files/uploads/agreements/fta/australia/asset_upload_file248_5155.pdf

⁶⁵ Australian Attorney-General's Department. (2019, July 16). *Abhorrent Violent Material Act Fact Sheet*.

<https://www.ag.gov.au/crime/publications/abhorrent-violent-material-act-fact-sheet>

⁶⁶ Parliament of Australia. (2019). *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019*.

https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1201

concerned that its requirements are insufficiently tailored to providers' operational capabilities and roles in facilitating user-generated content.

The Online Safety Act, passed in June 2021⁶⁷ and operational from January 2022, 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 2022.⁶⁸ 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).⁶⁹ Following the industry-code process, the eSafety Commissioner registered mandatory standards for relevant electronic services and designated internet services on June 21, 2024; those standards took effect on December 22, 2024.⁷⁰ Additional Age-Restricted Material Codes subsequently introduced obligations across multiple service categories, with commencement dates including December 27, 2025, and March 9, 2026, and later implementation dates for certain measures.⁷¹ Industry concerns include 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.

On September 8, 2026, the government announced targeted consultation on draft legislation introducing a digital duty of care and additional user controls over online feeds, with introduction to Parliament planned for later in 2026.⁷² The exposure draft would require covered providers to take reasonably practicable measures to provide a safe online environment, supported by risk assessments at least annually and before material service changes, together with user-control and other accountability requirements. It would replace the Basic Online Safety

⁶⁷ Australian Government. (2021). *Online Safety Act 2021* (No. 76, 2021).

<https://www.legislation.gov.au/C2021A00076/latest/text>

⁶⁸ 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/>

⁶⁹ 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>.

⁷⁰ eSafety Commissioner. (n.d.). *Register of Online Safety Codes and Standards*.

<https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards>

⁷¹ eSafety Commissioner. (2026, August 6). *Frequently asked questions about access to online porn and other adult content*. <https://www.esafety.gov.au/industry/codes/faq-access-to-online-porn-and-other-adult-content>

⁷² Albanese, A., & Wells, A. (2026, September 8). *My Feed, My Way*.

<https://minister.infrastructure.gov.au/wells/media-release/my-feed-my-way>

Expectations⁷³ and the existing industry-code and industry-standard framework, rather than simply add a duty to those instruments. The draft provides a 12-month period after Royal Assent before the principal duty-of-care and replacement provisions commence; these provisions are not yet law. USTR should monitor the feasibility of the proposed transition, the scope of implementing requirements, and interaction with continuing social-media minimum-age obligations to prevent disproportionate burdens on U.S. suppliers.

Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024 has moved into implementation.⁷⁴ Since December 10, 2025, covered platforms must take reasonable steps to prevent Australians under 16 from creating or retaining accounts, without an exception based on parental consent. The obligation restricts accounts rather than all access to publicly available content. The Online Safety Amendment (Strengthening Enforcement for the Social Media Minimum Age) Act 2026 received Royal Assent on September 11, 2026, and commenced on September 12.⁷⁵

For contraventions subject to the amendments, the maximum corporate penalty for breaching the minimum-age obligation doubled to 300,000 penalty units, currently A\$109.2 million. The amendments also strengthened the Commissioner's powers to obtain information and documents from platforms and third parties and to compel individuals to attend examinations and answer questions. They increased infringement-notice amounts, including to approximately A\$21.8 million for specified breaches of the minimum-age and alternative-identification requirements.

The eSafety Commissioner identifies Facebook, Instagram, Snapchat, Threads, TikTok, Twitch, X, YouTube, Kick, and Reddit among the covered services.⁷⁶ The March 2026 rules added criteria concerning recommender features or logged-in features, making the treatment of particular service designs important to determining coverage. The inclusion of numerous leading U.S. platforms creates significant compliance exposure for U.S. digital exporters.

Implementation requires platforms to assess users' ages, prevent account creation, and address existing accounts of underage subscribers. These obligations can impose substantial engineering, assessment, and appeals costs, while erroneous age determinations risk excluding eligible users. Although the legislation includes privacy safeguards and requires an alternative to government-issued identification or accredited digital identification, age assurance can still

⁷³ eSafety Commissioner. (2026, April 22). *Basic Online Safety Expectations*.

<https://www.esafety.gov.au/industry/basic-online-safety-expectations>

⁷⁴ eSafety Commissioner. (2026, September 15). *Social media age restrictions*.

<https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions>

⁷⁵ Australian Government. (2026, September 11). *Online Safety Amendment (Strengthening Enforcement for the Social Media Minimum Age) Act 2026 (No. 83, 2026)*, section 2.

<https://www.legislation.gov.au/C2026A00083/asmade>

⁷⁶ Not an exhaustive list. See reporting here: PBS NewsHour. (2025, December 3). *Australia to enforce social media age limit of 16 with fines up to \$33 million*.

<https://www.pbs.org/newshour/world/australia-to-enforce-social-media-age-limit-of-16-with-fines-up-to-33-million>

involve additional processing of personal information and friction for users. The availability of regulatory guidance does not eliminate uncertainty about how the reasonable-steps standard will be applied in individual enforcement cases.

The Commissioner's March 2026 compliance update documented continuing implementation problems and investigations involving Facebook, Instagram, Snapchat, TikTok, and YouTube.⁷⁷ These developments underscore the operational difficulty of enforcing an account-based age threshold across large services. CCIA urges USTR to examine whether implementation demands and penalties impose disproportionate barriers on U.S. suppliers, and to encourage proportionate approaches that protect children while preserving privacy, access to information, and legitimate online activity. Significant implementation issues, including opposition from parents and circumvention by adolescents are now emerging.⁷⁸ This law is also subject to High Court challenges brought by Reddit and the Digital Freedom Project. On July 29, 2026, the Court directed that the proceedings be heard together by the Full Court during its November 2026 sittings.⁷⁹ The challenges remain unresolved, and in the interim the minimum-age obligations remain in force. USTR should monitor the proceedings for any resulting changes to the framework's validity or operation.

Australia has enacted the Scams Prevention Framework, establishing a framework for enforceable obligations on designated sectors, initially banking, telecommunications, and digital platforms. Implementation is staged: requirements concerning Australian Financial Complaints Authority membership began on September 1, 2026, while most substantive obligations are scheduled to begin on March 31, 2027. Sector-specific codes and supporting rules remain important to the final allocation of responsibilities. CCIA is concerned that duties to prevent, detect, disrupt, report, and respond to scams, together with dispute-resolution requirements, could impose substantial compliance costs on U.S. digital services if they are not calibrated to providers' roles and capabilities, and urges USTR to monitor the implementation of this measure.

AUSFTA contains an obligation to provide liability limitations for online service providers relating to copyright infringement claims, analogous to 17 U.S.C. § 512.⁸⁰ However, Australia has failed to fully implement such obligations, and current implementations are far narrower than what is required. Australia's safe-harbor framework covers "carriage service" providers (telcos

⁷⁷ eSafety Commissioner. (2026, March). *Social Media Minimum Age: Compliance update*.

<https://www.esafety.gov.au/sites/default/files/2026-03/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf>

⁷⁸ Center Forward. (2026). Australia's Social Media Ban.

<https://center-forward.org/polling-and-research/socialmediaban/>.

⁷⁹ High Court of Australia. (2026, July 29). *The Digital Freedom Project Incorporated v Commonwealth of Australia & Ors (S163/2025): Order referring to Full Court*, orders 1–4.

https://www.hcourt.gov.au/sites/default/files/2026-07/DigFree-Cth_Order29.07.2026%28ref%20FC%29.pdf

⁸⁰ Office of the United States Trade Representative. (n.d.). *Australia–United States Free Trade Agreement: Chapter Seventeen—Intellectual Property Rights*, Article 17.11.29.

https://ustr.gov/sites/default/files/uploads/agreements/fta/australia/asset_upload_file469_5141.pdf

and ISPs) and specified educational, cultural, and disability-related institutions, while generally excluding commercial online service providers such as search engines and content-sharing platforms. CCIA considers this unduly narrow construction inconsistent with Australia's trade obligations under Article 17.11.29 of the FTA. This article makes clear that the protections envisioned should be available to all online service providers, not merely carriage service providers. Although Australian authorities documented this implementation flaw years ago, no legislation has been enacted to remedy it.⁸¹ CCIA urges USTR to continue to press Australia to fully comply with this AUSFTA commitment.

Challenges to the Development of AI

Australia initiated a consultation in September 2024 on mandatory guardrails for high-risk AI, including general-purpose AI, raising concerns about broad coverage and potentially disproportionate compliance obligations.⁸² The National AI Plan, released in December 2025, subsequently emphasized existing technology-neutral and sector-specific laws as the foundation for AI governance, supported by an AI Safety Institute, voluntary guidance, and targeted responses to identified regulatory gaps.⁸³ The Government recently released its National AI Standards Discussion Paper which sets out consultation on obligations from a data centre, training and infrastructure perspective as well as obligations from a copyright perspective, including control and transparency requirements.⁸⁴ USTR should monitor subsequent measures for unnecessary disclosure requirements, discriminatory treatment, or barriers to cross-border provision of AI services.

On October 26, 2025, the government announced that it was reversing a prior proposal and would not consider introducing a text-and-data-mining exception to copyright law.⁸⁵ It subsequently prioritized promotion of licensing arrangements for AI training, the treatment of AI-generated material, and expanded copyright enforcement through its Copyright and Artificial Intelligence Reference Group, managed by the Attorney General's Department. These developments do not mandate licensing, but the absence of a dedicated exception and the direction of further reform diminish legal certainty and will likely increase the cost of developing AI applications and services in Australia, or act as a barrier for AI investment. CCIA urges

⁸¹ 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>

⁸² Australian Department of Industry, Science and Resources. (2024, September 5). *Introducing mandatory guardrails for AI in high-risk settings: Proposals paper*. <https://consult.industry.gov.au/ai-mandatory-guardrails>

⁸³ Australian Department of Industry, Science and Resources. (2025, December 2). *National AI Plan*. <https://www.industry.gov.au/sites/default/files/2025-12/national-ai-plan.pdf>

⁸⁴ Australian Government. (2026, September). *Getting it right: Building AI infrastructure that works for Australia*. Department of the Prime Minister and Cabinet. <https://www.pmc.gov.au/sites/default/files/resource/download/ai-consultation-paper.pdf>.

⁸⁵ Rowland, M. (2025, October 26). *Albanese Government to ensure Australia is prepared for future copyright challenges emerging from AI*. <https://ministers.ag.gov.au/media-centre/albanese-government-ensure-australia-prepared-future-copyright-challenges-emerging-ai-26-10-2025>

USTR to monitor whether subsequent measures preserve workable, appropriately balanced conditions for U.S. AI developers and suppliers.

Taxation of Digital Products and Services

From July 1, 2018, Australia extended GST collection to covered low-value goods imported by Australian consumers, generally goods with a customs value of A\$1,000 or less.⁸⁶ Registration is generally required when relevant annual GST turnover reaches A\$75,000 or more. Depending on the transaction, responsibility for collection can fall on an overseas merchant, an electronic distribution platform, or a redeliverer. Purchases by GST-registered businesses for business use are generally outside this low-value consumer-goods collection regime. Registration and reporting are administered by the Australian Taxation Office. Nonresident supplier and platform collection is used in other jurisdictions but CCIA remains concerned that registration, transaction classification, and reporting requirements can create significant fixed compliance costs for smaller U.S. exporters and urges Australia to maintain accessible, proportionate compliance arrangements.

On September 4, 2026, the Australian Taxation Office finalized its software-royalties position in Taxation Ruling TR 2026/2, replacing draft TR 2024/D1, and released accompanying draft compliance guidance, PCG 2026/D4,⁸⁷ resulting in an interpretation of existing tax law and treaties, rather than a legislative amendment to the tax code.

The ruling maintains a broad approach to identifying royalty payments in software arrangements, including arrangements involving rights to authorize acts protected by copyright. This creates potential withholding-tax exposure for U.S. software suppliers and distributors, depending on contractual rights, transaction structure, and the applicable treaty. Whether the ruling has retrospective application and how it will affect companies' reliance on earlier guidance remains unclear, raising concerns about uncertainty, compliance costs, and inconsistent cross-border characterization of software payments.

Notwithstanding the High Court's August 2025 PepsiCo decision⁸⁸ on a similar matter, certain transactions (including relating to software) should still be able to claim embedded royalties without triggering withholding.⁸⁹ CCIA urges USTR to engage with Australia on interpretations

⁸⁶ Australian Board of Taxation. (n.d.). *Review of GST on low value imported goods*.

<https://taxboard.gov.au/review/low-value-imported-goods-review>

⁸⁷ McElwain, C., Geale, J., Chen, S., Breckveldt, C., & Lagamba, M. (2026, September 8). *ATO finalises software royalties ruling: certainty, but not comfort*. MinterEllison.

<https://www.minterellison.com/articles/ato-finalises-software-royalties-ruling-certainty>

⁸⁸ High Court of Australia. (2025, August 13). *Commissioner of Taxation v PepsiCo, Inc.* [2025] HCA 30.

<https://www.hcourt.gov.au/cases-and-judgments/cases/decided/case-m982024>

⁸⁹ McElwain, C., Geale, J., Chen, S., Breckveldt, C., & Lagamba, M. (2026, September 8). *ATO finalises software royalties ruling: certainty, but not comfort*. MinterEllison.

<https://www.minterellison.com/articles/ato-finalises-software-royalties-ruling-certainty>

that could impose inappropriate royalty withholding on ordinary software distribution or service transactions.

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 framework provides three forms of assistance: voluntary technical assistance requests; technical assistance notices requiring use of existing capabilities; and technical capability notices requiring the development of specified capabilities, subject to statutory conditions. Notices may not require a systemic weakness or vulnerability, and the framework includes requirements concerning reasonableness, proportionality, practicality, and technical feasibility. CCIA remains concerned that the operation of these powers, including the boundary between targeted assistance and systemic security risks, can undermine trust in communications services and impose substantial burdens on U.S. providers. 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

Australia's Security of Critical Infrastructure Act 2018, expanded through reforms in 2021 and 2022, establishes obligations for covered critical infrastructure, including certain data-storage and processing assets.⁹² Depending on the asset and applicable provisions, the framework includes incident reporting, risk-management requirements, enhanced cybersecurity obligations, and government-assistance powers subject to statutory conditions. CCIA remains concerned about the operational and security implications of government directions and intervention powers for U.S. technology suppliers.

Further amendments to the Critical Infrastructure Risk Management Program rules commenced on June 10, 2026,⁹³ strengthening requirements concerning matters including foreign ownership, control or influence, offshore access, supply chains, and personnel. The enhanced rules apply to nine specified asset subclasses, with transition periods for existing covered entities extending

⁹⁰ Parliament of Australia. (2018). *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*.

https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195

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 Australian Government. (2018). *Security of Critical Infrastructure Act 2018 (No. 29, 2018)*, as amended, section 12F and Parts 2–2C. <https://www.legislation.gov.au/C2018A00029/latest>

⁹³ Australian Government. (2026, June 9). *Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026*, section 2. <https://www.legislation.gov.au/F2026L00701/asmade/text>

into 2027 and 2028. Although not applicable to all cloud or data-processing services, they may affect U.S. technology suppliers through requirements imposed by covered customers, adding contractual, assessment, and access-control burdens.

Other Barriers to Digital Trade

On August 31, 2026, the government released the exposure draft Privacy Amendment (Personal Data Protection) Bill 2026.⁹⁴ The proposal would introduce a fair-and-reasonable standard for collecting, using, and disclosing personal information, strengthen consent requirements, and create an erasure right applying to specified large online platforms. Its platform-specific obligations could materially affect major U.S. digital suppliers. CCIA urges USTR to examine whether its coverage criteria and implementation requirements are objective, proportionate, and workable for cross-border services.

Separately, the Office of the Australian Information Commissioner consulted from March 31 to June 5, 2026, on a draft Children’s Online Privacy Code.⁹⁵ The proposal covered online services likely to be accessed by children under 18, giving it a broader age scope than the social-media minimum-age restrictions. It includes age-assessment requirements, subject to an exception where a service applies the code’s protections to all users, high-privacy defaults, and privacy-impact assessments. The Commissioner must finalize and register the code by December 10, 2026. USTR should monitor the final requirements and their interaction with online-safety obligations, particularly where overlapping age-assurance and service-design requirements increase compliance burdens for U.S. suppliers.

Austria

Taxation of Digital Products and Services

Austria’s 5% digital services tax on domestic online advertising took effect on January 1, 2020.⁹⁶ It applies to suppliers with annual worldwide revenues of at least €750 million and Austrian online advertising revenues of at least €25 million, excluding smaller domestic 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.⁹⁷ A covered service is deemed to have been

⁹⁴ Australian Attorney-General’s Department. (2026, August 31). *Privacy Reform – Consultation on Exposure Draft legislation*. <https://consultations.ag.gov.au/rights-and-protections/privacy-reform/>

⁹⁵ Office of the Australian Information Commissioner. (2026, March 31). *Draft Children’s Online Privacy Code (consultation for industry, civil society, academia)*. <https://www.oaic.gov.au/engage-with-us/consultations/draft-childrens-online-privacy-code-consultation-for-industry-civil-society-academia>

⁹⁶ KPMG. (2019, October 29). *Austria: Legislation Introducing Digital Services Tax*. <https://home.kpmg/us/en/home/insights/2019/10/tmf-austria-legislation-introducing-digital-services-tax.html>

⁹⁷ Austrian Federal Ministry of Finance. (n.d.). *Digital Tax Act 2020*. <https://www.bmf.gv.at/en/topics/taxation/digital-tax-act.html>

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 appears to reflect both discriminatory intent and impact, given that no such tax applies to traditional advertising, including that supplied by broadcasters by domestic suppliers. 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.⁹⁸ Annual digital services tax receipts reached €137.1 million in 2025. Collections totaled €95.6 million in January-July 2026, up 25.5% from the same period in 2025.⁹⁹ This tax regime risks distorting competition, discouraging foreign investment, and undermining the principles of non-discrimination in international trade. Although individual payers are not made public, the thresholds result in Austrian firms benefiting from a *de facto* exemption¹⁰⁰ thus implicating the discriminatory effect USTR identified in its Section 301 finding in 2021. USTR should refresh the record on this finding and consider an appropriate response.

Austria has enacted a Parcel Delivery Tax Act, effective October 1, 2026, imposing €2 per parcel on covered business-to-consumer distance sales delivered in Austria, with an alternative calculation per order.¹⁰¹ The tax applies where Austrian distance-sales revenues exceeded €100 million in the preceding fiscal year. Sales facilitated through online marketplaces are attributed to the marketplace, which becomes liable when the threshold is exceeded. Covered suppliers without an establishment in the EU or EEA must appoint an Austrian tax representative. These obligations create additional tax and administrative costs for covered U.S. online retailers and marketplaces.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Austria’s “digital-sovereignty” measures adopted in November 2025¹⁰² and its March 2026 Public AI Initiative promote government use of European cloud infrastructure and European AI models.¹⁰³ The AI initiative directs ministries to favor integration with the

⁹⁸Kurz, 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]. X. <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
⁹⁹ Austrian Federal Ministry of Finance. (2026). *Abgabenerfolg des Bundes (UG 16): Juli 2026*, “Digitalsteuer” row. https://service.bmf.gv.at/budget/akthh/2026/202607_HTML_UG16_F.htm

¹⁰⁰ <https://www.mondaq.com/Article/826030>

¹⁰¹ Austrian Federal Ministry of Finance. (2026, August 5). *Parcel Delivery Tax: Overview and FAQs*. https://www.bmf.gv.at/en/topics/taxation/parcel_delivery_tax_overview_and_faq.html

¹⁰² Austrian Federal Government. (2025, November 12). *Maßnahmen zur Stärkung der digitalen Souveränität der österreichischen Verwaltung im Zuge der Umsetzung des Digital Austria Act 2.0* [Cabinet paper 30/13], measures 5–7. https://www.bundestkanzleramt.gv.at/dam/jcr:25e542d4-887a-44f9-8076-63a6e524e83b/30_13_mrv.pdf

¹⁰³ Austrian Federal Government. (2026, March 19). *Public AI Initiative zur Modernisierung der Verwaltung – Künstliche Intelligenz als Hebel für eine souveräne, effiziente und bürgernahe Verwaltung* [Cabinet paper 45a/1], sections 1–2. https://www.bundestkanzleramt.gv.at/dam/jcr:c35699e9-76c6-43bb-b973-0747eccc90ed/45a_1_mrv.pdf

Federal Computing Centre's shared language-model service in development and procurement, while allowing additional models and certain external cloud applications. A May 2026 implementation report also describes preferential use of in-house cloud procurement and limited use of non-European cloud services, principally with EU/EEA server locations. These preferences raise concerns about U.S. suppliers' access to public-sector opportunities and Austria's compliance with its WTO GPA obligations. CCIA encourages USTR to ensure that Austria applies objective security and performance criteria without discriminating against suppliers based on origin.

Discriminatory Local Content Quotas and Audiovisual Services Mandates

In May 2026, Austria's Culture Ministry proposed a separate 5% levy on music-streaming services generating more than €2 million in annual Austrian revenues, including subscription and advertising revenues. The May draft envisaged implementation from January 1, 2027, with proceeds supporting Austria's music sector. As of October, legislation implementing this proposal had not advanced but the proposal warrants continued monitoring, given its discriminatory impact. Austria is also developing a levy and investment obligation for audiovisual streaming services to support domestic film production.¹⁰⁴ A model described by the Austrian Economic Chamber in May 2026 would impose a 7% levy plus either a further 5% levy or 5% direct investment in film production, with the public broadcaster ORF exempt. In September 2026, the Economy Ministry confirmed that an Austrian investment-obligation model remained under development.¹⁰⁵ Depending on its final design, the measure could impose substantial additional costs on U.S. streaming suppliers and redirect investment toward domestic production.

Azerbaijan

Government-Imposed Restrictions on Internet Content and Access Barriers

On June 30, 2026, Azerbaijan's Parliament passed omnibus amendments to its information and child protection laws requiring foreign social media platforms to establish local branch offices, enforce account bans for users under 16, and execute content removal orders within 24 hours. Non-compliance exposes foreign platforms to advertising bans and bandwidth throttling between 50% and 90%, creating severe access barriers for U.S. digital service exporters. CCIA urges

¹⁰⁴ Austrian Economic Chamber. (2026, May 18). *WKÖ-Fachverband Telekom/Rundfunk: Massive Kritik an Plänen für 12%-Streamingabgabe* [Press release]. https://www.ots.at/presseaussendung/OTS_20260518_OTS0050/wkoe-fachverband-telekomrundfunk-massive-kritik-an-plaenen-fuer-12-streamingabgabe

¹⁰⁵ Austrian Federal Ministry for Economy, Energy and Tourism. (2026, September 10). *Hattmannsdorfer: Investment Obligation für Film muss Arbeitsplätze schaffen und Österreich im Wettbewerb stärken*. <https://www.bmwet.gv.at/Presse/AktuellePressemeldungen/streamingabgabe.html>

USTR to address mandatory establishment and bandwidth throttling penalties as explicit, trade-distorting market access barriers.

Bangladesh

Customs

Bangladesh maintains a significant tax differential between imported and locally manufactured mobile devices maintaining an effective tax burden¹⁰⁶ on imported smartphones that is currently 64.25% (up from 43.43% last year).¹⁰⁷ By contrast, locally manufactured phones face an effective tax burden of 5-17%,¹⁰⁸ benefiting from reduced customs duty on imported parts and components (cut from 10% to 5%), a lower advance income tax (AIT) on 22 raw materials used in local manufacturing, and conditional VAT exemptions. The widening gap between tax rates applicable to imported and locally manufactured devices significantly disadvantages companies that do not maintain local manufacturing operations in Bangladesh¹⁰⁹ and warrants evaluation as a form of discrimination proscribed by GATS Article III.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

On April 10, 2026, Bangladesh enacted the Personal Data Protection Act and National Data Management Act, replacing the corresponding 2025 ordinances.¹¹⁰ The final personal-data law removes earlier express localization requirements and criminal penalties for company officials, but retains restrictions affecting cross-border services. Section 29 conditions overseas transfers on specified grounds, including consent or contractual arrangements, and limits destinations to those meeting technology and infrastructure requirements prescribed by regulation. Large-scale transfers of specified sensitive identifying data also require notification to the regulator. These requirements may significantly constrain U.S. providers' use of global infrastructure to offer services in Bangladesh, depending on implementation. Section 29(5) additionally authorizes government-imposed fees or charges on annual profits arising from the use of Bangladeshi citizens' personal data, creating uncertainty over potential additional costs and consistency with the 2004 U.S.-Bangladesh Tax Treaty, designed to prevent double taxation.

¹⁰⁶ "Effective tax burden" combines customs duties and domestic taxes.

¹⁰⁷ Bangladesh Minister of Finance. (2026). *National Budget Speech*.
https://customs.gov.bd/files/BudgetSpeech_2026_2027_E.pdf.

¹⁰⁸ Counterpoint Research. (2026). *Impact of Rising Import Duties on Bangladesh's Handset Market*.
<https://counterpointresearch.com/en/insights/impact-rising-import-duties-bangladeshs-handset-market>.

¹⁰⁹ <https://observerbd.com/news/597018>.

¹¹⁰ Government of Bangladesh. (2026, April 10). *Personal Data Protection Act, 2026 (Act No. 63 of 2026), section 44*. <https://bdlaws.minlaw.gov.bd/act-print-1692.html>

The National Data Management Act, 2026 also creates potential localization risks.¹¹¹ Sections 30(6) and 32 provide for mandatory database integration with the national data-exchange framework and allow the authority to require data covered by the Act's schedule to be incorporated into the national data-repository system. Section 31 permits restrictions on the interoperability, exchange, and sharing of data classified as nationally important or sensitive. Depending on implementation, these powers could constrain foreign cloud providers' use of overseas infrastructure.

In the U.S.–Bangladesh Agreement on Reciprocal Trade signed on February 9, 2026,¹¹² Bangladesh committed to facilitate business-related data transfers across trusted borders and refrain from discriminating against U.S. digital products and U.S. digital service suppliers. USTR should seek implementation of these commitments through Bangladesh's data governance regulations.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

The Bangladesh government has historically taken an aggressive stance against digital services platforms relating to content, particularly involving American companies. During July 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.¹¹³ The State 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.¹¹⁴ Social media access was restored later that month.¹¹⁵

Bangladesh's 2026 telecommunications reforms introduced restrictions on internet shutdowns and procedural safeguards for interception.¹¹⁶ However, the subsequent parliamentary legislation weakened some safeguards, and the framework continues to permit broad surveillance and

¹¹¹ Mahmood, S. (2026). *A New Digital Frontier: A Roadmap for Rights-Respecting Digital Governance Laws in Bangladesh* (2nd ed.). Tech Global Institute.

<https://techglobalinstitute.com/wp-content/uploads/2026/09/WHITE-PAPER-BANGLADESH.pdf>

¹¹² Office of the United States Trade Representative. (2026, February 9). *Agreement Between the United States of America and the People's Republic of Bangladesh on Reciprocal Trade*, Article 3.2.

<https://ustr.gov/sites/default/files/files/Press/Releases/2026/U.S.%20BGD%20Agreement%20on%20Reciprocal%20Trade%20Final%2009FEB2026%20LETTER.pdf>

¹¹³ The Daily Star. (2024, July 27). *Social Media Off-Limits Indefinitely*.

<https://www.thedailystar.net/news/bangladesh/news/social-media-limits-indefinitely-3662216>

¹¹⁴ 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>

¹¹⁵ Digitally Right & Open Observatory of Network Interference. (2025, July 31). *The Longest Silence: Internet Shutdowns During Bangladesh's 2024 Uprising*. <https://ooni.org/post/2025-bangladesh-report/>

¹¹⁶ Government of Bangladesh. (2026, February 5). *Bangladesh Telecommunication Regulation (Amendment) Ordinance, 2026 (Ordinance No. 25 of 2026)*, sections 64–65. <https://bdlaws.minlaw.gov.bd/act-print-1618.html>

binding directions to service providers with limited independent oversight.¹¹⁷ Compelled assistance and access to communications data create operational and privacy risks for digital suppliers. These powers should be subject to narrowly defined grounds, independent authorization, and effective avenues for challenge.

Bangladesh replaced the Cyber Security Act, 2023¹¹⁸ with a 2025 ordinance¹¹⁹ and enacted the Cyber Security Act, 2026¹²⁰ on April 10, 2026. Section 8 retains removal and blocking powers on grounds including cybersecurity, national security, and public order. It also requires tribunal approval within three days, with restoration of affected content if approval is not obtained, and public disclosure of blocked content. Despite these safeguards, broadly framed blocking grounds continue to create uncertainty for online platforms. Further amendments proposed in September 2026¹²¹ would expand speech-related offenses, including defamation and broadly defined forms of humiliation and bullying. If adopted, these provisions could increase pressure on platforms to restrict lawful expression.

Other Barriers to Digital Trade

On July 22, 2026, the Ministry of Commerce published the draft Cross-Border Digital Commerce Policy, 2026.¹²² Clause 5.3 would require foreign digital-commerce companies to obtain Bangladeshi DBID registration for online retail sales. Clause 8.3 would prohibit dissemination of foreign advertisements without establishment of a company in Bangladesh, a form of discrimination that may be inconsistent with the ART. If adopted, these requirements could restrict cross-border advertising and increase market-entry costs for U.S. suppliers. USTR should urge Bangladesh to avoid conditioning cross-border digital advertising on local establishments.

¹¹⁷ Human Rights Watch et al. (2026, July 28). *Joint Letter to Prime Minister Tarique Rahman Re: Surveillance and Interception in Bangladesh*.

<https://www.hrw.org/news/2026/07/28/joint-letter-to-prime-minister-tarique-rahman-re-surveillance-and-interception-in>

¹¹⁸ Government of Bangladesh. (2023, September 18). *Cyber Security Act, 2023 (Act No. 39 of 2023)*.

<https://bdlaws.minlaw.gov.bd/act-print-1457.html>

¹¹⁹ Government of Bangladesh. (2025, May 21). *Cyber Protection Ordinance, 2025 (Ordinance No. 25 of 2025)*.

<https://bdlaws.minlaw.gov.bd/act-print-1538.html>

¹²⁰ Government of Bangladesh. (2026, April 10). *Cyber Protection Act, 2026 (Act No. 81 of 2026)*.

<https://bdlaws.minlaw.gov.bd/act-print-1710.html>

¹²¹ Islam, Z. (2026, September 14). *Cyber security act: Draft changes echo DSA-era restrictions*. The Daily Star.

<https://www.thedailystar.net/news/bangladesh/news/cyber-security-act-draft-changes-echo-dsa-era-restrictions-4272271>

¹²² The Business Standard. (2026, July 25). *Govt to enforce registration for foreign cos like Facebook, YouTube, Google to run ads in Bangladesh*.

<https://www.tbsnews.net/bangladesh/govt-enforce-registration-foreign-digital-platforms-run-ads-bangladesh-1497896>

Taxation of Digital Products and Services

In its Finance Act 2026 passed on June 29, 2026, Bangladesh expanded the scope of its domestic Permanent Establishment (PE) definition under Section 2(92) of the Income Tax Act, 2023, to include significant “digital” or “online” activity or presence in Bangladesh by a non-resident entity. The new law deems a non-resident entity to constitute a PE in Bangladesh if the entity has 100,000 or more digital or online customers/subscribers, irrespective of any physical presence in Bangladesh. The applicable tax rate is the same 27.5% corporate income tax applicable to domestic corporations. How profits of a digital supplier will be attributed to Bangladesh remains unclear, however, as is the relief available under tax treaties (including the U.S.-Bangladesh Tax Treaty of 2004). Given the explicit targeting of foreign digital service exporters and risks of double-taxation USTR should carefully monitor implementation, to ensure that it is compliant with Article 3.1 (Digital Services Taxes) of the U.S.-Bangladesh Agreement on Reciprocal Trade.

Belgium

Taxation of Digital Products and Services

On April 17, 2026, Belgian lawmakers introduced Bill 56K1491 proposing a 3% digital services tax, with a proposed effective date of January 1, 2027.¹²³ The bill remains pending and would cover groups with consolidated worldwide revenue exceeding €750 million and Belgian taxable revenue exceeding €3 million. It targets online advertising, digital intermediation, and the sale or exploitation of user data. For intermediation, the text defines the taxable base as the total value of transactions facilitated between users where at least one is Belgian, potentially extending taxation beyond the platform’s own fees. These provisions would create significant tax and compliance burdens for U.S. digital suppliers and USTR should oppose this as a form of unjustified discrimination against U.S. suppliers.

A separate bill introduced on May 22, 2026 (56K1572), proposes digital permanent establishment rules, deemed-profit taxation, and a digital withholding mechanism, a more direct way of taxing profits of cross-border suppliers—a DST by another name¹²⁴ It would establish taxable presence for foreign businesses exceeding specified Belgian user, connection, or contract thresholds without requiring physical presence. The proposal also imposes reporting obligations and attributes revenue using digital activity measures. These provisions raise the same concerns

¹²³ Belgian Chamber of Representatives. (2026, April 17). *Proposition de loi modifiant le Code des droits et taxes divers, instaurant une taxe sur les services numériques* (DOC 56 1491/001, Articles 6 and 10). <https://www.lachambre.be/FLWB/PDF/56/1491/56K1491001.pdf>

¹²⁴ Belgian Chamber of Representatives. (2026, May 22). *Proposition de loi visant à adapter le Code des impôts sur les revenus 1992 à l'économie numérique* (DOC 56 1572/001). <https://www.dekamer.be/FLWB/PDF/56/1572/56K1572001.pdf>

of DSTs about overlapping taxation, double taxation, and additional compliance costs for U.S. suppliers serving Belgium remotely.¹²⁵

Discriminatory Local Content Quotas and Audiovisual Services Mandates

Belgium's regional audiovisual contribution regimes impose additional costs on foreign streaming and video-sharing services.¹²⁶ In the French Community, the contribution rate for covered providers with relevant annual turnover of at least €150 million rises to 7.55% of revenue in 2026 and 9.5% in 2027.¹²⁷ Providers choosing to contribute through direct investment must allocate at least 35% of that investment to French-speaking Belgian productions. On March 26, 2026, the Constitutional Court rejected most of Netflix's challenges but referred questions to the Court of Justice of the European Union concerning eligible investments, the allocation of fund payments, and recognition of contributions imposed by other Member States. These requirements constrain investment choices and raise concerns about overlapping obligations across markets, seriously affecting a suppliers' ability to offer pan-European services.

Flanders' expanded contribution regime, effective January 1, 2025, also covers video-sharing platforms.¹²⁸ Its 2026 implementation includes contributions from major U.S. streaming suppliers and lists Google, Meta, Snap, and Twitch among video-platform contributors, subject to pending Constitutional Court litigation.¹²⁹ Covered services must support qualifying audiovisual productions through direct co-production investment or payments to the Flemish Audiovisual Fund, extending production-financing obligations to platforms distributing user-generated content.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Belgium's June 19, 2022 copyright law establishes nonwaivable remuneration rights for authors and performers against covered online content-sharing and streaming services, including where the relevant exclusive rights have been transferred, imposing mandatory licensing for all but the most cursory extracts ("snippets").¹³⁰ These requirements raise concerns about additional payment obligations alongside existing licenses and the complexity of cross-border licensing. The law also authorizes the Belgian Institute for Postal Services and Telecommunications (BIPT)

¹²⁵ See: <https://taxfoundation.org/testimony/belgium-digital-tax-proposal/>.

¹²⁶ Belgian Constitutional Court. (2026, March 26). *Arrêt n° 36/2026*.

<https://fr.const-court.be/public/f/2026/2026-036f.pdf>

¹²⁷ Vlaams Audiovisueel Fonds. (n.d.). *Stimuleringsregeling*. <https://www.vaf.be/creatie/stimuleringsregeling>

¹²⁸ Vlaamse Regulator voor de Media. *Jaarlijks verslag vernieuwde stimuleringsregeling*.

<https://www.vlaamseregulatormedia.be/nl/jaarlijks-verslag-vernieuwde-stimuleringsregeling>

¹²⁹ Vlaams Audiovisueel Fonds. (n.d.). *Stimuleringsregeling*. <https://www.vaf.be/creatie/stimuleringsregeling>

¹³⁰ Belgium. (2022, June 19). *Loi transposant la directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE* (Articles 54 and 62).

https://www.ejustice.just.fgov.be/cgi/article_body.pl?caller=list&language=fr&numac=2022015053&pub_date=2022-08-01

to resolve disputes over remuneration for covered online uses of press publications through binding decisions following unsuccessful good-faith negotiations.

On July 6-7, 2026, the Court of Justice of the European Union heard Case C-663/24, *Streamz and Others*,¹³¹ concerning challenges to these provisions by Google, Meta, Spotify, and other companies. The plaintiffs challenged the compatibility of mandatory compensation with EU copyright rules, freedom to provide services, and freedom to conduct a business. The case is ongoing.

Bhutan

Taxation of Digital Products and Services

Bhutan enacted an SEP in its Income Tax Act 2025 (in force since January 1, 2026). A non-resident is deemed to have a SEP in Bhutan if the aggregate value of digital services supplied to users in Bhutan exceeds Nu. 5 million (approximately \$52,000 USD) in any Income Year. This threshold applies on an aggregate basis across all digital services provided by the non-resident to users in Bhutan, and captures a disproportionate wide range of foreign companies because of the low amount. The applicable tax rate is 5% on gross revenues or 22% of net income. This unilateral revenue tax explicitly targets foreign digital service exporters and creates severe double-taxation risks. CCIA urges USTR to request that Bhutan withdraw its unilateral SEP tax in favor of multilateral consensus.

Bolivia

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Bolivia maintains public-sector data localization requirements under its Free Software and Open Standards Implementation Plan (PISLEA), approved by Supreme Decree No. 5322 on January 23, 2025.¹³² Section 4.4 requires covered public entities to store non-public government data in their own infrastructure or state-operated cloud services within Bolivia, restricting opportunities for U.S. commercial cloud suppliers. Public data may use open platforms, provided that local backups remain in state technological infrastructure. The provision does not define “public” and “non-public” data, creating uncertainty over the restriction’s scope. 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.

¹³¹ Court of Justice of the European Union. (n.d.). *Hearing: Case C-663/24 Streamz and Others*. https://curia.europa.eu/site/jcms/p1_1000084836/en/hearing-case-c-663/24-streamz-and-others

¹³² Bolivia. (2025). *Plan de Implementación de Software Libre y Estándares Abiertos (PISLEA)* (Decreto Supremo N° 5322, annex). <https://agetic.gob.bo/sites/default/files/2025-02/ANEXO-DS-5322.pdf>

Bolivia's Financial System Supervision Authority (ASFI) maintains one of the most restrictive cloud-adoption regimes in the region for financial institutions. ASFI revised its cloud-services framework in 2026. Circular ASFI/926/2026 of February 11 introduced cloud requirements for supervised securities-market entities, including written prior "no objection," supporting documentation, risk assessments, and data-protection procedures.¹³³ Circular ASFI/955/2026 of June 11 established a dedicated cloud-services section in the financial-services information-security regulation, covering implementation projects, criteria and requirements for ASFI's no-objection process, contractual obligations, rejection, and service suspension or restriction.¹³⁴ The June changes apply to new contracts from publication in ASFI's regulatory gazette. These requirements can increase compliance costs and delay deployment of U.S. cloud services. Bolivia should replace prior approval with a notification mechanism with clear timelines and checklists, accept internationally recognized certifications (e.g., ISO 27001, SOC) in lieu of per-contract documentation and on-site audits, and eliminate the mandatory on-premises alternate site where the provider offers native cross-zone redundancy.

Brazil

Asymmetric Platform Regulation

Brazil continues to consider legislation imposing asymmetric regulation on digital service suppliers. Bill 2,768/2022, which would assign ANATEL a central role in regulating digital platforms, remains pending.¹³⁵ Separately, the government introduced Bill 4,675/2025 on September 18, 2025, proposing a new digital markets regime administered by Brazil's competition authority, CADE.¹³⁶ The latter bill remains pending in the Chamber of Deputies but is subject to streamlined debate under an urgency procedure. The proposed framework grants Brazil's Administrative Council for Economic Defense (CADE) broad powers to regulate digital services through a newly created Special Superintendence for Systemic Relevance, Free Competition and Consumer Protection in Digital Markets. This body would designate companies as "systemically relevant" and determine and apply special obligations to designated companies on a case-by-case basis. The bill provides CADE broad authority and open-ended criteria to designate companies, including a revenue threshold of R50 billion globally or R5 billion in Brazil, combined with qualitative characteristics including, but not limited to, operating multi-sided platforms and access to significant amounts of personal and business user data. A

¹³³ Autoridad de Supervisión del Sistema Financiero (ASFI). (2026, March). *Boletín informativo trimestral de actualización y emisión de normativa*, No. 71, pp. 9–10.

<https://www.asfi.gob.bo/sites/default/files/2026-04/Bolet%C3%A9n%2071%20-%20marzo%202026.pdf>

¹³⁴ Autoridad de Supervisión del Sistema Financiero (ASFI). (2026, June). *Boletín informativo trimestral de actualización y emisión de normativa*, No. 72, pp. 17–18.

<https://www.asfi.gob.bo/sites/default/files/2026-07/Bolet%C3%A9n%2072%20-%20junio%202026.pdf>

¹³⁵ Ortiz, A. *Parecer da Relatora ao Projeto de Lei nº 2.768, de 2022* [PRL 1 CDE, including substitute text]. Câmara dos Deputados. https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=3128531

¹³⁶ Brazilian National Congress. *Projeto de Lei nº 4.675/2025*.

<https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-4675-2025>

substitute bill submitted by the rapporteur on July 8, 2026 would permit CADE to designate economic groups as “systemically relevant” where annual revenue exceeds R\$50 billion globally or R\$5 billion in Brazil and certain qualitative factors are met.¹³⁷ Designations could last up to six years. Special obligations would require a separate administrative proceeding and would be tied to specified products or services. Potential obligations include interoperability and data portability, transparency concerning commercial terms and ranking, restrictions on self-preferencing and tying, and notification of acquisitions for informational purposes. Designated firms would also be required to maintain a juridical presence in Brazil. Obligations could take effect within 90 days after publication of the relevant decision. The Finance Ministry has consistently stated that no more than 5–10 companies would be designated, and that these will include the DMA's "gatekeeper" companies — which are largely U.S. companies (e.g., Amazon, Apple, Meta, and Microsoft).

As with the original bill, these procedural revisions still result in a regime where certain suppliers are subject to significant commercial constraints their competitors do not face, despite the absence of proven harm to competition. The thresholds and designation criteria are likely to disproportionately capture major U.S. digital services suppliers, although companies from other jurisdictions could also qualify. Mandatory changes to integrated services, interoperability requirements, local establishment costs, and potentially substantial competition-law penalties could discourage investment and product development and deprive consumers of innovative products and services. CCIA urges USTR to continue pressing the Brazilian government not to advance such an unnecessary, burdensome and likely discriminatory measure.

Enforcement under existing competition law has also produced significant changes to digital services. In December 2025, CADE approved a settlement with Apple concerning its iOS ecosystem, including commitments relating to alternative app stores, alternative payment methods, and links to external purchasing options.¹³⁸ Apple announced corresponding changes for Brazil on June 18, 2026, while identifying associated privacy, security, and child-protection risks and describing safeguards intended to mitigate them.¹³⁹ These commitments arise from a specific competition proceeding and distinct from the obligations contemplated under the pending digital-markets legislation.

CCIA also urges USTR to monitor enforcement under Brazil’s existing competition law to ensure that remedies affecting digital services rest on demonstrated competitive harm, account for efficiencies and consumer benefits, and provide due process and meaningful judicial review.

¹³⁷ Machado, A. (2026, July 8). *Substitutivo ao Projeto de Lei nº 4.675/2025 [PRLP 1]*, proposed Article 47-C, §§ 1–2. Câmara dos Deputados. https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=3159491

¹³⁸ Conselho Administrativo de Defesa Econômica (CADE). (2025, December 23). *Cade homologa TCC em investigação sobre práticas da Apple no iOS*. <https://www.gov.br/cade/pt-br/assuntos/noticias/cade-forma-maioria-pela-homologacao-de-tcc-em-investigacao-sobre-praticas-da-apple-no-ios>

¹³⁹ Apple. (2026, June 18). *Apple announces changes to iOS in Brazil*. <https://www.apple.com/newsroom/2026/06/apple-announces-changes-to-ios-in-brazil/>

Barriers to the Deployment and Operation of Network Infrastructure

Brazil's tax treatment of digital infrastructure has been a persistent concern for U.S. technology providers. Since late 2025, imported data-center equipment faced a compounded federal tax burden (reported at approximately 48.94%) — combining import duties, industrial product taxes (IPI), and social contributions (PIS/COFINS) — while a Chinese competitor benefited from favorable treatment through an Export Processing Zone (ZPE) arrangement, creating an uneven playing field for U.S. investors. This asymmetry disadvantaged U.S. companies that had already committed significant capital to the Brazilian market and risks distorting future investment decisions.

On September 15, 2026, President Lula signed Bill 278/2026 into law, establishing the Special Taxation Regime for Data Center Services ("ReData"), which suspends import duties, IPI, PIS/Pasep, and COFINS (including on imports) on ICT equipment and components intended for data centers for up to five years, converting to a permanent exemption once obligations are met. While ReData responds to the headline tax-burden concern for qualifying investments, it does not fully resolve the underlying issues and introduces new ones. First, the import-duty benefit applies only to products with no equivalent manufactured in Brazil, and the Manaus Free Trade Zone retains distinct treatment. Second, eligibility is tied to local-content and localization mandates that raise their own market-access concerns: participants must dedicate at least 10% of processing/storage capacity to the Brazilian market (which may not be exported or retained abroad), meet sustainability and water-efficiency criteria, source renewable/low-emission electricity, invest locally an amount equivalent to 2% of the value of products purchased using the benefits, and steer 40% of digital-economy investment to the North, Northeast, and Midwest regions. Program entry requires Ministry of Finance authorization, and non-compliance can trigger claw-back of suspended taxes with interest and penalties, or revocation of eligibility. USTR should monitor implementation — particularly the localization and local-content conditions and any residual asymmetry versus incentives previously extended to specific competitors — to ensure the regime does not simply substitute one form of discriminatory, trade-distorting treatment for another.

Brazil's General Telecommunications Law maintains local establishment requirements that can impede cross-border supply.¹⁴⁰ Article 133 requires providers seeking authorization for telecommunications services deemed of "collective interest" to be constituted under Brazilian law, with headquarters and administration in Brazil. Article 86 separately imposes requirements on concession holders, including maintaining an exclusive telecommunications purpose. For foreign satellite services, Article 171 requires that the service be offered through a Brazilian-established legal representative and gives preference to Brazilian satellites where they offer equivalent conditions. These requirements increase entry costs and limit the ability of U.S.

¹⁴⁰ Presidência da República. (1997, July 16). *Lei nº 9.472, de 16 de julho de 1997* (as amended), Articles 86 and 133(I). https://www.planalto.gov.br/ccivil_03/leis/19472.htm

suppliers to serve Brazil through their existing international operations. CCIA urges USTR to engage with Brazil with a view to removing nationality-based satellite preferences and establishment and representation requirements.

Brazil has begun taking steps to reverse its 2021 policy permitting unlicensed use of spectrum across the full 1,200 MHz of the 6 GHz band, a policy that contributed greatly to expanded internet access in Brazil. Following Resolution 772/2025, ANATEL opened Public Consultation 37/2026 in September 2026 on an auction of the upper 700 MHz, covering 6,425–7,125 MHz, with the auction contemplated by 2028.¹⁴¹ The proposal includes mobile coverage and regional digital infrastructure commitments, including data centers. These developments deepen uncertainty for U.S. equipment and services suppliers that invested in products and services dependent on Wi-Fi. Reducing spectrum available for unlicensed technologies risks constraining Wi-Fi capacity and requiring Brazil-specific product changes. CCIA urges USTR to advocate for predictable spectrum policy, meaningful consideration of existing investments, and sufficient transition arrangements.

ANATEL's Act 4,141 of April 11, 2025 establishes coordination priorities and interference-protection conditions for non-geostationary satellite systems.¹⁴² Its tables were amended in March 2026 through Acts 3,023 and 3,084.¹⁴³ For specified systems and frequency bands, an operator may neither cause harmful interference nor claim protection against higher-priority systems until the necessary coordination agreements are obtained. These conditions can serve to ensconce legacy systems and can increase uncertainty and operating costs for new entrants, including U.S. satellite suppliers, particularly where deployment requires negotiations with competing operators who have no incentive to reach agreement. CCIA urges transparent, technically justified coordination criteria and timely mechanisms for resolving disputes so that incumbent priority does not become an unnecessary obstacle to entry or expansion.

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,

¹⁴¹ Agência Nacional de Telecomunicações (ANATEL). (2026, September 4; updated September 8). *Edital de licitação da faixa de 6 GHz vai à consulta pública*.

<https://www.gov.br/anatel/pt-br/assuntos/noticias/edital-de-licitacao-da-faixa-de-6-ghz-vai-a-consulta-publica>

¹⁴² Agência Nacional de Telecomunicações (ANATEL). (2025, April 11). *Ato nº 4141, de 11 de abril de 2025* (as amended), Articles 1–6 and Annex.

<https://informacoes.anatel.gov.br/legislacao/atos-complementares-de-regulacao/2083-ato-4141>

¹⁴³ Agência Nacional de Telecomunicações (ANATEL). (n.d.). *Atos Complementares de Regulação* (entries for Ato nº 3023, de 2 de março de 2026, and Ato nº 3084, de 3 de março de 2026).

<https://informacoes.anatel.gov.br/legislacao/atos-complementares-de-regulacao>

the government introduced updated guidance for the ex-tarifário program,¹⁴⁴ 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 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 documentation requirements and opportunities for domestic producers to contest applications increase uncertainty over whether specialized imported equipment will receive tariff relief.

Domestic producers may contest applications, although the rules require supporting technical information and prohibit generic objections. The substantive concern is the narrow equivalence test: Article 14 of Resolution GECEX 512/2023 focuses on the equipment’s essential function and expressly excludes interoperability, operating costs, monitoring capabilities, maintenance features, and other auxiliary characteristics from that definition. CCIA is concerned that this test can deny tariff relief where locally produced equipment performs the same basic function but does not meet an importer’s operational requirements, thereby restricting access to specialized U.S. ICT and capital goods. 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.

Brazil adopted CONAMA Resolution 516 of July 8, 2026, establishing restrictions on ten hazardous substances in electrical and electronic equipment.¹⁴⁵ The measure introduces a national equipment registry, conformity declarations, and Portuguese-language technical documentation requirements, with phased substance-specific compliance deadlines. Although the restricted substances correspond to those covered by the EU’s RoHS framework, additional Brazilian registration and documentation requirements may create duplicative compliance costs for U.S. ICT suppliers. CCIA urges implementation that recognizes reliable international compliance documentation, provides workable transition periods, and avoids unnecessary testing and administrative duplication.

Changes to equipment tariffs in 2026 have compounded uncertainty for digital infrastructure investment. Resolution GECEX 852/2026 increased duties on numerous capital and information

¹⁴⁴ Comitê-Executivo de Gestão da Câmara de Comércio Exterior (GECEX). (2023, August 16). *Resolução GECEX nº 512, de 16 de agosto de 2023*.

<https://www.in.gov.br/en/web/dou/-/resolucao-gecex-n-512-de-16-de-agosto-de-2023-503880256>

¹⁴⁵ Conselho Nacional do Meio Ambiente (CONAMA). (2026, July 8). *Resolução CONAMA nº 516, de 8 de julho de 2026*, Article 4. <https://www.in.gov.br/web/dou/-/resolucao-conama-n-516-de-8-de-julho-de-2026-718408936>

technology goods,¹⁴⁶ while subsequent measures, including Resolution 866/2026, reversed selected increases and provided additional tariff relief.¹⁴⁷ The remaining burden therefore depends on the equipment's tariff classification and eligibility for exemptions. CCIA urges Brazil to remove duties on essential digital infrastructure equipment and provide predictable access to relief where domestic products do not offer commercially and technically equivalent capabilities. Claims of domestic equivalence should be assessed against performance, reliability, security, and compatibility requirements rather than broad product categories.

Discriminatory Local Content Quotas and Audiovisual Services Mandates

Brazil is currently considering streaming legislation, based on a bill approved by the Chamber of Deputies in November 2025.¹⁴⁸ As of October 2026 the measure remains pending in the Senate as the Chamber's substitute to Bill 2,331/2022.¹⁴⁹ The bill would extend CONDECINE (quotas and fees applicable to traditional broadcasting) to streaming services through progressive revenue-based schedules, reaching 4% for video-on-demand and internet television services and 0.8% for audiovisual content-sharing services. It also provides a 75% tax reduction for qualifying services whose offerings contain more than 50% Brazilian content.

The proposal additionally establishes Brazilian-content availability and prominence obligations, with a phased catalog quota for Brazilian works reaching 10% and an alternative based on offering more than 700 Brazilian works, half independent. It would require certain device interfaces to provide direct access to public communication and broadcast services. Article 7(8) expressly denies specified quota exemptions to providers controlled by, affiliated with, operating as a branch of, or otherwise dependent on a foreign legal entity. These include exemptions for services with fewer than 200,000 registered Brazilian users or incompatible thematic offerings, and relief from the independent-production component for providers below the highest CONDECINE rate. Separately, Article 8 would require VOD and internet television providers with annual gross revenue exceeding R\$500 million to carry designated public-communication content without additional charges to users. Article 16 would prohibit streaming availability of films commercially released in Brazilian cinemas until nine weeks after their theatrical release. These nationality-based benefits and mandated distribution advantages will disadvantage U.S. streaming services, content, and device suppliers, distort investment decisions, and constrain

¹⁴⁶ Comitê-Executivo de Gestão da Câmara de Comércio Exterior (GECEX). (2026, February 4). *Resolução GECEX nº 852, de 4 de fevereiro de 2026*, Article 1 and Annex.

<https://www.in.gov.br/web/dou/-/resolucao-gecex-n-852-de-4-de-fevereiro-de-2026-685397607>

¹⁴⁷ Comitê-Executivo de Gestão da Câmara de Comércio Exterior (GECEX). (2026, February 27). *Resolução GECEX nº 866, de 27 de fevereiro de 2026*, Articles I–4 and Annexes I–III.

<https://www.in.gov.br/web/dou/-/resolucao-gecex-n-866-de-27-de-fevereiro-de-2026-689563567>

¹⁴⁸ Congresso Nacional. *Projeto de Lei nº 2331, de 2022—Tramitação bicameral* (Chamber approval recorded November 5, 2025). <https://www.congressonacional.leg.br/materias/materias-bicameras/-/ver/pl-2331-2022>.

¹⁴⁹ Senado Federal. *Projeto de Lei nº 2331, de 2022 (Substitutivo da Câmara dos Deputados)* [Legislative record; status verified September 18, 2026]. <https://www25.senado.leg.br/web/atividade/materias/-/materia/171663>.

consumer choice, as CCIA has previously noted.¹⁵⁰ CCIA urges USTR to oppose these proposed discriminatory fiscal preferences and disproportionate catalog, prominence, and interface mandates.

Government-Imposed Content Restrictions and Related Access Barriers

Brazil's Classificação Indicativa framework applies age classifications to covered media, applications, and digital services.¹⁵¹ Its expanding application to online platforms creates concerns regarding the transparency and consistency of classification decisions and their interaction with age-assurance and parental-supervision requirements. CCIA urges authorities to publish clear criteria, identify the evidence supporting adverse decisions, provide effective opportunities for review, and account for services' safety features and parental tools. Comparable services should receive consistent treatment regardless of nationality.

Brazil has substantially expanded internet application providers' exposure to liability for third-party content. In June 2025, the Federal Supreme Court found Article 19 of the Marco Civil da Internet partially unconstitutional and established differentiated liability standards.¹⁵² On June 17, 2026, the Court concluded its consideration of clarification motions and specified a 60-day period for implementing structural duties of care.¹⁵³ The revised framework permits liability following failures to respond appropriately to notices and for systemic failures concerning specified serious unlawful content, while preserving judicial-order protections in certain circumstances. It does not, however, establish a blanket strict liability for every third-party post.

Decree 12,975, signed on May 20, 2026 and effective July 20, 2026, amends the Marco Civil's implementing regulation.¹⁵⁴ It establishes notice-and-action procedures, reasoned moderation decisions and appeals, systemic-risk duties, local establishment and legal representation, transparency requirements, and referrals to public authorities. It also requires retention of advertising records for one year after dissemination ends and retention of logical source-port information where necessary for identification of advertisers. For unlawful content distributed through paid advertising, boosting, or artificial distribution networks, it establishes a rebuttable presumption of responsibility that providers may contest by demonstrating diligent action.

¹⁵⁰ CCIA. (2025). *Brazil's VOD Bill Poses Key Trade Barrier*.

<https://ccianet.org/library/brazils-vod-bill-poses-key-trade-barriers-for-u-s-streaming-services/>.

¹⁵¹ Ministério da Justiça e Segurança Pública. (n.d.). *Classificação Indicativa*.

<https://www.gov.br/mj/pt-br/assuntos/seus-direitos/classificacao-1>.

¹⁵² Supremo Tribunal Federal. (2025, June 26). *STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros*.

<https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-d-e-terceiros/>

¹⁵³ Supremo Tribunal Federal. (n.d.). *Ajustes na tese de repercussão geral sobre a responsabilidade de plataformas digitais por conteúdo de terceiros* [Informativo STF; RE 1.037.396 ED/SP and related clarification motions, judgment concluded June 17, 2026]. <https://stf.jus.br/arquivo/informativo/documento/informativo.htm>

¹⁵⁴ Presidência da República. (2026, May 20). *Decreto nº 12.975, de 20 de maio de 2026*, Articles 1–2.

https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12975.htm

These obligations create substantial technical, operational, and legal burdens for U.S. suppliers serving Brazil. Uncertainty over systemic failures, AI-enabled distribution networks, adequate diligence, and future response deadlines may encourage excessive removal of lawful expression and commercial content. Additional retention obligations can also increase security risks and complicate compliance with data-minimization principles. Although the decree includes safeguards concerning contextual assessment and individual moderation decisions, their effectiveness will depend on implementation.

ANPD's implementation work continued through a consultation on the Marco Civil framework that closed on August 17, 2026.¹⁵⁵ In September, the agency opened a separate consultation on revisions to its inspection and administrative enforcement procedures. CCIA urges USTR to seek clearly bounded obligations, protection for lawful speech, proportionate retention requirements, meaningful judicial review, and adequate transition periods for subsequent rules.¹⁵⁶ Brazil should also avoid duplicative obligations under the Marco Civil, the Digital ECA, and the related framework on protecting women online.

Decree 12,976/2026, effective July 20, 2026, establishes additional obligations addressing violence against women online.¹⁵⁷ It requires removal of unauthorized intimate content within two hours after a qualifying notification. Pending further regulation, other covered notices require removal or a reasoned explanation for retaining content within six hours for manifestly unlawful content and 24 hours in other cases. The decree also provides for automatic blocking of reuploads of intimate content, subject to implementing rules; proactive measures against coordinated attacks; and phased, risk-proportionate safeguards against prohibited AI-generated intimate content. ANPD oversees implementation. CCIA urges technically workable deadlines, clear notice requirements, protection for lawful expression, and coordination with overlapping Marco Civil and Digital ECA obligations.

ANATEL Resolution 780/2025 expanded the conformity-assessment framework to impose responsibilities on online platforms involved in commercializing telecommunications products, including obligations concerning homologation information and irregular listings.¹⁵⁸ These requirements expose U.S. marketplaces to regulatory risk arising from third-party sellers' products and create substantial verification burdens at scale. CCIA urges ANATEL to distinguish manufacturers, importers, sellers, and intermediaries according to their actual functions and

¹⁵⁵ Agência Nacional de Proteção de Dados (ANPD). (n.d.). *Marco Civil da Internet*, "Participação Social." <https://www.gov.br/anpd/pt-br/assuntos/marco-civil-da-internet>

¹⁵⁶ Computer & Communications Industry Association (CCIA). (2026, June 24). *CCIA Concerns with Brazil's Amendments to the Marco Civil da Internet Implementing Regulation*. <https://ccianet.org/library/ccia-concerns-with-brazils-amendments-to-the-marco-civil-da-internet-implementing-regulation/>

¹⁵⁷ Presidência da República. (2026, May 20). *Decreto n° 12.976, de 20 de maio de 2026*, Articles 1, 4–10, and 15. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12976.htm

¹⁵⁸ Agência Nacional de Telecomunicações (ANATEL). (2025, August 1). *Resolução Anatel n° 780, de 1° de agosto de 2025*, Articles 2–3. <https://informacoes.anatel.gov.br/legislacao/resolucoes/2025/2054-resolucao-780>

ability to control compliance, and to provide workable notice-and-remediation procedures. The separate suspension of Article 6 concerning data centers does not itself suspend these marketplace provisions.

Brazil's Digital Child and Adolescent Statute, Law 15,211/2025, entered into force on March 17, 2026.¹⁵⁹ Decree 12,880 of March 18, 2026 further regulates the framework.¹⁶⁰ Covered services face obligations concerning age assurance, parental supervision, privacy and safety by design, advertising, and protection against harmful content. Social media accounts of users under 16 must be linked to a parent or legal guardian's account. Implementation remains a significant concern for U.S. platforms, app stores, and operating-system suppliers. ANPD has pursued guidance and staged monitoring, initially focusing on app stores and operating systems. CCIA urges clear allocation of responsibilities across the ecosystem, privacy-preserving and technically feasible age-assurance requirements, consistent treatment of comparable services, and adequate adaptation periods when additional requirements are specified.

Implementation has now progressed beyond initial monitoring of app stores and operating systems. On August 21, 2026, ANPD initiated broader monitoring of major platforms' compliance with the Digital ECA and Decrees 12,975 and 12,976.¹⁶¹ Separately, its August 12 preventive order required Discord to suspend Go Live and functionally equivalent video features for users located throughout Brazil, with reactivation subject to demonstrated safeguards and ANPD's express authorization.¹⁶² In related civil litigation, a federal court on September 2 allowed Discord ten working days to submit a proposal addressing specified safety, reporting, data-preservation, and representation requirements.¹⁶³ CCIA urges proportionate, evidence-based measures, clear conditions for restoring affected services, and effective review.

Pending also are 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.

¹⁵⁹ Presidência da República. (2025, September 17). *Lei nº 15.211, de 17 de setembro de 2025* (as amended), Article 41-A. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/115211.htm

¹⁶⁰ Presidência da República. (2026, March 18). *Decreto nº 12.880, de 18 de março de 2026*, Article 1. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm

¹⁶¹ Agência Nacional de Proteção de Dados (ANPD). (2026, August 21). *ANPD avalia como plataformas digitais atuam para prevenir conteúdos criminosos e proteger crianças e mulheres na internet*. <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-avalia-como-plataformas-digitais-atuam-para-prevenir-conteu-dos-criminosos-e-protoger-criancas-e-mulheres-na-internet>

¹⁶² Agência Nacional de Proteção de Dados (ANPD). (2026, August 12). *Em medida preventiva, ANPD determina que Discord suspenda transmissões ao vivo no Brasil*. <https://www.gov.br/anpd/pt-br/assuntos/noticias/em-medida-preventiva-anpd-determina-que-discord-suspenda-trans-missoes-ao-vivo-no-brasil>

¹⁶³ Lopes, R. (2026, September 2). *Justiça dá prazo de 10 dias para Discord apresentar nova proposta e tentar acordo com governo*. Folha de S.Paulo. <https://www1.folha.uol.com.br/cotidiano/2026/09/justica-da-prazo-de-10-dias-para-discord-apresentar-nova-propost-a-e-tentar-acordo-com-governo.shtml>

The first, Bill 4968/24, introduced in the Senate in December 2024¹⁶⁴ and currently before the Senate's Constitution and Justice Committee, seeks to establish a new right to remuneration for copyright and related rights holders for content used by online platforms. The bill would establish non-waivable remuneration rights for specified digital uses, including uses of works previously licensed or assigned, and would address certain communications initiated by third parties. CCIA remains concerned about additional remuneration obligations and interference with existing licensing arrangements, whose effects would depend on the applicable rights, contracts, and statutory offsets. Similarly, Bill 2370/19,¹⁶⁵ pending before the Chamber's Communication Committee, mirrors many of the Senate bill's core provisions. CCIA remains concerned that remuneration and liability provisions under discussion could require additional payments despite existing licenses, expose intermediaries to liability for unauthorized user uploads, or constrain their ability to manage content. Any such obligations should be assessed against the specific legislative text under consideration and should preserve contractual freedom and proportionate intermediary protections. 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 continues to explore bringing internet applications and value-added services within its regulatory framework governing telecommunications. Following earlier consultations in 2023 and 2024, its 2026 evidence-gathering proceeding on users' duties again addresses relationships between telecommunications operators and providers of content and applications. These proceedings risk supporting an unjustified shift in network economics, putting additional burdens on online service suppliers to contribute to network costs.

Separately, Bill 2,804/2024, introduced on July 9, 2024, remains pending in the Senate.¹⁶⁶ It would expand ANATEL's authority over internet services and require covered suppliers to contribute 5% of Brazilian gross operating revenue to the universal service fund for telecommunications, FUST.

Mandatory contributions imposed on large application and content providers would disproportionately burden U.S. suppliers and undermine commercially negotiated relationships between networks and online services. Such proposals overlook these suppliers' investments in data centers, caching, subsea cables, and other infrastructure that supports connectivity. CCIA

¹⁶⁴ Senado Federal. (2024). *Projeto de Lei nº 4.968/2024*. <https://legis.senado.leg.br/sdleg-getter/documento?dm=9879382>

¹⁶⁵ Câmara dos Deputados. (2019). *Projeto de Lei nº 2.370/2019*. https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1734276

¹⁶⁶ Senado Federal. (n.d.). *Projeto de Lei nº 2.804, de 2024* [Legislative record]. <https://www25.senado.leg.br/web/atividade/materias/-/materia/164634>; Coronel, A. (2024, July 9). *Projeto de Lei nº 2.804/2024*, Articles 2 and 6–8. Senado Federal. <https://legis.senado.leg.br/sdleg-getter/documento?dm=9697350>

urges USTR to oppose mandatory network payments and discriminatory funding obligations, preserve the distinction between telecommunications and value-added services, and seek transparent, competitively neutral universal-service arrangements.

ANATEL Resolution 780/2025 introduced a conformity-assessment and homologation requirement for data centers used by telecommunications providers.¹⁶⁷ The measure seeks to apply telecommunications-specific conformity assessment procedures to equipment used in data centers, despite no demonstrated need. However, Acórdão 58 of March 3, 2026 suspended the enforceability of Article 6 of this measure pending further consideration by the Board. The measure therefore remains an unresolved regulatory risk rather than a presently enforceable certification obligation.

Public Consultation 48/2025 subsequently developed proposed technical requirements and conformity-assessment procedures for telecommunications data centers.¹⁶⁸ CCIA's March 2026 submission¹⁶⁹ identified concerns that the proposed functional definitions could reach third-party cloud and colocation providers, including providers unable to determine whether a customer's workloads support critical telecommunications functions. Requirements concerning certification, audits, operational resilience, and disclosure of infrastructure information could duplicate existing international standards and create significant costs, delays, and security risks.

CCIA urges Brazil to limit obligations to clearly defined telecommunications functions and assign responsibility to entities that control the relevant networks and workloads. Any final framework should recognize appropriate international certifications, protect sensitive facility and network information, avoid unnecessary local testing and duplicate audits, and provide a transition period beginning only after final requirements are sufficiently specified. USTR should seek assurance that ANATEL will not use telecommunications certification to regulate general-purpose cloud and data-center services indiscriminately.

Brazil's broader national data-center policy also warrants scrutiny for its treatment of foreign infrastructure and cloud suppliers.¹⁷⁰ CCIA supports measures that reduce investment barriers, improve access to reliable energy, and encourage sustainable infrastructure. Such policies should remain open to suppliers regardless of ownership and should not condition market access on unnecessary data localization, technology transfer, or preference for domestic cloud services.

¹⁶⁷ Agência Nacional de Telecomunicações (ANATEL). (2025, August 1). *Resolução Anatel n° 780, de 1° de agosto de 2025*, Article 6. <https://informacoes.anatel.gov.br/legislacao/resolucoes/2025/2054-resolucao-780>

¹⁶⁸ Agência Nacional de Telecomunicações (ANATEL). (2025). *Consulta Pública n° 48/2025: Requisitos Técnicos e Procedimento Operacional para a Avaliação da Conformidade de Data Centers que Integram as Redes de Telecomunicações*. <https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?ConsultaId=20370>

¹⁶⁹ Computer & Communications Industry Association (CCIA). (2026, March 3). *CCIA Comments on ANATEL's Public Consultation No. 48*.

<https://ccianet.org/wp-content/uploads/2026/03/CCIA-Comments-on-ANATELs-Public-Consultation-No.-48.pdf>

¹⁷⁰ Computer & Communications Industry Association (CCIA). (2025). *CCIA Comments on Brazil National Data Center Policy "Connectivity and Infrastructure Axis"*.

<https://ccianet.org/wp-content/uploads/2025/09/CCIA-Comments-on-Brazil-National-Data-Center-Policy.pdf>

ReData was enacted as Law 15,504 of September 15, 2026.¹⁷¹ It provides conditional federal tax relief for qualifying data-center equipment, subject to qualification procedures and implementing acts. Conditions include sustainability and domestic R&D commitments and, as a baseline, reservation of at least 10% of supported service supply for the domestic market or R&D investment equal to 10% of the value of equipment acquired with ReData benefits. Import-duty relief is limited to listed products without equivalent national production, while specified products manufactured in the Manaus Free Trade Zone are excluded from IPI relief. Although the regime provides a five-year benefits period, its PIS/Cofins and IPI benefits produce effects only through December 31, 2026, under the tax-reform transition.

CCIA welcomes the prospect of investment incentives but urges Brazil to ensure that eligibility conditions do not undermine those benefits. Domestic-equivalence tests should reflect actual technical substitutability, and service-allocation and investment conditions should not unnecessarily restrict how U.S. suppliers organize their operations.

Challenges to the Development of AI

Bill 2,338/2023, approved by the Senate in December 2024, remains under consideration by a special committee in the Chamber of Deputies.¹⁷² This proposed AI framework fails to distinguish between high and low-risk applications and lacks a clear differentiation between AI developers and deployers, creating operational uncertainty up and down the AI value chain. CCIA is also concerned that expansive remuneration requirements for training uses, overlapping sectoral oversight, and disproportionate compliance obligations could restrict access to training materials and discourage the development and deployment of AI services in Brazil. Any final legislation should clearly allocate responsibilities across the AI value chain, reflect each actor's ability to control risks, preserve appropriate copyright limitations and exceptions (such as a text-and-data mining exception), and avoid duplicative regulation.

Restrictions on Cross-Border Data Flows

Brazil's General Data Protection Law, the LGPD, came fully into effect in August 2021.¹⁷³ Its international-transfer requirements continue to create compliance costs for U.S. suppliers, although Brazil has established mechanisms enabling lawful transfers and adopted differentiated rules for certain small processing agents.

¹⁷¹ Presidência da República. (2026, September 15). *Lei nº 15.504, de 15 de setembro de 2026*, Articles 1–2. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15504.htm

¹⁷² Câmara dos Deputados. (n.d.). *PL 2338/2023: Tramitação*. Retrieved September 18, 2026, from <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262>

¹⁷³ Agência Nacional de Proteção de Dados (ANPD). (2026, September 9). *Perguntas Frequentes*, section 1.3, “Quando a LGPD entrou em vigor?” <https://www.gov.br/anpd/pt-br/aceso-a-informacao/perguntas-frequentes>

ANPD Resolution 19/2024 established Brazilian standard contractual clauses and procedures for adequacy decisions and other transfer mechanisms.¹⁷⁴ Brazilian standard contractual clauses can be used without individual prior approval, while bespoke clauses and binding corporate rules require approval. In 2026, ANPD recognized the European Union as adequate under Resolution 32/2026.¹⁷⁵ Its published repository does not identify a corresponding U.S. adequacy decision or approvals of equivalent foreign standard clauses, bespoke clauses, or binding corporate rules. U.S. suppliers therefore continue to face additional contracting and compliance requirements where an alternative transfer mechanism is necessary. CCIA urges broader interoperability, timely decisions, and formal recognition of qualifying U.S. protections.

Government-cloud requirements create separate restrictions on cross-border supply. GSI Normative Instruction 8 of October 6, 2025 permits federal information classified as restricted or secret to be processed in qualifying private or community clouds, but requires providers to be established in Brazil and the relevant infrastructure to be located domestically.¹⁷⁶ Subject to narrow authorized exceptions, the information cannot be replicated, transferred, or processed abroad. Public and hybrid clouds (the typical U.S. suppliers' model) remain excluded for this category of classified information, limiting available delivery models for U.S. suppliers. CCIA urges security requirements proportionate to the sensitivity of the information and recognition of equivalent safeguards.

The government's Nuvem Brasileira initiative raises additional procurement concerns. Its August 2026 market-consultation materials¹⁷⁷ contemplate a nationally developed cloud platform operated through public enterprises, domestic technical capacity, shared ownership of intellectual property generated through the partnership, and government access to source code to preserve operational continuity. These remain proposed partnership conditions rather than a general prohibition on foreign cloud services. CCIA urges Brazil to preserve opportunities for U.S. suppliers and avoid unnecessary nationality-based restrictions or compulsory technology-sharing conditions in subsequent procurement.

Brazil continues developing a National Data Economy Policy, including work with the Brazilian Agency for Industrial Development to gather evidence on data use and sharing.¹⁷⁸ This initiative warrants monitoring, but falls short of an obligation to share non-personal data. CCIA urges

¹⁷⁴ Autoridade Nacional de Proteção de Dados (ANPD). (2024, August 23). *Resolução CD/ANPD nº 19, de 23 de agosto de 2024*. <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396>

¹⁷⁵ Agência Nacional de Proteção de Dados (ANPD). (2026, January 26). *Resolução nº 32, de 26 de janeiro de 2026*. <https://www.in.gov.br/web/dou/-/resolucao-n-32-de-26-de-janeiro-de-2026-683334547>

¹⁷⁶ Gabinete de Segurança Institucional da Presidência da República (GSI). (2025, October 6). *Instrução Normativa GSI/PR nº 8, de 6 de outubro de 2025*. <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-8-de-6-de-outubro-de-2025-660716869>

¹⁷⁷ MGI, SERPRO, ABDI, & BNDES. (2026, August). *Caderno de apoio da escuta de mercado sobre solução de Nuvem Brasileira*, sections 2, 4–5.

https://www.abdi.com.br/wp-content/uploads/2026/08/Caderno_nuvembrasileira.pdf

¹⁷⁸ Agência Brasileira de Desenvolvimento Industrial (ABDI). *Pesquisa Dados*. <https://www.abdi.com.br/pesquisadados/>

Brazil to protect confidential business information and trade secrets, preserve voluntary commercial arrangements, and avoid discriminatory access requirements or restrictions on cross-border data flows. Any mandatory sharing proposal should identify a specific public-interest justification and include proportionate safeguards.

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

The Department of Innovation of the Ministry of Development, Industry, and Trade (MDIC) is considering policies and legislative proposals related to the "data economy" modeled after the European Union's Data Act, focusing on the treatment of non-personal information.¹⁷⁹ Although concrete proposals have yet to emerge, the issue warrants careful monitoring, given the discriminatory aspects of what the EU has already implemented.

Taxation of Digital Products and Services

Brazil's IOF foreign-exchange tax increases the cost of certain cross-border payments for digital services. Decree 12,499 of June 11, 2025 replaced the May 2025 decrees and established a 3.5% rate for specified transactions, including covered cross-border payment arrangements and residual outward remittances not subject to another rate or exemption.¹⁸⁰ Other transactions receive different treatment, including a 1.1% rate for specified outward investment transfers. While onerous and arguably discriminatory, it applies only to a limited category of transactions.

For affected transactions, IOF adds to the price Brazilian customers pay for services supplied from abroad and may disadvantage cross-border suppliers relative to providers receiving domestic payments. Frequent changes also complicate pricing and compliance. CCIA urges USTR to seek predictable, non-discriminatory treatment of cross-border payments and reductions in transaction taxes that impede digital trade.

Brazil's CIDE contribution on financial remittances imposes a 10% charge on covered payments to non-residents, including specified royalties and technical or administrative services.¹⁸¹ In August 2025, the Federal Supreme Court upheld the expanded contribution, including its

¹⁷⁹ Germany Federal Ministry of Digital Transformation. (2025). *Deep Dive into Brazil's Data Economy*. https://digital-dialogues.net/en/news-details/A_deep_dive_into_Brazils_data_economy_Study_on_challenges_and_opportunities

¹⁸⁰ Presidência da República. (2025, June 11). *Decreto nº 12.499, de 11 de junho de 2025*, Articles 1–2. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12499.htm

¹⁸¹ Presidência da República. (2000, December 29). *Lei nº 10.168, de 29 de dezembro de 2000*, Article 2, §§ 2–4, as amended. https://www.planalto.gov.br/ccivil_03/leis/110168.htm

application beyond transactions involving technology transfer.¹⁸² This increases the importance of addressing the measure as an ongoing cost to cross-border supply. Its scope nevertheless requires qualification: the statute excludes remuneration for software-use licenses and commercialization or distribution rights unless the corresponding technology is transferred.

Where applicable, CIDE can combine with other taxes and withholding obligations to increase the cost of purchasing U.S. technology and services. CCIA urges Brazil to narrow the scope of burdensome remittance taxation, clarify its application to digital business models, and avoid overlapping charges that distort sourcing decisions.

In a helpful step facilitating e-commerce, Brazil removed the 20% federal import duty on qualifying purchases of up to US\$50 through the Remessa Conforme program in 2026.¹⁸³ Receita Federal's current guidance provides a zero rate for qualifying purchases up to that threshold and a US\$30 deduction from the import duty on qualifying purchases above US\$50 and up to US\$3,000.¹⁸⁴ This reduces a barrier identified in CCIA's 2025 submission. Significant duties on higher-value purchases, program compliance requirements, and applicable state taxation nevertheless continue to affect cross-border e-commerce. CCIA urges further simplification and predictable treatment of international online purchases.

Other Barriers to Digital Trade

Brazil's recent intervention in the payments market in support of a government-sponsored service raises concerns about competitive neutrality. The Central Bank of Brazil both regulates payment services and operates a competing service, Pix.¹⁸⁵ CCIA recognizes the benefits of efficient instant payments and the beneficial expansion of access to digital technologies but questions whether governance arrangements, participation requirements, and regulatory treatment provide equal opportunities for private and foreign suppliers. In June 2026, USTR's Section 301 determination identified Brazilian practices relating to digital trade and electronic payment services as unreasonable and burdensome to U.S. commerce.¹⁸⁶ On July 15, 2026,

¹⁸² Supremo Tribunal Federal. (2025, August 13). *STF valida alterações que ampliaram cobrança da Cide-Tecnologia*.

<https://noticias.stf.jus.br/postsnoticias/stf-valida-alteracoes-que-ampliaram-cobranca-da-cide-tecnologia/>

¹⁸³ Receita Federal do Brasil. *Novas Regras*.

<https://www.gov.br/receitafederal/pt-br/assuntos/aduana-e-comercio-exterior/manuais/remessas-postal-e-expressa/regras-futuras>

¹⁸⁴ Receita Federal do Brasil. *Novas Regras*, section 1, "Compras no Programa Remessa Conforme."

<https://www.gov.br/receitafederal/pt-br/assuntos/aduana-e-comercio-exterior/manuais/remessas-postal-e-expressa/regras-futuras>

¹⁸⁵ Duarte, A., Frost, J., Gambacorta, L., Koo Wilkens, P., & Shin, H. S. (2022, March 23). *Central banks, the monetary system and public payment infrastructures: Lessons from Brazil's Pix*. BIS Bulletin No. 52.

<https://www.bis.org/publ/bisbull52.htm>

¹⁸⁶ Office of the United States Trade Representative. (2026, June 1). *USTR Section 301 Determination on Brazil's Unreasonable Acts, Policies, and Practices*.

<https://ustr.gov/about/policy-offices/press-office/press-releases/2026/june/ustr-section-301-determination-brazils-unreasonable-acts-policies-and-practices>

USTR announced final Section 301 action imposing a 25% tariff on certain Brazilian goods following the broader investigation, which covered digital trade and electronic payments alongside other practices.¹⁸⁷ CCIA urges USTR to seek transparent, non-discriminatory rules, equivalent treatment of comparable risks, and effective safeguards separating regulatory decision-making from the operation of a competing payment system.

Separately, Bill 2141/2025, introduced on May 6, 2025, would mandate access to near-field communication (NFC) technology (e.g., integrated in mobile phones) for payment services.¹⁸⁸ The Science, Technology and Innovation Committee approved a substitute on May 20, 2026; the bill remains pending before the Consumer Protection Committee.¹⁸⁹ The substitute would require device manufacturers and mobile operating-system providers to grant payment-service providers free access to covered technologies, prohibit technical, commercial, or contractual restrictions on that access, and protect consumers' ability to choose alternative payment applications, including but not limited to Pix. Proposed sanctions include fines of up to 5% of annual gross revenue in Brazil, suspension of device sales, and temporary unavailability of systems or applications. These provisions raise serious concerns about suppliers' ability to protect proprietary technologies and could constrain commercial licensing arrangements. They would also impose substantial implementation and security burdens on U.S. technology suppliers. CCIA urges USTR to seek proportionate interoperability requirements that preserve objective security safeguards, reasonable remuneration for proprietary technology, and non-discriminatory treatment of competing payment services.

Brazil's Congress has been considering a right-to-repair law since 2024. PL 805/24 was approved by the Senate in May 2026 and awaits action in the lower house. It imposes prescriptive product design requirements, including restrictions on parts pairing, mandatory access to tools, spare parts, and repair information, user-removable and replaceable battery requirements, extended spare-parts availability periods, and repairability indices, that diverge from internationally standardized product architectures and global manufacturing practices.¹⁹⁰ Such requirements may compel manufacturers to undertake costly product redesign, while mandatory disclosure of embedded software and component information raises serious cybersecurity, product safety, and IP risks, particularly for sophisticated ICT products where unauthorized access to central processors and digital rights management protections can expose proprietary systems to exploitation and replication.

¹⁸⁷ Office of the United States Trade Representative. (2026, July 15). *USTR Section 301 Action on Brazil's Unreasonable Acts, Policies, and Practices*. <https://ustr.gov/about/policy-offices/press-office/press-releases/2026/july/ustr-section-301-action-brazils-unreasonable-acts-policies-and-practices>

¹⁸⁸ Câmara dos Deputados. (2025, May 6). *Projeto de Lei nº 2.141/2025*. https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2899430

¹⁸⁹ Câmara dos Deputados. (n.d.). *PL 2141/2025: Tramitação*. Retrieved September 18, 2026, from <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2504778>

¹⁹⁰ <https://www25.senado.leg.br/web/atividade/materias/-/materia/162652>

Cambodia

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Cambodia's Digital Government Policy 2022–2035 directs ministries and institutions without existing data centers to use national data centers, while those with existing facilities must connect to national infrastructure for backup.¹⁹¹ These requirements could constrain opportunities for U.S. cloud suppliers. MPTC held a consultation on a separate draft Cloud First Policy on October 2, 2025.¹⁹² CCIA encourages Cambodia to adopt technology-neutral procurement and security requirements that permit participation by qualified foreign cloud providers and avoid unnecessary localization restrictions.

Government-Imposed Content Restrictions and Related Access Barriers

Reports of censorship and mandated internet filtering and blocking continue to persist in Cambodia.¹⁹³ 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.

Cambodia's February 2021 National Internet Gateway sub-decree provides for centralized control over internet traffic.¹⁹⁴ Reporting published in October 2025 identified renewed implementation plans assigning responsibilities to MPTC and state-owned Telecom Cambodia.¹⁹⁵ Such infrastructure could facilitate blocking and surveillance, creating access risks for foreign digital services.

¹⁹¹ Royal Government of Cambodia. (2022, January 28). *Cambodia Digital Government Policy 2022–2035*, p. 29. https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf

¹⁹² Ministry of Post and Telecommunications. (2025, October 2). *Minister Chea Vandeth Presided Over the Opening Ceremony of the “Consultative Workshop on the Cambodia Cloud First Policy Draft”*. <https://mptc.gov.kh/en/2025/10/minister-chea-vandeth-presided-over-the-opening-ceremony-of-the-consultative-workshop-on-the-cambodia-cloud-first-policy-draft/>

¹⁹³ Freedom House. (2024). *Freedom on the Net 2024: Cambodia*. <https://freedomhouse.org/country/cambodia/freedom-net/2024>

¹⁹⁴ Royal Government of Cambodia. (2021, February 16). *Sub-decree No. 23 on the Establishment of National Internet Gateway (NIG)*. https://data.opendevlopmentcambodia.net/laws_record/sub-decree-no-23-on-the-establishment-of-national-internet-gateway-nig

¹⁹⁵ Freedom House. (2025). *Freedom on the Net 2025: Cambodia*. <https://freedomhouse.org/country/cambodia/freedom-net/2025>

MPTC and the Ministry of Justice continued reviewing the draft Cybersecurity Law in July 2026.¹⁹⁶ An earlier public version¹⁹⁷ would permit extensive government access to private computer systems during cybersecurity incidents and impose broad compliance obligations on entities designated as critical information infrastructure, including digital and media services. CCIA urges Cambodia to narrow these powers, provide independent oversight, and ensure proportionate obligations for service providers.

Restrictions on Cross Border Data Flows

Cambodia released a draft Law on Personal Data Protection (LPDP) on July 23, 2025,¹⁹⁸ modeled in part on the EU's GDPR. MPTC held a validation workshop on August 5, 2026, confirming that the legislation remained a draft undergoing consultation before the formal legislative process.¹⁹⁹ 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 domestic entities and foreign entities offering goods or services to, or monitoring, individuals residing in Cambodia, with implementation proposed two years after entry into force.

The revised draft dated July 31, 2026 raises compliance concerns for U.S. suppliers.²⁰⁰ Article 31 requires overseas recipients to provide equivalent or higher protection, maintains the transferring controller's accountability, and permits MPTC to suspend or prohibit transfers presenting serious risks or violating the law. Detailed transfer conditions remain subject to subsequent guidelines. Article 45 leaves administrative offenses and enforcement procedures to ministerial regulation. Articles 51 and 53 provide criminal penalties for violations of high-risk breach-notification obligations, including corporate fines of KHR 200 million–1 billion. Article 28 requires notification of potentially harmful breaches within 72 hours of awareness, while permitting valid reasons for delay. Implementation should provide clear transfer mechanisms, workable timelines, and proportionate enforcement.

¹⁹⁶ Ministry of Post and Telecommunications. (2026, July 10). *Secretary of State Kong Phallack Led MPTC Delegation to Attend a Technical Meeting on the Draft Cybersecurity Law*. <https://mptc.gov.kh/en/2026/07/secretary-of-state-kong-phallack-led-mptc-delegation-to-attend-a-technical-meeting-on-the-draft-cybersecurity-law/>

¹⁹⁷ Access Now & International Commission of Jurists. (2023, October 2). *Legal Analysis: Cambodia Draft Law on Cybersecurity*. <https://www.icj.org/wp-content/uploads/2023/10/Legal-Analysis-Cambodia-Cybersecurity-Draft-Law-.pdf>

¹⁹⁸ Ministry of Post and Telecommunications. (2025). *Draft Law on Personal Data Protection*. https://data.opendevelopmentcambodia.net/laws_record/draft-law-on-personal-data-protection

¹⁹⁹ Ministry of Post and Telecommunications. (2026, August 5). *Ministry of Post and Telecommunications Holds Validation Workshop on the Draft Law on Personal Data Protection*. <https://mptc.gov.kh/en/2026/08/ministry-of-post-and-telecommunications-holds-validation-workshop-on-the-draft-law-on-personal-data-protection/>

²⁰⁰ Ministry of Post and Telecommunications. (2026, July 31). *Draft Law on Personal Data Protection*. https://data.opendevelopmentcambodia.net/en/laws_record/draft-personal-data-protection-law

Cameroon

Taxation of Digital Products and Services

Cameroon's 2026 Finance Law enacted a Significant Economic Presence (SEP) tax regime targeting non-resident digital platforms. Taxpayers will be considered as having a SEP in Cameroon if either (1) their gross receipts from digital services to customers or users located in Cameroon exceed FCFA 50 million (approx. US\$89,000) in a tax year; or (2) they have more than 1,000 users, customers, or account holders located in Cameroon in a tax year. For nonresident companies with SEP, Cameroon deems a taxable profit for the relevant digital income at 10% of gross income earned in Cameroon and then applies a 3% tax to gross income from Cameroon-sourced digital activities. This unilateral revenue tax explicitly targets foreign digital service exporters and creates severe double-taxation risks, particularly for U.S. suppliers given the absence of a tax treaty with Cameroon. CCIA urges USTR to request that Cameroon withdraw its unilateral SEP tax in favor of multilateral solutions to international taxation.

Canada

Asymmetric Platform Regulation

On November 17, 2022, the Canadian Government opened a consultation seeking feedback on its initiative to update the Canadian Competition Act.²⁰¹ The consultation specifically sought public comment on data and digital markets, asking whether “sector-specific mechanisms” should be adopted and for suggested approaches for intersecting with privacy and data protection. The accompanying consultation paper, “The Future of Competition Policy in Canada,”²⁰² explored possible reforms addressing unilateral anti-competitive conduct, including abuse of dominance by large online platforms, and the implications of new technology and business practices for deceptive marketing rules. The federal government released its official summary report in September 2023. While the Competition Act has undergone several amendments recently, asymmetric regulation targeting digital service suppliers has not yet been proposed.

Customs-Related Restrictions and Import Barriers for Goods

²⁰¹ 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>; Department of Justice Canada. (n.d.). *Competition Act, R.S.C., 1985, c. C-34*. <https://laws-lois.justice.gc.ca/eng/acts/c-34/>.

²⁰² 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

Effective September 8, 2026, Canada imposed additional tariffs on specified technology products originating from the United States, including 50% tariffs on smartphones, certain networking and routing equipment, and certain monitors, and a 25% tariff on specified printed circuit assemblies.²⁰³ These measures directly increase the cost of covered U.S. technology exports and disrupt integrated North American supply chains. Their application turns on the products' U.S. origin, rather than the nationality of the brand owner. CCIA urges USTR to work with Canada to remove these retaliatory barriers and restore predictable, tariff-free trade in technology products.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

On August 13, 2025, Shared Services Canada (SSC) issued a request for information concerning sovereign public cloud capabilities.²⁰⁴ An updated procurement notice published on March 3, 2026 describes a sovereign cloud procurement stream supplementing existing federal cloud procurement arrangements.²⁰⁵ The proposed requirements include keeping covered data in Canada and insulating providers and their ultimate parent companies from foreign legal compulsion that could require access, disclosure, or service interruption without Canadian authorization. The notice limits eligibility for the upcoming open competitive process to small and medium-sized businesses and also contemplates targeted procurement processes involving Canadian firms. SSC has invoked the National Security Exception for all phases of the procurement. 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.²⁰⁶ 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.

Canada's Policy on Prioritizing Canadian Suppliers and Canadian Content in Strategic Federal Procurements took effect on December 16, 2025.²⁰⁷ Covered sectors expressly include cloud services, data centres, software, hardware, and telecommunications. The policy grants qualifying Canadian suppliers a 10% reduction in evaluated price and generally allocates 25% of evaluation

²⁰³ Department of Finance Canada. (2026, August 26). *List of products from the United States subject to counter-tariffs effective September 8, 2026*. <https://www.canada.ca/en/departement-finance/news/2026/08/list-of-products-from-the-united-states-subject-to-counter-tariffs-effective-september-8-2026.html>

²⁰⁴ 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>

²⁰⁵ Shared Services Canada. (2026, March 3). *Request for Information – Sovereign Public Cloud Capability – Upcoming Competitive Processes*. <https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/cb-416-17296820>

²⁰⁶ CCIA. (2025, September 29). *Canada's Sovereign Cloud Initiative*. <https://ccianet.org/library/canadas-sovereign-cloud-initiative/>

²⁰⁷ Public Services and Procurement Canada. (2026, February 20). *Policy on Prioritizing Canadian Suppliers and Canadian Content in Strategic Federal Procurements*. <https://canadabuys.canada.ca/en/buy-canadian-policy/policy-prioritizing-canadian-suppliers-and-canadian-content-strategic-federal-procurements>

scoring to Canadian value-added, or applies a corresponding price-based methodology. Suppliers from applicable trading partners remain eligible where a relevant procurement agreement applies, and qualifying Canadian operations of foreign-owned firms may meet the Canadian-supplier definition. Nevertheless, the preferences can disadvantage U.S. suppliers and services delivered from outside Canada.²⁰⁸ The Administration has responded in kind²⁰⁹ and CCIA urges both sides to negotiate to restore the status quo ante.

Ontario's updated Procurement Restriction Policy, effective April 13, 2026, generally excludes defined U.S. businesses from new goods and services procurements by provincial government and designated broader-public-sector entities, regardless of procurement value, subject to exceptions.²¹⁰ The definition covers suppliers headquartered in the United States, or controlled by a corporation headquartered there, that have fewer than 250 full-time employees in Canada. An exception permits participation in services procurements where at least 90% of the staff delivering the contracted services will be located in Canada. These restrictions create direct market-access barriers for affected U.S. technology suppliers and can condition access on local staffing. USTR should seek removal of discriminatory restrictions and preferences affecting U.S. suppliers, given commitments Ontario made to the United States under the WTO GPA.

Discriminatory Local Content Quotas and Audiovisual Mandates

The Online Streaming Act received Royal Assent and entered into law on April 27, 2023.²¹¹ Under the law, the CRTC is empowered to impose discoverability and contribution obligations on qualifying online broadcasting undertakings, including covered programming made available through social media services, requiring affected services to fund and give preferential treatment to Canadian content and creators. 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 June 2024 framework imposed a 5% base contribution on covered online audio and audiovisual undertakings unaffiliated with Canadian broadcasters, subject to a C\$25 million

²⁰⁸ Akin Gump. (2026). *President Trump Directs Removal of Canadian Products*. <https://www.akingump.com/en/insights/alerts/president-trump-directs-removal-of-canadian-products-from-federal-procurement>.

²⁰⁹ The White House. (2026). *Restoring Reciprocity in Government Procurement*. <https://www.whitehouse.gov/presidential-actions/2026/09/restoring-reciprocity-in-government-procurement/>.

²¹⁰ Ontario Ministry of Public and Business Service Delivery and Procurement. (2026, March 31). *Procurement Restriction Policy (U.S. Businesses): A Guide for Government & BPS Entities*. <https://www.supplyontario.ca/wp-content/uploads/US-Procurement-Restriction-Policy-Guide-March-31-2026-2.pdf>

²¹¹ Parliament of Canada. (2023, April 27). *Online Streaming Act, S.C. 2023, c. 8 (Bill C-11)*. <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-11/royal-assent>

annual Canadian contribution-revenue threshold assessed at the ownership-group level.²¹² The framework excludes revenues from certain online services, including those attributable to user-generated content, podcasts, audiobooks, and video games.

On May 21, 2026, the CRTC adopted a further audiovisual expenditure framework setting a 15% requirement for covered unaffiliated online broadcasting groups, inclusive of the existing 5% base contribution.²¹³ It established a 25% contribution requirement for traditional broadcasters (representing a reduction for their previous 30-45% requirement). For groups with at least C\$100 million in annual Canadian broadcasting revenues, at least 30% of required expenditures would be directed to “enhanced partnerships” in which Canadians hold majority copyright ownership. The decision contemplated implementation through subsequent proceedings establishing tailored conditions of service.

The government subsequently announced a reconsideration of this approach. On June 3, 2026, it announced new policy directions and a review of the CRTC’s recent decisions, alongside additional public funding for Canadian culture.²¹⁴ A July 17 Department of Justice court letter indicated that the government intended to eliminate the original 5% base contribution, but did not clarify steps with respect to other requirements (e.g., investment obligations).²¹⁵ Given the advanced state of the CRTC’s adopted framework, and the absence of any announced alternative, the CRTC’s current policy remains in limbo awaiting formal policy instructions from the government. Since the underlying law remains in effect and the CRTC retains broad discretion in implementing it, legal certainty with respect to the discriminatory effects of this law will not be achieved absent repeal. CCIA urges USTR to pursue this goal.

The impact of the Online Streaming Act will fall overwhelmingly on U.S. suppliers. In September 2025, CCIA estimated that the combined Canadian revenues of the U.S. online video and music companies included in its analysis of the contribution framework would reach nearly

²¹² Canadian Radio-television and Telecommunications Commission. (2024, June 4). *Broadcasting Regulatory Policy CRTC 2024-121: The Path Forward – Supporting Canadian and Indigenous content through base contributions*. <https://crtc.gc.ca/eng/archive/2024/2024-121.htm>

²¹³ Canadian Radio-television and Telecommunications Commission. (2026, May 21). *Broadcasting Regulatory Policy CRTC 2026-96: The Path Forward – Supporting the creation and distribution of Canadian programming in the audio-visual sector – Part 2 – A modernized framework for Canadian programming expenditures*. <https://crtc.gc.ca/eng/archive/2026/2026-96.htm>

²¹⁴ Canadian Heritage. (2026, June 3). *Government of Canada announces immediate support to strengthen Canadian culture and ensure Canadian content remains affordable*. <https://www.canada.ca/en/canadian-heritage/news/2026/06/government-of-canada-announces-immediate-support-to-strengthen-canadian-culture-and-ensure-canadian-content-remains-affordable.html>

²¹⁵ Geist, M. (2026, July 29). *Starting Over: Court Filing Confirms the CRTC’s Streamer Contribution Decisions Are Dead With a Full Online Streaming Act Reset to Come*. <https://www.michaelgeist.ca/2026/07/starting-over-court-filing-confirms-the-crtcs-streamer-contribution-decisions-a-re-dead-with-a-full-online-streaming-act-reset-to-come/>

USD \$7 billion by the end of 2025.²¹⁶ CCIA considers these obligations discriminatory and inconsistent with USMCA Articles 19.4, 15.3.1, and 14.10.1(b). Breaching these provisions would be subject to the cultural-industries exception in Article 32.6.²¹⁷ However, while that exception protects a measure that would otherwise be inconsistent with the Agreement, the subsequent Article 32.6.4 permits a response of equivalent commercial effect, exposing Canada to legal retaliation that could exceed \$1 billion per year.

On November 18, 2025, the CRTC adopted a revised framework for certifying Canadian audiovisual programming—rules that determine what content qualifies both for existing quotas (e.g., applicable to traditional broadcasters) and any further quotas the CRTC may apply to online suppliers.²¹⁸ The framework requires that qualifying content contain at least 20% Canadian copyright ownership, alongside applicable Canadian creative-participation requirements. Consequently, wholly U.S.-owned productions cannot qualify under this route even if produced in Canada. Productions with majority foreign ownership may still qualify if they satisfy the Canadian ownership minimum and other requirements. Conditioning eligibility on Canadian ownership continues to disadvantage wholly U.S.-owned content and can influence investment and licensing arrangements. The decision also provides for publication of specified Canadian revenue and expenditure information for broadcasting ownership groups meeting the C\$25 million threshold. The detailed data required raises serious concerns with respect to the disclosure of business-confidential information.

On May 21, 2026, the CRTC adopted an audiovisual discoverability framework addressing the promotion, visibility, and availability of Canadian and Indigenous programming, with service-specific obligations to be developed through subsequent proceedings.²¹⁹ Requirements governing presentation and promotion may constrain how affected services organize their offerings and respond to audience preferences. However, the Broadcasting Act expressly prohibits the CRTC from mandating specific computer algorithms or access to source code through discoverability orders.

²¹⁶Computer & Communications Industry Association. (2025, September). *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>

²¹⁷ Computer & Communications Industry Association. (2024, June). *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/>

²¹⁸ Canadian Radio-television and Telecommunications Commission. (2025, November 18). *Broadcasting Regulatory Policy CRTC 2025-299: The Path Forward – Defining “Canadian program” and supporting the creation and distribution of Canadian programming in the audio-visual sector – Part 1 – Certification framework for Canadian programs, artificial intelligence, data collection and publication, and reporting requirements*.

<https://crtc.gc.ca/eng/archive/2025/2025-299.htm>

²¹⁹ Canadian Radio-television and Telecommunications Commission. (2026, May 21). *Broadcasting Regulatory Policy CRTC 2026-95: The Path Forward – Working towards a sustainable Canadian broadcasting system – Part 1 – Discoverability of Canadian and Indigenous content and services, and support for services of exceptional importance*. <https://crtc.gc.ca/eng/archive/2026/2026-95.htm>

The treatment of social media services remains contentious. The CRTC declined to categorically exempt social media platforms from registration in 2023,²²⁰ and its declared status as a broadcasting service does result in certain regulatory fees. However, registration for these services does not implicate the contribution or discoverability regime. The government's binding policy instructs the CRTC to exclude programs created and uploaded by social media users, including podcasts. CCIA urges USTR to monitor implementation to ensure that these exclusions are respected and that discoverability requirements do not impose discriminatory restrictions on U.S. services.

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.²²¹ CCIA urges USTR to actively oppose implementation of these measures and consider a proportionate response if negotiations do not yield a satisfactory solution. The current pause in implementation is welcome, but ultimately rescission of the Online Streaming Act, is the only long-term means to prevent lasting harm to U.S. suppliers, Canadian consumers, and the broader digital economy.

Quebec has established a parallel provincial framework affecting online cultural-content services. Bill 109 passed on December 11, 2025 and received assent on December 12, 2025.²²² The legislation establishes powers to require covered digital platforms to register, make specified quantities or proportions of French-language cultural content available, and promote its discovery. It also provides for obligations affecting interfaces, intermediaries, and connected televisions or similar devices, including requirements concerning access to designated platforms. The legislation requires relevant interfaces to be easily configurable in French but falls short of a universal French-by-default setting. Detailed operational requirements will require implementing regulations which have yet to be issued so the practical effect of this measure remains

²²⁰ Canadian Radio-television and Telecommunications Commission. (2023, September 29). *Broadcasting Regulatory Policy CRTC 2023-329 and Broadcasting Order CRTC 2023-330: Online Undertakings Registration Regulations, and exemption order regarding those regulations*. <https://crtc.gc.ca/eng/archive/2023/2023-329.htm>

²²¹ YouTube Creators. (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=pKEGnAo4Egg>; Geist, M. (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/>

²²² Québec Official Publisher. (2025, December 12). *Bill 109: An Act to affirm the cultural sovereignty of Québec and to enact the Act respecting the discoverability of French-language cultural content in the digital environment (2025, chapter 38)*. https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/en/2025/2025C38A.PDF; Computer & Communications Industry Association. (2025, December). *Trade Implications of Québec's Cultural Sovereignty Streaming Act, Bill 109*. <https://ccianet.org/wp-content/uploads/2025/12/Trade-Implications-of-Quebecs-Cultural-Sovereignty-Streaming-Act-Bill-109.pdf>

undetermined. Nonetheless, what Quebec is proposing will impose an additional layer of content-selection, presentation, and compliance requirements on U.S. audio and video services operating in Quebec, adding complexity to overlapping federal broadcasting regulation. In addition, questions have been raised as to whether such a measure is even constitutional under Canadian law.²²³ CCIA urges USTR to address discriminatory implementation and seek clear limits on requirements that condition market access on preferential treatment for designated cultural content or services.

Forced Revenue Transfers for Digital News

In April 2022, Canadian Heritage introduced Bill C-18, the Online News Act,²²⁴ 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, 2023.

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, this legislation 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.²²⁵ 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.²²⁶ 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

²²³ Geist. (2025) *Quebec’s Streaming Regulation Bill 109*.

<https://www.michaelgeist.ca/2025/06/quebecs-streaming-regulation-bill-109-unconstitutional-unnecessary-and-unworkable/>

²²⁴ Parliament of Canada. (2022). *Bill C-18: An Act respecting online communications platforms that make news content available to persons in Canada (first reading)*.

<https://www.parl.ca/DocumentViewer/en/44-1/bill/C-18/first-reading>

²²⁵ House of Commons of Canada. (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>

²²⁶ 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>

regulations²²⁷ 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.²²⁸

The final implementing regulations²²⁹ replaced the proposed revenue-based contribution formula with an exemption pathway under which one U.S. company provides C\$100 million annually, adjusted for inflation, through an agreement supporting eligible Canadian news businesses.²³⁰ The regulations cap allocations to private broadcasters at 30% and to CBC/Radio-Canada at 7%, with the balance allocated to other eligible news businesses. This framework continues to condition relief from mandatory bargaining obligations on a substantial payment by a U.S. digital service, raising concerns about compelled revenue transfers and discriminatory treatment. In the face of this unjustified burden, one targeted U.S. firm chose to exit the news market, depriving news organizations of valuable referral traffic and consumers of an alternative means of accessing news.

The harms to the internet landscape and consumers in Canada are clear, 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.”²³¹ USTR should assess the application of this law under relevant USMCA and WTO obligations, taking account of the treatment of comparable suppliers, applicable coverage thresholds, and relevant exceptions, including USMCA Article 32.6.

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

²²⁷ Government of Canada. (2023, September 2). *Regulations Respecting the Application of the Online News Act, the Duty to Notify and the Request for Exemptions*. Canada Gazette, Part I, Vol. 157, No. 35.

<https://gazette.gc.ca/rp-pr/p1/2023/2023-09-02/html/reg1-eng.html>

²²⁸ 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>

²²⁹ Government of Canada. (2024, January 3). *Online News Act Application and Exemption Regulations: SOR/2023-276*. Canada Gazette, Part II, Vol. 158, No. 1.

<https://gazette.gc.ca/rp-pr/p2/2024-01-03/html/sor-dors276-eng.html>

²³⁰ Canadian Radio-television and Telecommunications Commission. (2024, October 28). *Online News Decision CRTC 2024-262: Exemption Order from the Online News Act granted to Google*.

<https://crtc.gc.ca/eng/archive/2024/2024-262.htm>

²³¹ 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/>

its wide and timely distribution.²³² 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 to address its adverse effects on U.S. suppliers and potential conflicts with international trade obligations.

Government Imposed Restrictions on Internet Content and Related Access Barriers

Canada's recent online-harms proposals, including Bill C-63,²³³ introduced on February 26, 2024, and Bill C-412,²³⁴ lapsed without enactment. On June 10, 2026, the government introduced Bill C-34, the Safe Social Media Act, which is before the House of Commons at second reading.²³⁵ The bill would establish obligations for regulated social media services and AI chatbot services, including safety measures, plans, and reporting requirements. It would also restrict accounts for users under 16 on specified regulated social media services, subject to exemptions based on sufficient safeguards.

The proposal includes removal requirements for specified child sexual victimization and non-consensual intimate content, generally within 24 hours unless a different period is prescribed. It provides for administrative monetary penalties up to the greater of C\$10 million or 3% of global gross revenue, and, for specified offences prosecuted by indictment, fines up to the greater of C\$20 million or 5%. Although motivated by legitimate concerns, these proposed duties could create substantial compliance burdens for U.S. providers. USTR should seek clear scope, proportionate implementation, and safeguards against requirements that unnecessarily restrict lawful services or undermine privacy and security.

Challenges to the Development of AI

The Artificial Intelligence and Data Act proposed in former Bill C-27 lapsed in 2025 without enactment.²³⁶ Canada launched a new national AI strategy in June 2026, emphasizing domestic AI capabilities and a build-partner-buy approach.²³⁷ This raises important implementation questions for U.S. suppliers: whether participation will enhance access to international

²³² 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>

²³³ Parliament of Canada. (n.d.). *Bill C-63, 44th Parliament, 1st session*. LEGISinfo. <https://www.parl.ca/legisinfo/en/bill/44-1/c-63>

²³⁴ Parliament of Canada. (n.d.). *Bill C-412: Promotion of Safety in the Digital Age Act, 44th Parliament, 1st session*. LEGISinfo. <https://www.parl.ca/legisinfo/en/bill/44-1/c-412>

²³⁵ Parliament of Canada. (n.d.). *Bill C-34: Safe Social Media Act, 45th Parliament, 1st session*. LEGISinfo. <https://www.parl.ca/legisinfo/en/bill/45-1/c-34>

²³⁶ Parliament of Canada. (n.d.). *Bill C-27: Digital Charter Implementation Act, 2022, 44th Parliament, 1st session*. LEGISinfo. <https://www.parl.ca/legisinfo/en/bill/44-1/c-27>

²³⁷ Innovation, Science and Economic Development Canada. (2026, June 8). *Canada's National Artificial Intelligence Strategy: AI for All*. <https://ised-isde.canada.ca/site/ised/en/canadas-national-artificial-intelligence-strategy-ai-all>

technology and reflect competitive procurement or diminished access through discriminatory preferences. Consistent with CCIA's comments on Canada's AI strategy,²³⁸ USTR should encourage interoperable, risk-based policies and oppose nationality-based restrictions on AI services, infrastructure, and investment.

On July 23, 2026, the government opened a consultation on AI transparency, running through September 23, 2026.²³⁹ It addresses matters including system information, training-data transparency, incident reporting, and treatment of AI agents. This initiative merits monitoring with a view to ensuring that any resulting proposed measures protect confidential business information and avoid unnecessary duplication or compliance burdens for services operating across borders.

Canada's Copyright Act lacks explicit provisions for AI-generated works, creating uncertainty about their copyrightability and ownership. The Copyright Act also lacks a specific exception for text and data mining, which are crucial for AI model training. While limited exceptions like fair dealing may apply, the absence of clear guidelines and definitive judicial decisions could restrict the use of copyrighted materials in AI development. As AI advances, Canada will need to update its copyright framework to address these issues and clarify AI-related activities.

Restrictions on Cross-Border Data Flows

The Government of Quebec passed privacy legislation in September 2021 that introduced additional conditions for transferring personal information outside Quebec.²⁴⁰ Covered businesses must conduct a privacy impact assessment before such transfers, considering the information's sensitivity, intended use, safeguards, and the destination jurisdiction's legal framework. Transfers may proceed where the assessment establishes adequate protection and must be governed by a written agreement reflecting the assessment and any necessary risk-mitigation measures. These requirements create additional assessment and contracting obligations for cross-border services. 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

²³⁸ Computer & Communications Industry Association. (2025, October 30). *CCIA Comments on Canada's AI Strategy*. <https://ccianet.org/library/ccia-comments-on-canadas-ai-strategy/>

²³⁹ Innovation, Science and Economic Development Canada. (2026, July 23). *Government of Canada launches public consultation on AI transparency*. <https://www.canada.ca/en/innovation-science-economic-development/news/2026/07/government-of-canada-launches-public-consultation-on-ai-transparency.html>

²⁴⁰ 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>

entering into force September 22, 2023.²⁴¹ 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 2022.²⁴²

On June 15, 2026, the Canadian government introduced Bill C-36, the Protecting Privacy and Consumer Data Act, which is before the House of Commons at second reading.²⁴³ The proposed Protecting Privacy and Consumer Data Act would require organizations to ensure equivalent protection for personal information transferred to service providers and disclose whether interprovincial or international transfers may have reasonably foreseeable privacy implications. Section 57 would additionally require organizations, before disclosing or transferring personal information outside Canada, to conduct a privacy impact assessment in accordance with prescribed requirements and implement measures mitigating the identified risks. Organizations would have to provide the proposed Commission with access to, or a copy of, the assessment on request. These transfer-specific duties could impose additional compliance costs on integrated U.S.–Canada services. Its consent exception for publicly available information would depend on prescribed categories, leaving the treatment of some information used in AI development dependent on regulations. The bill also provides explanation rights for certain automated decisions having significant effects on individuals. These provisions warrant attention to regulatory clarity and interoperability. USTR should monitor development of this bill, and its consistency with USMCA’s data transfer obligations (Article 19.11). If passed, USTR should encourage implementation that protects privacy while supporting cross-border services and avoiding unnecessary restrictions on legitimate data use.

Taxation of Digital Products and Services

Canada formally repealed its Digital Services Tax Act on March 26, 2026,²⁴⁴ following its June 2025 announcement that it would rescind the measure.²⁴⁵ The Canada Revenue Agency states that businesses no longer have obligations under the Act and that payments will be refunded with interest calculated from the date of receipt. CCIA welcomes the removal of this discriminatory

²⁴¹ 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/>; Lewis Brisbois. (2022, February 16). *Canada Reforms Its Data Privacy Laws Through Enactment of Quebec Bill 64*. <https://lewisbrisbois.com/insights/blogs/canada-reforms-its-data-privacy-laws-through-enactment-of-quebec-bill-64>

²⁴² U.S. International Trade Commission. (2022, August). *The Year in Trade 2021: Operation of the Trade Agreements Program* (73rd report, Publication No. 5349). <https://www.usitc.gov/publications/332/pub5349.pdf>

²⁴³ Parliament of Canada. (n.d.). *Bill C-36: An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts, 45th Parliament, 1st session*. LEGISinfo. <https://www.parl.ca/legisinfo/en/bill/45-1/c-36>

²⁴⁴ Canada Revenue Agency. (2026, March 26). *Digital services tax repealed*. <https://www.canada.ca/en/services/taxes/excise-taxes-duties-and-levies/digital-services-tax.html>

²⁴⁵ 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>

tax.²⁴⁶ USTR should monitor completion of the refund process and discourage the introduction of a replacement measure that similarly targets U.S. digital suppliers.

Threats to the Security of Devices and Services

Canada's cybersecurity legislation, formerly Bill C-8, received Royal Assent on June 15, 2026.²⁴⁷ Its Telecommunications Act amendments, focusing on untrustworthy network equipment, authorize security orders restricting specified products and services from being marketed in Canada, requiring equipment removal, and prohibiting or terminating service agreements. The powers are subject to statutory necessity and reasonableness requirements, but orders may include non-disclosure restrictions and resulting financial losses are not compensable under the Act. The legislation also establishes the Critical Cyber Systems Protection Act framework for designated operators, including cybersecurity programs, supply-chain risk management, and incident reporting; commencement of that framework is to be set by order. These powers could affect U.S. technology suppliers through restrictions imposed on Canadian customers. USTR should seek transparent, proportionate, nationality-neutral implementation and safeguards against unnecessary exclusion of U.S. products and services.

On March 12, 2026, the government introduced Bill C-22, the Lawful Access Act.²⁴⁸ The bill passed the House of Commons on June 18, 2026 and is currently under Senate review. It would expand mechanisms for obtaining subscriber and transmission information and establish a Supporting Authorized Access to Information Act governing service-provider capabilities and assistance. Its provisions concerning technical requirements, information retention, and assistance could create substantial implementation costs and security concerns for U.S. communications and cloud providers.

The House-passed text contains safeguards that materially limit these powers. It provides judicial authorization for subscriber-information production orders and restricts requirements to decrypt user-encrypted information unless the provider supplied the encryption and possesses the necessary means of decryption. It also restricts requirements that would create a systemic vulnerability, but that goal is in tension with rights for targeted authorized access. USTR should scrutinize the practical effect of these safeguards and any implementing regulations, including whether technical-capability obligations undermine secure services or impose disproportionate costs on foreign suppliers.

²⁴⁶ Computer & Communications Industry Association. (2026, March 30). *CCIA Applauds Canada's Withdrawal of Discriminatory Digital Services Tax*.

²⁴⁷ Parliament of Canada. (n.d.). *Bill C-8: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 45th Parliament, 1st session. LEGISinfo. <https://ccianet.org/news/2026/03/ccia-applauds-canadas-withdrawal-of-discriminatory-digital-services-tax/>
<https://www.parl.ca/legisinfo/en/bill/45-1/c-8>

²⁴⁸ Parliament of Canada. (n.d.). *Bill C-22: Lawful Access Act, 2026*, 45th Parliament, 1st session. LEGISinfo. <https://www.parl.ca/legisinfo/en/bill/45-1/c-22>

Chile

Customs-Related Restrictions and Import Barriers for Goods

Under the U.S.-Chile Free Trade Agreement,²⁴⁹ 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.” Despite progress, this system is not yet fully implemented. USTR should encourage Chile to ensure that its electronic courier-manifest procedures provide effective access for express-shipment operators and timely customs clearance.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Chilean financial regulator (CMF) has rules related to the general IT outsourcing of services (RAN 20-7) that allow use of cloud services from suppliers based both in Chile and abroad. Chapter 20-7 of the Comisión para el Mercado Financiero’s (CMF) banking rules generally requires a back-up data-processing center in Chile when significant or strategic activities are processed abroad.²⁵⁰ Following a public consultation process in 2019, the CMF agreed to create an exception for the requirement. However, the regulator authorized a narrow exception exclusively for banks that maintain adequate operational risk management based on a CMF assessment—a standard that excludes many Chilean financial institutions. A consultation opened by the CMF in May 2026 introduces a “fourth party” definition that would pass compliance obligations onto subcontractors and would retain in-country contingency requirements. These conditions can constrain U.S. cloud suppliers’ ability to serve Chilean financial institutions through global infrastructure. USTR should encourage CMF to preserve workable alternatives to local infrastructure and ensure that additional oversight requirements remain proportionate.

Challenges to the Development of Artificial Intelligence

Chile’s bill regulating artificial intelligence systems (consolidated Bulletins Nos. 16.821-19 and 15.869-19) passed the Chamber of Deputies in October 2025 and remains under Senate consideration.²⁵¹ The proposal classifies AI uses by risk and establishes requirements concerning human oversight, technical safety, transparency, and accountability, with enforcement assigned to the Data Protection Agency. Its implementing classifications and requirements could affect U.S. suppliers offering AI-enabled services in

²⁴⁹ Office of the United States Trade Representative. (2003, June 6). *United States–Chile Free Trade Agreement*. <https://ustr.gov/trade-agreements/free-trade-agreements/chile-fta/final-text>

²⁵⁰ Comisión para el Mercado Financiero. (2019, December 26). *CMF publica cambios a normativa sobre externalización de servicios en bancos e instituciones financieras*. <https://www.cmfchile.cl/portal/prensa/625/w4-article-28049.html>

²⁵¹ Cámara de Diputadas y Diputados de Chile. (n.d.). *Regula los sistemas de inteligencia artificial: Boletín N° 16821-19, refundido con N° 15869-19—Tramitación*. <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmBOLETIN=1784&prmID=17429>

Chile. USTR should monitor this bill and encourage clear, proportionate obligations and alignment with international standards to avoid unnecessary barriers to cross-border supply.

Restrictions on Cross Border Data Flows

Chile's Personal Data Protection Law,²⁵² inspired by the EU's General Data Protection Regulation, is scheduled to enter into force in December 2026. In December 2025, the Ministry of Economy approved model contractual clauses for international data transfers as an interim mechanism pending equivalent rules from the Data Protection Agency.²⁵³ In February 2026, Law No. 21.806 also authorized the Agency's governing council to undertake specified preparatory and rulemaking functions before the new regime takes effect.²⁵⁴

A government bill dated August 31, 2026 (Bulletin No. 18.623-07), proposes postponing implementation until December 1, 2027 but its fate is uncertain.²⁵⁵ USTR should urge Chile to clarify the implementation timetable and the continuing validity of interim transfer mechanisms, and provide sufficient time to comply with final rules without disrupting cross-border data flows.

Government Imposed Restrictions on Internet Content and Related Access Barriers

Chile's bill on digital simulations and synthetic content (Bulletin No. 17.795-19) would require platforms to remove content within 24 to 48 hours on the basis of a private request, without a judicial order, and to prevent re-uploads of substantially identical material without a new order. These duties place removal decisions on providers without judicial review and create pressure toward general monitoring of user content. USTR should urge Chile to condition removal obligations on judicial orders and to avoid stay-down duties that function as general monitoring requirements.

²⁵² *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>.

²⁵³ Ministerio de Economía, Fomento y Turismo. (2025, December 19). *Resolución exenta N° RAEX202503748: Aprueba las cláusulas contractuales modelo para transferencias internacionales que indica*. <https://www.diariooficial.interior.gob.cl/publicaciones/2025/12/19/44328/01/2742586.pdf>

²⁵⁴ Chile. (2026, February 5). *Ley N° 21.806: Otorga reajuste general de remuneraciones a las y los trabajadores del sector público, concede aguinaldos que señala, concede otros beneficios que indica y modifica diversos cuerpos legales*, art. 54. <https://www.bcn.cl/leychile/navegar?idNorma=1221118>

²⁵⁵ Presidencia de la República de Chile. (2026, August 31). *Mensaje N° 110-374: Proyecto de ley que modifica la ley N° 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales* (Boletín N° 18.623-07). <https://www.camara.cl/verDoc.aspx?prmID=18854&prmTIPO=INICIATIVA>

Other Barriers to Digital Trade

Chile took additional steps to implement its Cybersecurity Framework Law in 2026,²⁵⁶ which generally entered into force on January 1, 2025. This law is modeled after the EU's Network and Information Security Directive 2 (NIS2). Provisions governing designation and specific duties of Operators of Vital Importance, incident reporting, and sanctions took effect on March 1, 2025.²⁵⁷ On July 24, 2026, the National Cybersecurity Agency (ANCI) completed its first designation process, identifying 1,154 institutions as Operators of Vital Importance subject to enhanced cybersecurity obligations.²⁵⁸ Chile requires cybersecurity incidents to be reported within 3 hours, compared to the international standard of 72 hours, requiring foreign companies to create costly Chile-specific compliance systems. The financial impact is substantial: according to the "AI Unlocking Ambitions" study, companies must dedicate 19% of their investment capital just to meet local regulatory requirements including this. ANCI also addressed an access concern in December 2025 through General Instruction No. 2, which permits alternative authentication for incident-reporting personnel unable to obtain Clave Única (a government-run digital identity service), subject to verification of their relationship with the regulated institution. USTR should encourage ANCI to make this alternative readily accessible to overseas personnel and implement cybersecurity obligations proportionately.

On February 22, 2026, Chile implemented a QR-code labeling regime for most non-medical short-range wireless devices under SUBTEL Resolution No. 737/2025 and subsequent amendments.²⁵⁹ The regime replaces prior certification for covered devices but requires QR-linked Spanish-language compliance information and identification of an importer or representative in Chile. It also applies to previously certified inventory. Alternative placement on the device or accompanying paper documentation is permitted where placement on exterior packaging is not feasible. USTR has identified concerns about country-specific packaging and applicability to existing inventory and should encourage flexible labeling and workable treatment of previously certified stock to minimize unnecessary burdens on U.S. suppliers.

²⁵⁶ Ministerio del Interior y Seguridad Pública. (2024, December 24). *Decreto con fuerza de ley N° 1-21.663: Fija planta de personal de directivos de la Agencia Nacional de Ciberseguridad y regula otras materias a que se refiere el artículo primero transitorio de la Ley N° 21.663*, art. 2.

<https://www.diariooficial.interior.gob.cl/publicaciones/2024/12/24/44032/01/2588834.pdf>

²⁵⁷ *Ley Marco de Ciberseguridad* [Chile] Law no. 21663. (2024).

<https://www.bcn.cl/leychile/navegar?idNorma=1202434>.

²⁵⁸ Agencia Nacional de Ciberseguridad. (2026, July 24). *ANCI finaliza el primer proceso de calificación de Operadores de Importancia Vital*.

<https://anci.gob.cl/noticias/anci-finaliza-el-primer-proceso-de-calificacion-de-operadores-de-importancia-vital/>

²⁵⁹ Subsecretaría de Telecomunicaciones. (2025, May 22). *Resolución exenta N° 737: Modifica Resolución N° 1.985 exenta, de 2017, de la Subsecretaría de Telecomunicaciones que fija norma técnica de equipos de alcance reducido*. <https://www.bcn.cl/leychile/navegar?idNorma=1213556>

A Child Safety bill²⁶⁰ under discussion in Congress and supported by the Executive creates obligations that apply to every provider of digital platforms that offers services to users in Chile, regardless of its place of incorporation, domicile, or establishment (Article 2). This approach is overly broad, as it effectively subjects every service provided from the U.S. to Chile to the full scope of Chilean regulation. Furthermore, Article 19 of the Bill requires foreign providers to designate a legal representative domiciled in Chile within ninety calendar days of the publication of the law, under penalty of a serious infringement that, if repeated, may lead to the suspension of the service.

Chile's bill regulating neurotechnology and neural data (Boletín N° 13.828-19) would create a distinct "neural data" category, impose strict liability on providers, and condition activity on prior government permits. Its definitions of neurotechnology are broad enough to cover consumer wearable devices and could subject them to classification and registration as medical devices. These requirements would restrict the supply of AI-enabled and wearable products to Chile by U.S. companies. USTR should urge Chile to avoid over-regulation and advance on necessary amendments to limit impact on consumer products, innovation and investment.

Chile's bill on digital simulations and synthetic content (Boletín No. 17.795-19) allows for electronic contact mechanism (rather than local representative) and enforcement to the courts with capped, locally denominated fines. Risks nevertheless persist: the text under discussion would still require platforms to remove content within 24 to 48 hours on the basis of a private request, without a judicial order, and to prevent re-uploads of substantially identical material without a new order. These duties place removal decisions on providers without judicial review and create pressure toward general monitoring of user content. USTR should urge Chile to condition removal obligations on judicial orders and to avoid stay-down duties that function as general monitoring requirements.

A bill before the Chilean Congress (Boletín 18362-19) would require digital platforms to establish a legal domicile and appoint a jointly liable local representative in Chile, respond to judicial requests within 48 hours, and refrain from invoking their own terms of service, subject to high fines or suspension of service. Joint liability is tantamount to a mandatory local establishment and may be inconsistent with Chile's commitments under the U.S.-Chile Free Trade Agreement. It would also disqualify affected providers from the simplified VAT regime for non-residents while creating permanent establishment exposure. This bill would particularly affect U.S. digital companies in Chile. USTR should urge Chile to honor existing trade commitments.

²⁶⁰ Chile National Congress. (2026). Boletín N°18246-18.
https://www.camara.cl/verDoc.aspx?prmID=36328&prmTipo=DOCUMENTO_COMISIONDOCUMENTO.

China

The Chinese market continues to be hostile to foreign companies, and the focus on U.S. information technologies and internet services has intensified. Restrictions affecting information infrastructure, cloud services, data transfers, and e-commerce, together with extensive website blocking, continue to impede foreign suppliers' access to the Chinese market.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

China significantly limits foreign cloud service operators' market access, in concert with its national plan to promote the Chinese cloud computing industry. China categorizes cloud as a telecommunications service subject to telecommunications licensing. Only companies established in China, after obtaining a telecom business license, can offer cloud services. Foreign companies' participation in the applicable sector (value added telecommunication (VAT)) is highly restrictive. Based on current regulations, foreign companies are still denied access to the business sectors critical to cloud services nationwide, including Internet data center (IDC) business, and content distribution network (CDN) service. Although the Ministry of Industry and Information Technology announced liberalization of the VAT sector on a pilot basis in April 2024, access is limited to four designated areas, posing commercial and technical difficulties for cloud service providers with interconnected data centers both inside and outside those areas. By June 2026, authorities reported approving 166 foreign-invested enterprises under the program.²⁶¹ USTR should seek broader, transparent, and commercially meaningful access for U.S. cloud providers beyond the pilot framework.

Government Imposed Restrictions on Internet Content and Related Access Barriers

Over the past several years, China has introduced a series of measures that significantly tighten state control over online expression and impose extensive new compliance burdens on online services. Together, these initiatives illustrate a model of digital governance centered on pervasive state oversight, mandatory identity tracking, and broad content control.

- 2022 Internet Comment Rules: Effective December 15, 2022, the revised rules require backend identity verification, real-time monitoring, removal and reporting of prohibited information, and moderation staff proportionate to service scale. Comments on news information must undergo review before publication. The rules also cover replies, livestream comments, and "likes," extending compliance obligations across multiple forms of user engagement.²⁶²

²⁶¹ Ministry of Industry and Information Technology. (2026, June 3). 166家外资企业获增值电信业务经营试点批复 [166 Foreign-Invested Enterprises Receive Approvals Under the Value-Added Telecommunications Pilot]. Xinhua. <https://www.xinhuanet.com/fortune/20260603/e6187635a2c441e6bb5cda59a15ac0c9/c.html>

²⁶² Cyberspace Administration of China. (2022, November 16). 互联网跟帖评论服务管理规定 [Provisions on the Administration of Internet Comment Services], Articles 4, 7 and 16. https://www.cac.gov.cn/2022-11/16/c_1670253725725039.htm

- 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.²⁶³
- National Network Identity Authentication: Rules effective July 15, 2025, established a government-operated service issuing digital identifiers for online identity verification.²⁶⁴ Participation is voluntary, and alternative lawful verification methods must remain available. Participating platforms generally may not demand additional plaintext identity information from users successfully verified through the service. Although intended to reduce platforms' collection of identity data, centralized government authentication raises concerns about state oversight of online activity.
- 2026 Draft Internet Information Service Measures: In July 2026, CAC released a revised draft of the Internet Information Service Administrative Measures.²⁶⁵ The proposal would shift regulatory approval for covered services to CAC, reinforce real-name verification and ongoing account checks, and impose extensive content-monitoring, removal, recordkeeping, and reporting duties. These requirements could further raise market-entry and operating costs for U.S. suppliers. USTR should monitor the proposal's final scope and implementation.

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.

Challenges to the Development of AI

China's Interim Measures for Generative Artificial Intelligence Services, effective August 15, 2023, apply to AI-enabled services offered to the public in China.²⁶⁶ Providers of

²⁶³ Jiang, C. (2023, 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>

²⁶⁴ Ministry of Public Security et al. (2025, May 19). 国家网络身份认证公共服务管理办法 [Administrative Measures for the National Network Identity Authentication Public Service], Order No. 173, Articles 2–3 and 16. https://www.cac.gov.cn/2025-05/23/c_1749711107835487.htm

²⁶⁵ Cyberspace Administration of China. (2026, July 3). 国家互联网信息办公室关于《互联网信息服务管理办法(修订草案征求意见稿)》再次公开征求意见的通知 [Notice Again Soliciting Public Comments on the Internet Information Service Administrative Measures (Revised Draft)]. https://www.cac.gov.cn/2026-07/03/c_1784822399677167.htm

²⁶⁶ Cyberspace Administration of China et al. (2023, July 10). 生成式人工智能服务管理暂行办法 [Interim Measures for the Administration of Generative Artificial Intelligence Services], Order No. 15, Articles 2 and 24. https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

services with public-opinion attributes or social-mobilization capabilities must conduct security assessments and complete algorithm filings but so far are not subject to a standalone AI licensing requirement. Providers must comply with broad content restrictions and promotion of “socialist core values,” satisfy training-data and personal-information requirements, and take corrective action when unlawful content is identified. They must also put in place limits on use by minors. Regulators may require explanations of training-data sources and algorithms and share with the regulators necessary technical attributes and data sources. Although proprietary consumer-facing models (Claude, Gemini, ChatGPT) are blocked in China, these obligations create substantial compliance and market-access challenges for U.S. providers seeking to serve enterprise customers.

China finalized its National AI Industry Comprehensive Standardization System Construction Guidelines in June 2024.²⁶⁷ The guidelines set targets for developing more than 50 national and industry standards and participating in more than 20 international standards by 2026. USTR should monitor whether implementation creates China-specific requirements that disadvantage foreign suppliers or diverge unnecessarily from international standards.

China also issued GB/T 45654-2025, “Cybersecurity Technology—Basic Security Requirements for Generative Artificial Intelligence Service,” effective November 1, 2025.²⁶⁸ This is a recommended national standard, as opposed to a regulation. Its application alongside mandatory AI rules warrants scrutiny for additional compliance burdens and disclosure risks, particularly if it becomes de facto mandatory.

Additionally, China’s AI-generated content labeling measures took effect September 1, 2025.²⁶⁹ Covered providers must apply visible labels in specified cases and embed identifying information in file metadata. Content-distribution platforms must check metadata and label identified or suspected AI-generated content, while application-distribution platforms must verify relevant labeling materials. These obligations require changes across content-generation and distribution systems, increasing compliance costs for U.S. suppliers.

Moreover, effective July 15, 2026, China’s Interim Measures for AI Anthropomorphic Interaction Services impose additional obligations on services providing sustained emotional

²⁶⁷ Ministry of Industry and Information Technology et al. (2024, June 5). 四部门关于印发国家人工智能产业综合标准化体系建设指南(2024版)的通知 [Notice Issuing the National AI Industry Comprehensive Standardization System Construction Guidelines (2024 Edition)], 工信部联科[2024]113号.

https://www.cac.gov.cn/2024-07/03/c_1721686809220407.htm

²⁶⁸ State Administration for Market Regulation and Standardization Administration of China. (2025, April 25). 网络安全技术 生成式人工智能服务安全基本要求 [Cybersecurity Technology—Basic Security Requirements for Generative Artificial Intelligence Service], GB/T 45654-2025.

<https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=F67D3F376E0A0A0FF5317FB36B32A30A>

²⁶⁹ Cyberspace Administration of China et al. (2025, March 7). 人工智能生成合成内容标识办法 [Measures for Labeling AI-Generated Synthetic Content], Article 14.

https://www.cac.gov.cn/2025-03/14/c_1743654684782215.htm

interaction.²⁷⁰ Providers must conduct security assessments when launching covered services or making specified changes, submit assessment reports, complete algorithm filings, and implement user-protection and content controls. Ordinary assistants without sustained emotional interaction fall outside the rules. The assessment, filing, and political-content requirements create additional barriers for U.S. providers entering this market.

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.²⁷¹ The United States International Trade Commission has estimated that billions of dollars are being lost in the market as a result.²⁷² 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 continues to censor cross-border internet traffic through extensive website blocking, broadly restricting access to foreign information and digital services. China's blocking mechanism, colloquially known as the Great Firewall, is fundamentally protectionist and anticompetitive, and contrary to China's WTO commitments and separate commitments to the United States.²⁷³

Stringent restrictions on the cross-border transfer of data, both personal and non-personal, are implemented through three overlapping laws: the Cybersecurity Law, originally effective June 1, 2017, and amended effective January 1, 2026,²⁷⁴ the 2021 Data Security Law,²⁷⁵ and the 2021 Personal Information Protection Law.²⁷⁶ Other measures include:

²⁷⁰ Cyberspace Administration of China et al. (2026, April 10). 人工智能拟人化互动服务管理暂行办法 [Interim Measures for the Administration of AI Anthropomorphic Interaction Services], Order No. 21, Articles 2, 9–26 and 32. https://www.cac.gov.cn/2026-04/10/c_1777558395078289.htm

²⁷¹ CCIA. (2022, October 28). *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>

²⁷² 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; U.S. International Trade Commission. (2022, July). *Foreign Censorship, Part 2: Trade and Economic Effects on U.S. Businesses*, Publication No. 5334, Tables 3.3–3.4 and Figure 3.4. <https://www.usitc.gov/publications/332/pub5334.pdf>

²⁷³ 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.

²⁷⁴ Standing Committee of the National People's Congress. (2025, October 28). 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China, as amended], Article 81. https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm

²⁷⁵ Standing Committee of the National People's Congress. (2021, June 10). 中华人民共和国数据安全法 [Data Security Law of the People's Republic of China], Presidential Order No. 84. <https://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml>

²⁷⁶ 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/>

- The Decision on Strengthening Online Information Protection, effective from December 28, 2012 (Decision);
- 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.
- The Measures for Personal Information Export Certification, effective January 1, 2026.
- The Compliance Guidelines on Promoting and Regulating Cross-border data flows in the Financial Sector, effective April 17, 2025.

China's cross-border data regime continues to impose classification, assessment, contractual, and reporting burdens, although exemptions cover certain commercial, employment-related, and lower-volume transfers. Effective January 1, 2026, new measures formalize certification as an alternative to standard contracts for eligible transfers by non-CII operators.²⁷⁷ Certification requires a personal-information protection impact assessment and is valid for three years. The export of data deemed "important" and transfers meeting higher thresholds remain subject to security assessment unless an applicable exemption applies. Uncertainty over classification and sector-specific requirements continues to complicate international operations and use of global cloud services.

Threats to the Security of Devices and Services

China's Cryptography Law went into effect on January 1, 2020,²⁷⁸ 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 used to protect information that is deemed to not be state secrets. China's revised Commercial Cryptography Administrative Regulations took effect on July 1, 2023, establishing certification,

²⁷⁷ Cyberspace Administration of China and State Administration for Market Regulation. (2025, October 14). 个人信息出境认证办法 [Measures for Personal Information Export Certification], Order No. 20, Articles 3, 5 and 19. https://www.cac.gov.cn/2025-10/17/c_1762449728720008.htm

²⁷⁸ 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>

security-assessment, and regulatory approval requirements for covered encryption products and uses.²⁷⁹ Further rules governing commercial cryptography in CII took effect on August 1, 2025.²⁸⁰ These require certified encryption products and services, regulatory approval of algorithms, protocols, and key-management mechanisms, and assessments of encryption deployment, alongside annual reporting obligations. These requirements can increase compliance costs and restrict foreign suppliers' ability to deploy their existing technologies in China.

Revised Measures for the Administration of Cryptography Use in Electronic Authentication Services took effect on July 1, 2026.²⁸¹ They require covered providers to obtain a cryptography-use license and maintain electronic authentication systems in China that comply with applicable national cryptographic standards. Licensing may involve security reviews, interoperability testing, and on-site inspections. These requirements can constrain cross-border service delivery and increase market-entry costs for U.S. suppliers.

Industry remains concerned about China's implementation of its Standardization Law and restrictions on foreign participation in standards development. USTR's 2026 NTE Report confirms that foreign companies may participate in some cybersecurity standards working groups but remain excluded from the encryption standards working group. Requirements to use domestic cryptographic algorithms in certain applications, together with standards that diverge from international standards, can require product modifications and increase compliance costs for U.S. suppliers.

The 2021 Critical Information Infrastructure (CII) Security Protection Regulation mandates enhanced protection of CII. This regulation promotes the procurement of "secure and trustworthy" network products and services, potentially resulting in unequal treatment between domestic and foreign companies' products. Companies identified as CII operators face additional obligations under Chinese security legislation, including mandatory certification, assessment, and cybersecurity reviews. In a similar vein, the concept of "important data" was introduced in Article 37 of the Cybersecurity Law (CSL) in 2017. In recent years, a series of guidelines have been continuously issued to guide data processors in data classification and identification of important data, imposing an increasing compliance burden on companies that own important data.

²⁷⁹ State Council of the People's Republic of China. (2023, April 27). 商用密码管理条例 [Commercial Cryptography Administrative Regulations], Order No. 760, Articles 20–22, 31–34, 38–40 and 67. https://www.mee.gov.cn/zcwj/gwywj/202305/t20230529_1031579.shtml

²⁸⁰ State Cryptography Administration, Cyberspace Administration of China, and Ministry of Public Security. (2025, June 11). 关键信息基础设施商用密码使用管理规定 [Provisions on the Administration of Commercial Cryptography Use in Critical Information Infrastructure], Order No. 5, Articles 2 and 25. https://www.cac.gov.cn/2025-07/01/c_1753083518894995.htm

²⁸¹ State Cryptography Administration. (2026, May 30). 电子认证服务使用密码管理办法 [Measures for the Administration of Cryptography Use in Electronic Authentication Services], Order No. 6, Article 25. https://www.oscca.gov.cn/sca/xxgk/2026-06/03/content_1061341.shtml

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.²⁸² CII operators face heightened security obligations, including annual network-security assessments and certification or testing requirements for covered products. Procurement is subject to cybersecurity review when it affects or may affect national security. Relatedly, the concept of "important data," introduced in Article 37 of the Cybersecurity Law in 2017,²⁸³ 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.

China's Measures for Network Data Security Risk Assessment took effect August 20, 2026.²⁸⁴ Processors of data deemed "important" must conduct annual risk assessments, retain reports for at least three years, and submit them within 20 working days after completing the annual assessment. Regulators may require assessments by certified third parties under specified circumstances. These procedures reinforce the compliance costs and disclosure concerns associated with important-data designation.

China's National Cybersecurity Incident Reporting Measures took effect November 1, 2025.²⁸⁵ For incidents meeting the prescribed severity threshold, reporting deadlines run from discovery or awareness and generally require reporting within one hour for CII incidents, two hours for central state bodies and their directly affiliated units, and four hours for other network operators. Preliminary reports may be supplemented as

²⁸² State Council of the People's Republic of China. (2021, July 30). 关键信息基础设施安全保护条例 [Regulations on the Security Protection of Critical Information Infrastructure], Order No. 745. https://www.cac.gov.cn/2021-08/17/c_1630785976988160.htm

²⁸³ 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

²⁸⁴ Cyberspace Administration of China, Ministry of Industry and Information Technology, and Ministry of Public Security. (2026, June 18). 网络数据安全风险评估办法 [Measures for Network Data Security Risk Assessment], Order No. 24, Article 25. Reproduced by CERNET. https://www.cernet.edu.cn/xxh/focus/zc/202606/t20260622_2747167.shtml

²⁸⁵ Cyberspace Administration of China. (2025, September 11). 国家网络安全事件报告管理办法 [National Cybersecurity Incident Reporting Measures], Article 14. https://www.cac.gov.cn/2025-09/15/c_1759583017717009.htm

information becomes available. Operators must also require relevant service providers to notify them of detected incidents and assist with reporting. These short deadlines can increase incident-response and coordination costs for U.S. suppliers.

China's cybersecurity review regime further compounds these barriers. The Cybersecurity Review Measures (CSRM), effective February 15, 2022,²⁸⁶ 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,²⁸⁷ effectively barring CII operators from purchasing its products. On August 6, 2026, the Cybersecurity Review Office initiated a review of Palo Alto Networks products sold in China.²⁸⁸ Additionally, in January 2026, Reuters reported that Chinese authorities had instructed domestic companies to stop using cybersecurity software from more than a dozen U.S. and Israeli suppliers, including VMware, Palo Alto Networks, and Fortinet, citing national security.²⁸⁹ USTR should seek clarification of the reported restrictions' legal basis, scope, and implementation and address resulting barriers to U.S. suppliers. These cases illustrate 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.

Effective January 1, 2026, China grants qualifying domestic products a 20% price deduction for bid-evaluation purposes when competing with non-domestic products in government procurement.²⁹⁰ Eligibility depends on production in China, with product-specific component and production-process requirements to be phased in. Foreign-invested manufacturers may qualify on equal terms, but imported technology goods face a competitive disadvantage. USTR should seek

²⁸⁶ 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/>

²⁸⁷ 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-technologies-2023-05-21/>

²⁸⁸ Cybersecurity Review Office. (2026, August 6). 关于对派拓公司在华销售产品启动网络安全审查的公告 [Announcement Initiating a Cybersecurity Review of Palo Alto Networks Products Sold in China].

https://www.cac.gov.cn/2026-08/06/c_1787764332950791.htm

²⁸⁹ Reuters. (2026, January 14). *Exclusive: Beijing Tells Chinese Firms to Stop Using US and Israeli Cybersecurity Software, Sources Say*.

<https://www.reuters.com/world/china/beijing-tells-chinese-firms-stop-using-us-israeli-cybersecurity-software-sources-2026-01-14/>

²⁹⁰ General Office of the State Council. (2025, September 28). 国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知 [Notice on Implementing Domestic Product Standards and Related Policies in Government Procurement], 国办发[2025]34号.

https://www.mof.gov.cn/zhengwuxinxi/caizhengxinwen/202509/t20250930_3973725.htm

nondiscriminatory procurement access and monitor whether implementation pressures U.S. suppliers to localize production.

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, and to implementing expedited customs procedures for express shipments.²⁹¹ 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. USTR's 2026 NTE Report identifies an outstanding implementation gap: Colombia had not enabled electronic copies of invoices to replace physical copies, and paper-based customs clearance continued to hamper imports and exports. CCIA urges USTR to continue engagement with Colombia to address this barrier.

Article 32 of pending Bill 004/2026 House proposes repealing, from January 1, 2027, the VAT exclusion in Article 428(j) of the Tax Statute for qualifying postal and express shipments valued at no more than the current threshold of US\$200.²⁹² The proposed repeal would remove VAT relief for qualifying low-value cross-border purchases, including purchases through e-commerce platforms, and could adversely affect U.S. exports to Colombia and the platforms that support them. Tax Reform Bill 004 also proposes an increase to the Significant Economic Presence rate from 3% to 5%, as well as a tax on the gross revenue of non-resident digital suppliers.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Colombia Compra Eficiente's Public Cloud V framework became operational on March 5, 2026, aiming to facilitate the migration of government workloads onto the cloud.²⁹³ This measure does not require internationally recognized security certifications such as FedRAMP or equivalent, allowing Alibaba Cloud and Huawei Cloud to enter the catalog for the first time and compete to host Colombian government workloads. Clause 37 of

²⁹¹ Office of the United States Trade Representative. (2006, November 22). *United States–Colombia Trade Promotion Agreement: Chapter Five—Customs Administration and Trade Facilitation*, Articles 5.3 and 5.7. https://ustr.gov/sites/default/files/uploads/agreements/fta/colombia/asset_upload_file149_10189.pdf

²⁹² Ministerio de Hacienda y Crédito Público. (2026, July 20). *Proyecto de Ley 004 de 2026 Cámara: Por medio de la cual se adopta una reforma tributaria y se dictan otras disposiciones*, Article 32(1). <https://www.pwc.com/co/es/prensa/documentos/2026/julio/Proyecto-de-Ley-000426-26.pdf>

²⁹³ Agencia Nacional de Contratación Pública–Colombia Compra Eficiente. (2026, February 2). *Acuerdo Marco de Precios (AMP/SDA) de Servicios de Nube Pública V*. <https://www.colombiacompra.gov.co/archivos/portfolio-item/acuerdo-marco-de-precios-amp-sda-de-servicios-de-de-nube-publica-v>

Cloud Framework V ("Data and Information Repatriation and Digital Sovereignty") requires buyer entities and providers to assess whether the provider has cloud infrastructure in Colombia. Where this is viable, systems and data must be repatriated to Colombian territory, with the costs chargeable to the buyer entity. Presidential Directive No. 06 of August 13, 2025 permits national executive agencies to procure qualifying innovative solutions directly through the Colombian wholesale connectivity supplier Internexa, when it acts as a public innovation laboratory.²⁹⁴ USTR should monitor implementation to ensure that this channel does not disadvantage U.S. cloud suppliers and that procurement remains transparent and nondiscriminatory, consistent with the United States-Colombia FTA.

These localization concerns are further heightened by legislative developments, specifically Bill 025/2026C on Artificial Intelligence.²⁹⁵ The proposal enshrines technological sovereignty and digital autonomy as a guiding principle in Article 3.11, explicitly calling on the State to prevent asymmetries of dependency on transnational platforms and ensure sovereign control over strategic national information. Although reliance on the state-backed Public Computing Infrastructure or sovereign cloud will not be mandatory, per Article 21, the bill introduces preferential access conditions for AI actors processing Strategic Data of National Interest. When combined with broad discretionary powers to define such data categories, these preferential regimes risk creating de facto localization barriers that distort competition and disadvantage international cloud providers.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

A September 2025 OTT study by the Colombian telecommunications regulator, the CRC, found no technical basis for imposing network-use payments on OTT providers.²⁹⁶ It nevertheless recommended additional information-gathering, examining relationships between content-delivery networks and internet service providers, and reviewing financing through the universal service fund, FUTIC. On July 30, 2026, the CRC adopted Resolution 8303, establishing additional internet-traffic reporting requirements for covered telecommunications operators, including mobile traffic by application, effective January 1, 2027.²⁹⁷ In May 2026, the CRC published a consultation study on unsolicited traffic and digital advertising. While the

²⁹⁴ Presidencia de la República de Colombia. (2025, August 13). *Directiva Presidencial 06 de 2025: Fortalecimiento del Proceso de Compras Públicas de Tecnología e Innovación*.

https://normograma.com/documentospdf/icfes2024/compilacion/docs/directiva_presidencia_0006_2025.htm

²⁹⁵ Cámara de Representantes de Colombia. (2026, septiembre). Informe de ponencia para primer debate al Proyecto de Ley No. 025 de 2026 Cámara: Por medio de la cual se regula la inteligencia artificial en Colombia para garantizar su desarrollo ético y responsable y se dictan otras disposiciones, Comisión Sexta Constitucional Permanente.

²⁹⁶ Comisión de Regulación de Comunicaciones (CRC). (2025, September). *Estudio sobre el rol de los servicios «Over the Top» OTT en Colombia–2024*.

<https://www.crcom.gov.co/es/biblioteca-virtual/estudio-sobre-rol-servicios-over-top-ott-en-colombia-2024>

²⁹⁷ Comisión de Regulación de Comunicaciones (CRC). (2026, July 30). *Resolución No. 8303 de 2026*, Articles 1 and 3. <https://www.crcom.gov.co/sites/default/files/normatividad/00008303.pdf>

CRC acknowledged its lack of authority to regulate or directly demand data from OTTs, it examines how these loads consume network resources.²⁹⁸ Increased scrutiny by the CRC on OTTs and their bandwidth consumption risks reopening arguments for network usage fees. USTR should monitor subsequent measures for discriminatory charges or disproportionate obligations affecting U.S. digital services.

Colombia's Decree 769/2026 implements the Safe Digital Environments Law (Law 2489 of 2025) and requires digital platforms, services, and software providers to mitigate online risks to children, including content-reporting and removal mechanisms, risk assessments, transparency, parental controls, age verification, and privacy- and security-by-design requirements.²⁹⁹ The decree left important implementation details to subsequent technical guidelines, creating uncertainty around platforms' content-moderation and risk-management obligations, with potential implications for freedom of expression and privacy. USTR should continue to monitor this issue under the incoming administration, including whether it repeals Decree 769 or introduces substantive changes to provide greater regulatory clarity and ensure that implementation does not result in intrusive platform regulation or restrictions on freedom of expression.

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.³⁰⁰ Revision to the legislation in 2018 that sought to implement the U.S.-Colombia FTA copyright chapter includes no language on online intermediaries.³⁰¹ 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. Colombia provides a limited quotation exception, but lacks a broad, express text-and-data-mining exception, leaving uncertainty for computational analysis and other non-expressive uses of publicly available data.

²⁹⁸ Comisión de Regulación de Comunicaciones [Communications Regulation Commission, Colombia]. (2026, May). Monetización en la industria de contenidos, tráfico y contenido no solicitado — Resumen [Monetization in the content industry, traffic and unsolicited content — Summary], Doc. 11000-41-3-1. <https://www.crcom.gov.co/sites/default/files/weberc/noticias/documents/ESTUDIO-MONETIZACION-INDUSTRIA-CONTENIDOS-TRAFICO-CONTENIDO-NO-SOLICITADO-130526.pdf>.

²⁹⁹ Government of Colombia. (2026). *Decreto 769*. <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=193750>.

³⁰⁰ Office of the United States Trade Representative. (2006, November 22). *United States–Colombia Trade Promotion Agreement*, Article 16.11, paragraph 29.

<https://ustr.gov/trade-agreements/free-trade-agreements/colombia-fta/final-text>

³⁰¹ Herrera, J. R. (2018, September 5). *The Recent and Relevant Copyright Bill in Colombia (Law 1915-2018)*. Kluwer Copyright Blog.

<https://legalblogs.wolterskluwer.com/copyright-blog/the-recent-and-relevant-copyright-bill-in-colombia-law-1915-2018/>

PL 083/2026, a bill proposed in Colombia's Congress in July 2026, would require biometric or equivalent identity verification of users, impose duties on platforms to prevent and mitigate allegedly defamatory content, mandate warning labels, and require court-ordered retractions to receive equivalent distribution. These requirements could compel intrusive identity collection and require platforms to make preliminary determinations about the legality of user speech. USTR should urge Colombia to preserve judicial responsibility for defamation determinations and avoid imposing general monitoring or universal identification requirements on digital services.

PL 083/2026 regulates social media companies, requiring identity verification for all users, and adds transparency duties focused on content removal. The proposed law could also block digital platforms in Colombia that fail to comply with its measures. PL Estatutaria 208/2026 would ban users under 14 years old from social media accounts and require age verification proportional to risk. The draft law would also ban targeted advertising for users under the age of 18.

Taxation of Digital Products and Services

Law 2277 of December 13, 2022 established Colombia's significant economic presence (SEP) regime, effective January 1, 2024.³⁰² It covers qualifying nonresident suppliers of goods and specified digital services, including cloud services, who engage in "deliberate and systematic" interaction with the Colombian market and meet certain revenue thresholds (covered gross revenue of at least 31,300 UVT, or about \$500,000). Deliberate and systematic interaction is presumed where the supplier interacts with at least 300,000 Colombian customers or users, or permits prices to be displayed or payments to be made in Colombian pesos.

The rule institutes a 10% withholding tax on revenues of a non-resident with an entity determined to be an SEP in Colombia, even if it does not qualify as a permanent establishment under traditional international tax principles. 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. Although this tax is not exclusive to digital services, it shares many aspects with DSTs and for digital services has a similar effect and raises similar concerns. Eligible nonresidents may register with DIAN and elect to file an annual return at 3% of covered gross revenue, requesting that the 10% withholding mechanism not apply. DIAN provides remote registration and filing procedures; this election does not require establishing a Colombian entity or permanent establishment. Like DSTs, Colombia's SEP regime represents a unilateral gross-revenue tax. U.S. suppliers may face double taxation where Colombian SEP payments cannot be fully credited against U.S. tax on the same income, an outcome exacerbated by the lack of a tax treaty between the two countries. CCIA urges USTR and Treasury to address the SEP regime's compliance costs, potential double taxation, and

³⁰² Congreso de Colombia. (2022, December 13). *Ley 2277 de 2022*, Article 57 (adding Article 20-3 to the Tax Statute, including paragraph 8 on entry into force). https://normograma.dian.gov.co/dian/compilacion/docs/ley_2277_2022.htm

differing tax treatment of resident and nonresident suppliers. In addition, USTR should examine the measure's treatment of U.S. suppliers under applicable trade commitments, taking account of the USCTPA's specific rules and exceptions for taxation measures.³⁰³

Bill 004/2026 House, introduced on July 20, 2026, again proposes increasing the elective SEP tax from 3% to 5% of covered gross revenue under Article 29.³⁰⁴ Article 32 would also repeal the VAT exclusion for cloud computing, hosting, and webpage provision from January 1, 2027. Similarly, Bill 031/2025 House further expands unilateral taxation on digital commerce. Article 23 increases the elective SEP rate from 3% to 6% on gross revenue for digital advertising provided by social media platforms.³⁰⁵ If adopted, they would increase tax costs for affected foreign digital-service suppliers and cloud customers.

Côte d'Ivoire

Taxation of Digital Products and Services

Côte d'Ivoire's 2026 Fiscal Annex enacted a Significant Economic Presence (SEP) tax regime targeting non-resident digital platforms. Under the framework, foreign digital companies generating more than 50 million CFA francs in local gross revenue are subject to a 30% corporate income tax assessed on a deemed local profit margin of 10% of gross revenues. This unilateral revenue tax explicitly targets foreign digital service exporters and creates severe double-taxation risks. CCIA urges USTR to request that Côte d'Ivoire withdraw its unilateral SEP tax in favor of multilateral consensus approaches to international taxation.

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.

³⁰³ USCTPA Article 22.3 governs the agreement's application to taxation measures. SEP tax registration is available to nonresidents through DIAN and does not itself require a Colombian establishment.

³⁰⁴ Ministerio de Hacienda y Crédito Público. (2026, July 20). *Proyecto de Ley 004 de 2026 Cámara: Por medio de la cual se adopta una reforma tributaria y se dictan otras disposiciones*, Article 29. <https://www.pwc.com/co/es/prensa/documentos/2026/julio/Proyecto-de-Ley-000426-26.pdf>

³⁰⁵ Cámara de Representantes de Colombia. (2025, November 25). Informe de ponencia positiva para segundo debate al Proyecto de Ley 031 de 2025 Cámara: Por medio de la cual se adoptan medidas para la transparencia, normalización y fortalecimiento del sistema tributario, aduanero, cambiario y fiscal, para la reactivación económica, y se dictan otras disposiciones, Gaceta del Congreso No. 2245, Articles 23 & 36. http://www.secretariassenado.gov.co/senado/basedoc/gaceta/2025/gaceta_2245_2025.pdf

Croatia's State Information Infrastructure Act, effective May 1, 2025,³⁰⁶ requires specified records containing personal data to be stored in data centers in Croatia. Records of non-personal data may be stored in Croatia or another EU Member State, subject to prescribed conditions, including public-security restrictions that may require storage in Croatia. These requirements restrict cross-border hosting opportunities for U.S. cloud suppliers.

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), an entity wholly owned by the Republic of Croatia, has served as a major IT services provider for public sector bodies,³⁰⁷ 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.³⁰⁸ Article 17 of the State Information Infrastructure Act requires state administration bodies, other state bodies, and public institutions founded solely by the Republic of Croatia to use CDU hosting services. Article 7 permits government-approved exemptions from parts of the state infrastructure for organizational, technological, or security reasons. This framework can constrain opportunities for independent commercial cloud providers. CCIA urges USTR to examine whether these localization and procurement practices unduly restrict U.S. suppliers' access. Croatia's May 2026 procurement amendments retain Article 84's prohibition on less favorable treatment of suppliers, goods, and services covered by the EU's WTO Government Procurement Agreement commitments or other binding international procurement agreements.³⁰⁹ USTR should assess discriminatory tender conditions against those obligations where applicable.

Other Barriers to Digital Trade

Croatia's Foreign Investment Screening Act (NN 136/2025), effective November 13, 2025, introduced mandatory prior approval for covered investments by non-EU/EEA investors, including U.S. investors, in designated Croatian entities.³¹⁰ Covered sectors include cloud computing, data centers, content delivery networks, and managed IT services. Approval requirements cover acquisitions of qualifying holdings of at least 10 percent, increases or

³⁰⁶ Croatian Parliament. (2025, April 23). *Zakon o državnoj informacijskoj infrastrukturi* [State Information Infrastructure Act], NN 72/2025, Article 38. https://narodne-novine.nn.hr/clanci/sluzbeni/2025_04_72_934.html

³⁰⁷ Oldag, J. (2018, January 30). *New Euritas member: APIS IT*. Euritas. <https://www.euritas.eu/2018/01/30/apis-it-our-new-member-from-croatia/>

³⁰⁸ Oldag, J. (2019, December 4). *APIS IT marked 55 years of operation with opening of Shared Services Centre for Croatian public administration*. Euritas. <https://www.euritas.eu/2019/12/04/apis-it-marked-55-years-of-operation-with-opening-of-shared-services-centre-for-croatian-public-administration/>

³⁰⁹ Croatian Parliament. (2026, May 8). *Zakon o izmjenama i dopunama Zakona o javnoj nabavi* [Act Amending the Public Procurement Act], NN 48/2026, Article 16 (replacing Article 84). https://narodne-novine.nn.hr/clanci/sluzbeni/2026_05_48_584.html

³¹⁰ Croatian Parliament. (2025, November 5). *Zakon o provjeri stranih ulaganja* [Foreign Investment Screening Act], NN 136/2025, Articles 6, 10–12 and 32. https://narodne-novine.nn.hr/clanci/sluzbeni/2025_11_136_2010.html

decreases in qualifying holdings, and acquisitions of control. Covered transactions cannot be completed before approval. Application rules (NN 68/2026) became effective June 27, 2026.³¹¹ The statutory decision period is generally 120 days after submission of a complete application, extending to 150 days in specified cases. The list of designated entities is not public. CCIA urges USTR to monitor implementation, particularly the transparency of designation and the effect of approval timelines on U.S. investment in digital infrastructure.

Cuba

Government Imposed Restrictions on Internet Content and Related Access Barriers

The Cuban government has a persistent record of disrupting access or blocking Internet services to stifle political dissent and organization.³¹² Government ownership and control of Empresa de Telecomunicaciones de Cuba S.A. (ETECSA), the state telecommunications monopoly, facilitates such restrictions. During the July 2021 protests, access to Facebook, WhatsApp, Instagram, and Telegram was disrupted.³¹³

Cuba's Social Communication Law (Law 162/2023), effective October 4, 2024, further restricts online content.³¹⁴ Articles 13 and 51 prohibit digital content intended to subvert the constitutional order or destabilize the socialist state. Article 54 requires telecommunications and hosting providers to participate in monitoring compliance, notify those responsible of violations for removal, and implement applicable measures. These provisions create broad grounds for censorship and impose enforcement responsibilities on service providers.

Targeted connectivity restrictions continued in 2026, limiting access to digital services and independent reporting.³¹⁵ The Cuban Institute for Freedom of Expression and Press (ICLEP) reported that seven content creators experienced simultaneous internet and mobile telephone cutoffs on May 16 after their meeting with the U.S. Embassy.³¹⁶ ICLEP also documented a

³¹¹ Croatian Ministry of Finance. (2026, June 26). *Pravilnik o sadržaju zahtjeva za odobrenje stranog ulaganja* [Rules on the Content of Applications for Approval of Foreign Investments], NN 68/2026, Article 10. https://narodne-novine.nn.hr/clanci/sluzbeni/2026_06_68_821.html

³¹² 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/>

³¹³ 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/>

³¹⁴ National Assembly of People's Power of Cuba. (2024, June 5). *Ley 162/2023 "De Comunicación Social"* [Social Communication Law], Gaceta Oficial No. 48, Articles 13 and 51 and Ninth Final Provision. https://www.gacetaoficial.gob.cu/sites/default/files/goc-2024-o48_0.pdf

³¹⁵ Instituto Cubano por la Libertad de Expresión y Prensa (ICLEP). (2026, June 10). *Cuba en mayo de 2026: la cárcel se vuelve epicentro de la represión*. <https://iclep.org/post/cuba-en-mayo-de-2026-la-carcel-se-vuelve-epicentro-de-la-represioninforme-mayo-2026/>

³¹⁶ Instituto Cubano por la Libertad de Expresión y Prensa (ICLEP). (2026, May 19). *Corte masivo y coordinado de servicios de internet y telefonía contra creadores de contenido tras encuentro con Mike Hammer*. <https://iclep.org/post/corte-de-servicios-de-internet-y-telefonía-contra-creadores-de-contenido-tras-encuentro-con-mike-hammer/>

daylong mobile-data cutoff affecting three journalists from El Espirituano on May 20, which it characterized as retaliation for their reporting.³¹⁷

Cuba also restricts access to alternative internet infrastructure. Ministry of Communications Resolution 1/2026, published on May 21, 2026, excludes terminals using non-geostationary satellites for public personal telecommunications services from its technical-authorization route where the service provider lacks an agreement with the Cuban government.³¹⁸ It also prohibits importing equipment used to access computer or telecommunications networks without authorization. These restrictions impede access to satellite-internet services offered independently of the state telecommunications network.

Cyprus

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In March 2026, Cyprus adopted its National Cloud Policy, establishing standards for government cloud hosting, security, and procurement.³¹⁹ The policy requires providers to support data hosting in Cyprus or EU jurisdictions that comply with data-protection requirements, and gives preference to providers offering local or region-specific hosting options. Cyprus also completed construction of two government data centers in November 2025. USTR should examine whether implementation of the policy's hosting and procurement requirements unnecessarily restricts cross-border cloud services or disadvantages U.S. suppliers. To the extent such measures extend to the private market, USTR should investigate their consistency with Cyprus's applicable GATS commitments, including those covering cross-border data-processing and database services.

³¹⁷ Instituto Cubano por la Libertad de Expresión y Prensa (ICLEP). (2026, May 21). *OCLE denuncia corte selectivo de internet contra periodistas de El Espirituano durante el 20 de mayo en Sancti Spiritus*.

<https://iclep.org/post/oclep-denuncia-corte-selectivo-de-internet-contra-periodistas-de-el-espirituano-durante-el-20-de-mayo-en-sancti-spiritus/>

³¹⁸ Cuban Ministry of Communications. (2026, May 21). *Resolución 1/2026*, Gaceta Oficial No. 66 Extraordinaria, Section Four, paragraph (d)(iv). <https://www.gacetaoficial.gob.cu/sites/default/files/goc-2026-ex66.pdf>

³¹⁹ European Commission. (n.d.). *New cloud policy with regard to government IT systems and services and infrastructure set-up—Two data centres with hosting services*. https://reforms-investments.ec.europa.eu/projects/new-cloud-policy-regard-government-it-systems-and-services-and-infrastructure-set-two-data-centres_en.

Czech Republic

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Czech Republic's Cybersecurity Act, No. 264/2025, implementing the EU NIS 2 Directive, took effect on November 1, 2025.³²⁰ Decree No. 411/2025³²¹ and NÚKIB's July 2026 guidance³²² address public cloud procurement, classifying public administration information systems into four security levels according to potential impacts. Under Decree No. 505/2025³²³ effective January 1, 2026, high-security cloud services generally must store customer data and specified operational data at rest within the EU or EFTA, subject to published exceptions. Critical-security services face Czech-territory processing requirements, with limited exceptions. NÚKIB's 2026 exception lists include major U.S. suppliers.³²⁴ USTR should ensure that U.S. suppliers continue to benefit from appropriate flexibility, based on proportionate, transparent requirements that avoid unnecessary restrictions on U.S. cloud suppliers.

Government-Imposed Content Restrictions and Related Access Barriers

The Czech Republic's implementation of the EU Copyright Directive (EUCD) went into effect in January 2023.³²⁵ Section 87b of the Copyright Act imposes press-publisher licensing and remuneration obligations, including restrictions on certain service changes by providers deemed "dominant."³²⁶ If remuneration negotiations remain unresolved after 60 days, either party may ask the Ministry of Culture to determine payment using statutory criteria, subject to judicial review. Both parties must supply information necessary for that determination. These obligations create commercial and compliance concerns for U.S. search and social media services, and implicate TRIPS limitations and exceptions (e.g., with respect to quotation). Specified violations carry fines up to the greater of CZK 500,000 or 1% of the offender's worldwide annual turnover for the preceding financial year. In December 2022, Google announced that it would remove

³²⁰ Parliament of the Czech Republic. (2025, June 11). *Zákon č. 264/2025 Sb., o kybernetické bezpečnosti*, §§ 1(3) and 73. <https://e-sbirka.gov.cz/sb/2025/264>.

³²¹ Národní úřad pro kybernetickou a informační bezpečnost. (2025, September 26). *Vyhláška č. 411/2025 Sb., o bezpečnostních úrovních informačních systémů veřejné správy*, §§ 3–4. <https://www.zakonyprolidi.cz/cs/2025-411>.

³²² Národní úřad pro kybernetickou a informační bezpečnost. (2026, July 23). *Průvodce zařazením do bezpečnostní úrovně* (Version 1.0). https://nukib.gov.cz/download/publikace/podpurne_materialy/2026-07-23_Pruvodce-zarazenm-do-bezpecnostni-urovne_v1.pdf.

³²³ Národní úřad pro kybernetickou a informační bezpečnost. (2025, November 28). *Vyhláška č. 505/2025 Sb., o některých požadavcích pro zápis do katalogu cloud computingu*, §§ 11–12 (repeal and effective date). <https://e-sbirka.gov.cz/sb/2025/505>.

³²⁴ Národní úřad pro kybernetickou a informační bezpečnost. (n.d.). *Cloud computing – výjimky z uložení dat*. <https://nukib.gov.cz/cs/uredni-deska/cloud-computing/>.

³²⁵ Bird & Bird. (n.d.). *Czechia*. <https://www.twobirds.com/en/trending-topics/copyright-directive/copyright-directive-countries/czech-republic>

³²⁶ Parliament of the Czech Republic. (2000, April 7). *Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)*, as amended, § 87b(3), (9), and (14)–(15). <https://mze.gov.cz/public/portal/mze/legislativa/vap49278-33612>

protected press-content previews and discontinue News Showcase in Czechia in response to the legislation.³²⁷

Discriminatory Local Content Quotas and Audiovisual Service Mandates

Amendments to the Audiovisual Act effective January 1, 2025 extended audiovisual contribution obligations to foreign on-demand audiovisual service providers targeting Czech viewers.³²⁸ Covered providers must contribute 3.5% of relevant Czech-market revenues to the State Audiovisual Fund or qualifying direct investment. Eligible investments can reduce the payment to the Fund to a minimum of 1%; exemptions include low-turnover and low-audience services. In July 2026, the Fund confirmed collection under the expanded regime and instituted noncompliance proceedings against four foreign providers.³²⁹ The levy and investment conditions constitute a burdensome and discriminatory measure against U.S. suppliers.

Democratic Republic of the Congo

Taxation of Digital Products and Services

On July 20, 2026, Inter-Ministerial Decree No. 015/2026, establishing an extraterritorial authorization fee and tax framework targeting foreign digital service providers operating "from or to" the DRC. The decree establishes five separate service categories—including social networking, content delivery networks (CDNs), marketplaces, and web hosting—and requires non-resident suppliers deemed to hold a "dominant position" to pay cumulative annual authorization fees totaling up to \$68,000 USD per year, alongside non-compliance penalties ranging from 25% to 200% of fees owed.³³⁰

By assessing flat charges on gross global or service revenues without regard to local profitability or physical establishment, this measure operates as a unilateral, discriminatory digital trade barrier that conflicts with international tax consensus under the OECD/G20 Inclusive Framework

³²⁷ Connal, S. (2022, December 12). *Updates to Google's Services in Czechia in Light of the Czech Transposition of the European Copyright Directive*. Google Search Central Blog.

<https://developers.google.com/search/blog/2022/12/google-services-in-czechia>

³²⁸ Parliament of the Czech Republic. (2024, December 11). *Zákon č. 480/2024 Sb., kterým se mění zákon č. 496/2012 Sb., o audiovizuálních dílech a podpoře kinematografie a o změně některých zákonů (zákon o audiovizu), ve znění pozdějších předpisů, a další související zákony*, Article I, point 141, and Article V.

<https://e-sbirka.gov.cz/sb/2024/480>

³²⁹ Státní fond audiovize. (2026, July 22). *Státní fond audiovize: Nový systém audiovizuálních poplatků přinesl fondu vyšší příjmy, výsledkem je vyšší podpora pro příští rok*.

<https://sfa.gov.cz/data/article/2026/07/TZ-SFA-vyssi-poplatky-a-podpora-pro-pristi-rok.pdf>

³³⁰ Zogo, W. (2026, August 3). RDC : Le Ministère de l'économie numérique fixe les taxes et redevances dues pour les services numériques, les fintechs, les datacenters et les plateformes [DRC: The Ministry of the Digital Economy sets the duties and fees owed for digital services, fintechs, data centers and platforms]. Droit Médias Finance. <https://www.droitmediasfinance.com/index.php/actualites/droit-tech-fintech/1348-rdc-le-ministere-de-leconomie-numerique-fixe-les-taxes-et-redevances-dus-pour-les-services-numeriques-les-fintechs-et-les-plateformes>.

on Pillar One. Although enforcement was temporarily paused in August 2026 for public consultations, the underlying decree remains active law. CCIA urges USTR to press the DRC government to rescind Decree No. 015/2026 and refrain from imposing unilateral revenue levies on U.S. digital exporters.

Denmark

Taxation of Digital Products and Services/Local Content Quotas and Audiovisual Mandates

Effective 2025, Denmark imposes a 2% turnover tax on non-resident providers of streaming TV and films, rising to 5% if the provider invests less than 5% of its Danish revenues in Danish-language content.³³¹

Government-Imposed Content Restrictions and Related Access Barriers

In 2026, the Government of Denmark proposed a draft bill establishing a national minimum age limit of 15 years for children and young people to access certain digital services.³³² While introduced under the guise of enhancing the online protection of minors, the proposed scope and design of the regulation present significant trade concerns for U.S. digital service providers.

Specifically, the draft framework proposes scoping its primary regulatory obligations and access restrictions based on platform size, closely aligning with the "Very Large Online Platform" (VLOP) designations established under the European Union's Digital Services Act (DSA). Because the VLOP designation and associated user-threshold metrics are met almost exclusively by large, global companies, the regulation would disproportionately target and burden U.S.-based providers. Conversely, smaller platforms—including those of domestic Danish or local European origin—would be largely exempted from these stringent requirements, despite often hosting identical features such as direct messaging, unassisted live-streaming, or open algorithmic feeds. This size-based scoping mechanism effectively creates a discriminatory regulatory environment that advantages local commercial services over their U.S. competitors.

The Government of Denmark has proposed a draft bill to establish a national "Media Ombudsman" with broad, ill-defined administrative powers over online content creators.³³³ While the declared objective of the bill is to promote fairness in the digital media landscape, the

³³¹ Nordisk Film and TV. (2025). *New Danish Cultural Levy is Up and Running*.

<https://nordiskfilmogtvfond.com/news/stories/new-danish-cultural-levy-is-up-and-running>

³³² Jurcenoks, E., Korsgaard, R. L., & Hansen, K. (2026, September 10). New draft bill on social media age limits in Denmark. Plesner. <https://plesner.com/en/news/new-draft-bill-social-media-age-limits-denmark>.

³³³ Kulturministeriet [Danish Ministry of Culture]. (2026, September 2). Høring over forslag til lov om medieombudsmanden [Consultation on the draft Act on the Media Ombudsman]. Høringsportalen. <https://hoeringsportalen.dk/Hearing/Details/71429>.

proposed framework introduces highly disproportionate liabilities, severe criminal penalties, and institutional overreach that disproportionately burden independent creators and U.S. digital platforms. The proposed bill, specifically under Sections 15 and 16, would empower the Media Ombudsman to initiate civil and criminal proceedings against hosting services, layering additional liability on top of the EU Digital Services Act. By creating a highly restrictive environment for digital expression, the bill threatens to stifle the local digital economy, disrupt the harmonized framework for online services, and serve as a significant barrier to digital trade.

Challenges to the Development of Artificial Intelligence

In September 2025 Denmark's Expert Group on Copyright and Artificial Intelligence published a proposal focusing on text and data mining exceptions for the training of Artificial Intelligence models.³³⁴ The Expert Group's Recommendation 2 advocates restricting the harmonized TDM exceptions established under Article 4 of the EU's Digital Single Market (DSM) Directive by replacing the current standard "opt-out" regime—which allows rights holders to opt out of automated scraping in a machine-readable format—with a restrictive "opt-in" model requiring explicit, prior consent for any TDM activities. The Expert Group has also recommended mandatory arbitration, specifically, a "final offer" mandatory arbitration pilot scheme, initially targeting press publications. Under this model, U.S. digital services would be legally compelled to participate in licensing negotiations with local publishers. If negotiations fail, both parties would be forced to submit final offers to an independent arbitration body, which would issue a binding decision. Such mandatory frameworks bypass market-based negotiations and deny foreign platforms the basic commercial freedom to decline licensing agreements.³³⁵ Given the recent clarification of the U.S. position with respect to text and data mining, USTR should oppose any such proposal.

Other Digital Trade Barriers

In October 2026, the Danish Ministry of Culture formally introduced L 49, a bill amending the Danish Copyright Act to establish new national rights protecting performing artists and

³³⁴ Bechbruun. (2025). *New report from the Expert Group on Copyright and AI*. <https://bechbruun.com/insights/news-and-cases/new-report-from-the-expert-group-on-copyright-and-artificial-intelligence-ai/>

³³⁵ Danish Ministry of Culture. (2025), *Recommendations of Expert Group on Copyright and Artificial Intelligence*. https://kum.dk/fileadmin/_kum/1_Nyheder_og_presse/2025/Rapport_Ekspertgruppe_for_ophavsret_og_kunstig_intelligens.pdf.

individuals against "realistic, digitally generated imitations" (deepfakes).³³⁶ Denmark's decision to integrate these new personality and likeness rights directly into the Copyright Act (specifically under Section 65a) creates an unclear hybrid of traditional copyright law and personality/performance rights. This conflation raises several critical concerns and unresolved legal questions.

While the bill contains exemptions intended to safeguard lawful speech—such as caricature, parody, satire, pastiche, and social critique—these concepts are vague and highly dependent on subjective, case-by-case interpretations. Crucially, the bill introduces an "exemption to the exemption" (specifically in Section 73 a, subsection 2), where satirical or parodic content can still be deemed infringing if it is classified as "misinformation" that poses a serious risk to certain public or private interests. This highly complex, layered test is difficult for digital hosting platforms to assess in practice. Without robust procedural safeguards, this framework is highly vulnerable to bad-faith, abusive removal requests by political or other actors seeking to suppress legitimate, critical speech and satire.

Dominican Republic

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

In 2026, the Dominican Republic proposed a draft new General Law on Telecommunications, Digital Infrastructure and Connectivity that would extend legacy telecommunications obligations to cloud computing, data centers, content delivery networks, and other information services through an undefined concept of "functional linkage."³³⁷ Because the "functional linkage" trigger sets no threshold of control, indispensability, or territorial impact, the regulated perimeter is undefined, potentially sweeping in facilities and providers that perform no telecommunications function. (Arts. 1–3, 4.1, 5). These obligations are technically unworkable under the cloud shared-responsibility model, in which providers secure the infrastructure of the cloud while customers control security and cloud providers have no visibility into customer workloads. The resulting uncertainty would deter investment and slow digital adoption. The Dominican Republic should confine the new law to the conveyance of signals over public networks and the scarce resources that support them, and add an explicit, unconditional exclusion for computing, storage, hosting, database, analytics, artificial-intelligence, content-delivery, and managed-DNS services

³³⁶ Kulturministeriet [Danish Ministry of Culture]. (2026, October 8). Kulturminister vil dæmme op for delinger af digitale efterligninger fra årsskiftet [Culture Minister seeks to curb sharing of digital imitations from the turn of the year].

<https://kum.dk/aktuelt/nyheder/kulturminister-vil-daemme-op-for-delinger-af-digitale-efterligninger-fra-aarsskiftet>; Ekspertgruppe om ophavsret og kunstig intelligens [Expert Group on Copyright and Artificial Intelligence]. (2025, September). Ekspertgruppe om ophavsret og kunstig intelligens, Recommendation 4. Kulturministeriet [Danish Ministry of Culture].

https://kum.dk/fileadmin/_kum/1_Nyheder_og_presse/2025/Rapport_Ekspertgruppe_for_ophavsret_og_kunstig_intelligens.pdf.

³³⁷ INDOTEL. (2026). Borrador Anteproyecto de Ley Telecomunicaciones.

<https://indotel.gob.do/wp-content/uploads/2026/09/Borrador-Anteproyecto-de-Ley-Telecomunicaciones.pdf>

as information services outside its scope. Failure to do so could be viewed as inconsistent with the deregulatory provisions of the CAFTA-DR FTA (Article 13.6).

Ecuador

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Ecuador requires public sector entities to procure cloud computing services through government-owned telecommunications companies, principally the National Telecommunications Corporation (CNT), rather than contracting directly with cloud service providers.³³⁸ The requirement derives from Ministerial Agreement No. 141 (MINTEL, 2011), which was expanded in 2019 to cover cloud and other digital services for all public entities; after a brief exclusion of cloud services in 2023, MINTEL reinstated the mandate. Although forced data localization was eliminated through the Fintech Law reform of the Ingenios Code, allowing government data to be stored outside Ecuador, the obligation to contract cloud through CNT when serving the State remains in force. The mandatory intermediary increases costs, slows service delivery, and creates anti-competitive effects, since all U.S. providers must route sales through the same state-owned entity. Ecuador should allow public entities to procure cloud directly from qualified providers on a technology-neutral basis, through a transparent framework that does not mandate intermediation by state-owned telecommunications companies.

Challenges to the Development of Artificial Intelligence

On February 12, 2026, Ecuador's Data Protection Authority (SPDP) issued Resolution No. SPDP-SPD-2026-0009-R governing personal data protection in AI systems, including systems located abroad, effective March 10, 2026.³³⁹ Requirements include transparency, risk management, impact assessments under applicable data-protection rules, processing records, and risk-based audits. The SPDP may audit systems and impose corrective measures. On September 9, 2026, the SPDP issued Resolution No. SPDP-SPD-2026-0037-R amending this framework.³⁴⁰ The amendment limits processors' obligations to processing operations over which they have access, visibility, or effective control (*i.e.*, excluding third-party cloud suppliers), while requiring evidence when they claim these conditions are absent. Processors providing, developing, or maintaining AI systems must supply controllers with information necessary for compliance

³³⁸ Ministerio de Telecomunicaciones y Sociedad de la Información (2023, August 23). Acuerdo Ministerial MINTEL Nro. 0017 del 2023.

³³⁹ Superintendencia de Protección de Datos Personales. (2026, March 10). *Resolución No. SPDP-SPD-2026-0009-R: Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial*. Registro Oficial No. 240. https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJYXJwZXRhIjoicm8iLCJldWlkIjozMzA4MzdiZGEtZTdiOS00N2O4LTllY2MtZmIzYjBhYmZkYzOyLnBkZiJ9

³⁴⁰ Superintendencia de Protección de Datos Personales. (2026, September 9). *Resolución No. SPDP-SPD-2026-0037-R*. <https://spdp.gob.ec/wp-content/uploads/2026/09/SPDP-SPD-2026-0037-R.pdf>

concerning system operation, limitations, foreseeable risks, and controls, without disclosing their commercial or industrial secrets or intellectual property. CCIA urges USTR to ensure proportionate implementation, clear guidance on consumer rights relating to automated-decision making, and safeguards for confidential business information to avoid unnecessary burdens on U.S. suppliers.

Currently, there is an AI Governance bill being discussed in the Education Commission of the National Assembly that poses several risks for U.S. companies.³⁴¹ The bill imposes restrictions on AI training, including requirements to seek rightsholders' permission to train on copyrighted works via a license or other exception. The draft bill also imposes obligations on companies to publish training source summaries, create due diligence standards and algorithm transparency, and furnishes Criminal Code amendments to outlaw the use of generative AI to create unauthorized synthetic media, deepfakes, or impersonations. Finally, the draft bill delegates regulatory powers to the data protection authority whose oversight to date has been a challenge for foreign technology companies. USTR should recommend this bill be dismissed due to its overly-onerous requirements for companies.

Restrictions on Cross-Border Data Flows

On January 28, 2026, the SPDP issued Resolution No. SPDP-SPD-2026-0004-R establishing procedures for domestic and international personal-data transfers.³⁴² This measure recognizes the Ibero-American Data Protection Network's controller-to-controller model clauses, but requires transfer safeguards to include the recipient's express submission to Ecuadorian jurisdiction and applicable SPDP and judicial decisions—a condition U.S.-based suppliers may deem an unacceptable legal risk. CCIA urges USTR to seek interoperable transfer mechanisms and proportionate requirements that facilitate cross-border services.

The United States and Ecuador signed an Agreement on Reciprocal Trade on March 13, 2026.³⁴³ Its digital provisions address discriminatory digital services taxes and treatment of U.S. digital services, cross-border data flows, compelled technology transfer, and customs duties on

³⁴¹ Asamblea Nacional del Ecuador. (2026, September 1). Proyecto de Ley Orgánica para el desarrollo, uso ético y gobernanza de la inteligencia artificial en el Ecuador. [https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-19130/3030.%20Proyecto%20de%20Ley%20Org%C3%A1nica%20para%20el%20desarrollo.%20uso%20%C3%A9tico%20y%20gobernanza%20de%20la%20inteligencia%20artificial%20en%20el%20Ecuador%20\(As.%20Cecilia%20Baltazar%20-%2020485405\)/485405-baltazar.pdf](https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-19130/3030.%20Proyecto%20de%20Ley%20Org%C3%A1nica%20para%20el%20desarrollo.%20uso%20%C3%A9tico%20y%20gobernanza%20de%20la%20inteligencia%20artificial%20en%20el%20Ecuador%20(As.%20Cecilia%20Baltazar%20-%2020485405)/485405-baltazar.pdf)

³⁴² Superintendencia de Protección de Datos Personales. (2026, January 28). *Resolución No. SPDP-SPD-2026-0004-R: Norma General de Transferencias o Comunicaciones Nacionales e Internacionales de Datos Personales*. <https://spdp.gob.ec/wp-content/uploads/2026/01/04.01.01-SPSP-SPD-2026-0004-R-Norma-general-de-transferencias-signed.pdf>

³⁴³ Office of the United States Trade Representative. (2026, March 13). *Ambassador Greer Signs the United States-Ecuador Agreement on Reciprocal Trade*. <https://ustr.gov/about/policy-offices/press-office/press-releases/2026/march/ambassador-greer-signs-united-states-ecuador-agreement-reciprocal-trade>

electronic transmissions. Annex III, Article 3.1 provides that Ecuador shall endeavor to recognize U.S. data-protection adequacy by December 31, 2026 and recognize international certification mechanisms such as Global CBPR and PRP. CCIA urges USTR to prioritize implementation of these commitments and monitor whether Ecuador's data-transfer requirements impede U.S. suppliers.

Other Barriers to Digital Trade

On September 9, 2026, Ecuador's privacy regulator, the SPDP, issued Resolution No. SPDP-SPD-2026-0039-R regulating biometric-data processing.³⁴⁴ It requires impact assessments before implementing biometric systems, with updates every twelve months and when processing risks change. Consent-based processing generally requires an equivalent non-biometric alternative, subject to a documented technical-impossibility exception. CCIA urges USTR to monitor implementation and seek proportionate requirements that accommodate legitimate authentication and fraud-prevention services.

Relatedly, the SPDP opened a consultation in September 2026 on a draft health-data resolution³⁴⁵ that would create a standalone "neural data" and "neurorights" regime by administrative regulation rather than legislation. The ten-title instrument reaches well beyond clinical settings—covering consumer wearables, health applications, connected sensors, digital assistants, telemedicine, and every international health-data transfer—with a one-year compliance period from publication. It defines a "connected health device" as any equipment, sensor, or embedded system that handles health data and communicates with another system, and defines neural data to include inferred and behavioral signals without distinguishing central from peripheral nervous system activity, capturing gesture-based input and ordinary wearables by definition. Neither "neurorights" nor "neural data" appears in Ecuador's Organic Law on Personal Data Protection, which already treats physical and mental health data as sensitive irrespective of source. Three features sit uneasily with the ART: SPDP pre-approval of proprietary technical protocols as a condition of processing, cuts against the prohibition on requiring access to technology, source code, or other proprietary knowledge as a condition of doing business; a mandatory impact assessment for every international health-data transfer, with no risk threshold, cuts against cross-border data-flow commitments; and restrictions on advertising and secondary use of broadly defined health-related data raise non-discrimination concerns for U.S. digital services. CCIA urges USTR to encourage Ecuador to apply its existing data-protection law rather than build a parallel regime, to press for technical and industry consultation before adoption, to seek a technology-neutral and risk-based rule scoped to invasive clinical neurotechnology rather than consumer devices.

³⁴⁴ Superintendencia de Protección de Datos Personales. (2026, September 9). *Resolución No. SPDP-SPD-2026-0039-R: Norma General para el Tratamiento de Datos Biométricos*.

<https://spdp.gob.ec/wp-content/uploads/2026/09/SPDP-SPD-2026-0039-R.pdf>

³⁴⁵ Superintendencia de Protección de Datos Personales. (2026) *SPDP-SPD-202600*R*

https://www.spdp.gob.ec/wp-content/uploads/2026/10/23092026_014159_Proyecto_Norma_Datos_Salud-1.pdf

The Bill on Children's Protection in Digital and Economic Exposure Environments includes requirements for reporting, transparency, and data retention, provides for fines of up to 10% of local revenue, grants the Ministry of Labor and Human Development the authority to order the removal of content without a court order, prohibits behavioral advertising, and requires companies to have a physical or electronic point of contact to address requests from local authorities.³⁴⁶ USTR should monitor these bills as they advance.

In August 2026 a ruling party member introduced a new e-commerce bill that establishes joint liability for third-party content, reversing the burden of proof, imposing strict algorithmic and operational transparency obligations, and imposing fines of up to 4% of local sales.³⁴⁷

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. Customs valuation practices often deviate from WTO-compliant methodologies, with declared values on commercial invoices, even when verified, frequently disregarded.³⁴⁸ Inconsistent application of HS codes can lead to goods being reclassified under higher tariff categories, and arbitrary 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.

Since January 1, 2026, Egypt has extended mandatory Advance Cargo Information (ACI) requirements to air shipments.³⁴⁹ The regime includes exemptions, notably for qualifying

³⁴⁶ Asamblea Nacional del Ecuador. (2026, July 29). Proyecto de Ley Orgánica de Protección Integral de Niñas, Niños y Adolescentes en Entornos Digitales y de Exposición Económica. [https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-19130/2998.%20Proyecto%20de%20Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20Integral%20de%20Ni%C3%B1as.%20Ni%C3%B1os%20y%20Adolescentes%20en%20Entornos%20Digitales%20y%20de%20Exposici%C3%B3n%20Econ%C3%B3mica%20\(As.%20Luigi%20Garc%C3%ADa%20-%20484205\)/pp%20proyecto%20de%20ley%20484205-garc%C3%8Da-1.pdf](https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-19130/2998.%20Proyecto%20de%20Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20Integral%20de%20Ni%C3%B1as.%20Ni%C3%B1os%20y%20Adolescentes%20en%20Entornos%20Digitales%20y%20de%20Exposici%C3%B3n%20Econ%C3%B3mica%20(As.%20Luigi%20Garc%C3%ADa%20-%20484205)/pp%20proyecto%20de%20ley%20484205-garc%C3%8Da-1.pdf).

³⁴⁷ Asamblea Nacional del Ecuador. (2026, August 6). Proyecto de Ley Orgánica Reformatoria a varios cuerpos legales para una protección integral en el comercio electrónico. [https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-19130/3005.%20Proyecto%20de%20Ley%20Org%C3%A1nica%20Reformatoria%20a%20varios%20cuerpos%20legales%20para%20una%20protecci%C3%B3n%20integral%20en%20el%20comercio%20electr%C3%B3nico%20\(A.%20Mario%20Zambrano%20-%20484527\)/484527-zambrano.pdf](https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-19130/3005.%20Proyecto%20de%20Ley%20Org%C3%A1nica%20Reformatoria%20a%20varios%20cuerpos%20legales%20para%20una%20protecci%C3%B3n%20integral%20en%20el%20comercio%20electr%C3%B3nico%20(A.%20Mario%20Zambrano%20-%20484527)/484527-zambrano.pdf)

³⁴⁸ European Commission Access2Markets. (2025, April 29). *Inconsistent customs valuation of imports in different ports*. https://trade.ec.europa.eu/access-to-markets/nl/barriers/details?isSps=false&barrier_id=14222

³⁴⁹ Nafeza. (n.d.). *Advance Cargo Information System (Aviation)*. <https://www.nafeza.gov.eg/en/pages/39>

single-parcel express shipments weighing no more than 50 kg. Egyptian importers must maintain updated registration information on Nafeza (Egypt's single window), while foreign exporters must register on the linked blockchain platform and electronically submit shipment documentation. These requirements add significant compliance steps for cross-border e-commerce suppliers and other exporters, and disproportionately affect smaller businesses.

Government-Imposed Content Restrictions and Related Access Barriers

The Supreme Council for Media Regulation (SCMR), governed by Law No. 180 of 2018,³⁵⁰ serves as the central regulatory body for Egypt's media sector. Its responsibilities include licensing television, radio, and covered online platforms, administering notification requirements for Egyptian newspapers, and 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 with its requirements has introduced notable operational and financial burdens for both domestic and international companies.

Article 19 of Law No. 180 of 2018 extends specified content restrictions and SCMR suspension or blocking powers to personal websites, blogs, and accounts with at least 5,000 followers.³⁵¹ Separately, SCMR Decree No. 26 of 2020 establishes licensing requirements for covered media outlets and websites.³⁵² Fees vary by category, with the licensing schedule specifying EGP 3 million (over \$50,000) for certain foreign website categories, including social-networking, on-demand content, and goods-and-services marketing websites. On June 8, 2024, the SCMR announced that unlicensed digital platforms and websites operating in Egypt would face blocking within three months.³⁵³ It also instructed the Central Bank of Egypt to halt bank transfers to unlicensed websites and platforms. The threatened restrictions on both access and payments create significant operating risks for affected foreign suppliers. Because SCMR is not transparent in its blocking measures, the number of affected sites is unknown.

Amendments to the licensing framework introduced accreditation requirements for covered "social information technology companies," including certain streaming and content-sharing platforms.³⁵⁴ Accreditation entails substantive content-management obligations: covered companies must maintain complaint-handling mechanisms, submit semiannual reports in Arabic and English, and respond to notified complaints by removing harmful content within 24 hours,

³⁵⁰ Egypt. (2018). *Law No. 180 of 2018 on Press, Media and the Supreme Council for Media Regulation*. <https://www.wipo.int/wipolex/en/legislation/details/19960>

³⁵¹ Egypt. (2018, August 27). *Law No. 180 of 2018 on Press, Media and the Supreme Council for Media Regulation*, Article 19. <https://www.wipo.int/wipolex/en/legislation/details/19960>

³⁵² Supreme Council for Media Regulation. (2020, May 5). *لائحة تنظيم التراخيص بالمجلس الأعلى*. قرار رقم 26 لسنة 2020 بإصدار لائحة تنظيم التراخيص بالمجلس الأعلى [Decree No. 26 of 2020 issuing the licensing regulations of the Supreme Council for Media Regulation]. https://masaar.net/ar/egypt_laws/لائحة-تنظيم-التراخيص-بالمجلس-الأعلى/

³⁵³ Al Tamimi & Company. (2024, June 24). *Regulating Websites and Platforms in Egypt: Compliance Requirements*. <https://www.tamimi.com/news/regulating-websites-and-platforms-in-egypt-compliance-requirements/>

³⁵⁴ SMEX. (2022, October 7). *How The Supreme Council For Media Will Subject Netflix And Disney To Egyptian Laws*. <https://smex.org/how-the-supreme-council-for-media-will-subject-netflix-and-disney-to-egyptian-laws-2/>

with immediate removal in specified cases. Broad prohibited-content categories and SCMR enforcement discretion create compliance uncertainty for foreign platforms.

In July-August 2025, Egyptian authorities arrested or prosecuted numerous online content creators under broadly-framed morality and family-values provisions, including Article 25 of the Cybercrime Law. Human Rights Watch documented at least 29 cases from Interior Ministry statements and identified reports of eight additional cases.³⁵⁵ Such enforcement creates uncertainty for creators and can chill lawful content production on digital platforms.

On February 4, 2026, the SCMR announced implementation of a block on the U.S. game platform Roblox in coordination with the National Telecommunications Regulatory Authority, following concerns about children's online safety.³⁵⁶ The action illustrates the use of platform-wide blocking, with direct consequences for access to foreign digital services. In September 2026, the Administrative Court dismissed Roblox's challenge to the blocking decision for lack of standing.³⁵⁷ The dismissal left the decision intact without determining the substantive legality of the block.

Restrictions on Cross-Border Data Flows

Egypt's Executive Regulations for Personal Data Protection Law No. 151/2020, published on November 1, 2025, create significant compliance burdens for cross-border digital services as the transition period approaches its November 2026 conclusion.³⁵⁸ The framework generally conditions overseas transfers on equivalent protection and PDPC authorization, subject to statutory exceptions, while requiring consent, detailed documentation, and destination-specific approvals. Applications may take up to 90 business days to be processed, and involve significant fees. Foreign controllers without an Egyptian presence must appoint a PDPC-approved local representative, while violations of transfer provisions can trigger imprisonment and substantial fines. USTR should encourage Egypt to streamline these requirements and recognize interoperable transfer safeguards to reduce unnecessary barriers for U.S. and other foreign digital-service suppliers.

³⁵⁵ 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>

³⁵⁶ Supreme Council for Media Regulation. (2026, February 4). *في مصر اعتباراً من* [SCMR: Roblox blocking implemented in Egypt starting today]. <https://scm.gov.eg/الأعلى-للاعلام-تنفيذ-حجب-لعبة-روبلكس/>

³⁵⁷ Eissa, M. (2026, September 13). *Administrative Court dismisses challenge to Roblox blocking for lack of standing* [Arabic]. El Watan. <https://www.elwatannews.com/news/details/8357584>

³⁵⁸ Egyptian Ministry of Communications and Information Technology. (2025, November 1). *Decree No. 816 of 2025 concerning the issuance of the Executive Regulations of the Personal Data Protection Law promulgated by Law No. 151 of 2020* [English translation]. Al-Waqa'i' al-Misriyya, No. 244, Supplement A. https://www.thesedonaconference.org/sites/default/files/meeting_paper/7.4%20Egypt%20Personal%20Data%20Protection%20Law%20-%20Executive%20Regulations.pdf

Ethiopia

Government Audit Powers and Mandatory Platform Licensing

Ethiopia's House of Peoples' Representatives enacted the Critical Infrastructure Cybersecurity Proclamation No. 1426/2026, requiring businesses to report cybersecurity incidents within 48 hours, a requirement that should be relaxed to allow businesses to investigate breaches within a reasonable timeframe. The evolving international norm for reporting is 72 hours.³⁵⁹

European Union

The European Commission is currently pursuing an expansive digital 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.”³⁶⁰ Measures include industrial and competition policy, platform regulation and increased platform liability, regulation of AI and a range of technology-specific certification schemes, including under the rubric of cybersecurity. The pursuit of “technological sovereignty” appears designed to disadvantage U.S. exporters to the benefit of domestic EU competitors, but will likely also undermine Europe's long-term prospects for digital innovation—a risk identified by Mario Draghi, who links Europe's failure to embrace digitally-friendly policies to one of its most pressing weaknesses, its lagging innovation and the inevitable consequence, declining productivity.³⁶¹

Asymmetric Platform Regulation

The Digital Markets Act (DMA)³⁶² entered into force on November 1, 2022, with core provisions taking effect 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, and exclude comparable, competing EU suppliers, reflecting the intent of key policymakers.³⁶³ Similarly, the

³⁵⁹ CSIS. (2024). *Select List of Global Cybersecurity Reporting Requirements*.

<https://www.csis.org/blogs/strategic-technologies-blog/select-list-global-cyber-incidents-reporting-requirements>

³⁶⁰ Breton, T. (2023, September 5). *Tech and geopolitics: Building European resilience in the digital age* <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-brex-it-will-5g-survive-the-age-of-the-european-empire/>.

³⁶¹ 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

³⁶² European Parliament and Council of the European Union. (2022, September 14). *Regulation (EU) 2022/1925 (Digital Markets Act)*. <https://eur-lex.europa.eu/eli/reg/2022/1925/oj>

³⁶³ Espinoza, J. (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>

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 under this measure. Although it originally considered designating up to 25 companies³⁶⁴ as so-called “gatekeepers” under the DMA (a number that would have likely swept in European operators), the European Commission ultimately only designated six companies, and 22 of their services, as subject to the new rules. Five of the six initially designated companies were American. The designation list has subsequently evolved: the Commission designated Apple’s iPadOS in April 2024 and Booking.com in May 2024, and removed Meta’s Facebook Marketplace designation in April 2025. As of September 2026, the DMA covers seven gatekeepers and 23 core platform services.³⁶⁵ The European Commission (EC) is currently preparing to extend the DMA to cloud operators by designating two U.S. cloud service providers as gatekeepers despite them not meeting the quantitative thresholds set out in the legislation, and doubts about whether the DMA is “fit for purpose” for a regulating this structurally distinct sector.³⁶⁶

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).³⁶⁷ In addition to outright prohibitions, gatekeepers are subject to prescriptive product design obligations, designed to aid rivals. Under Article 8, the Commission may specify measures that designated gatekeepers must implement to comply with the interoperability mandates of Articles 6 and 7. Under this and similar provisions the DMA compels 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. This process enables rivals to seek interventions that increase gatekeepers’ costs, diminish the quality and security of their products, and generally constrains product development. Compliance costs are compounded by a lack of clarity on how to satisfy many of these obligations, leaving gatekeepers to interpret ambiguous requirements with little regulatory guidance and limited legal certainty. 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.³⁶⁸ These extraordinary costs contrast dramatically with the EU’s own initial cost-benefit analysis, which estimated a per-gatekeeper cost of €1.4

³⁶⁴ European Commission. (2020). *Impact assessment of the Digital Markets Act*.

<https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act>

³⁶⁵ European Commission. (n.d.). *Gatekeepers portal*. https://digital-markets-act.ec.europa.eu/gatekeepers-portal_en

³⁶⁶ CCIA Europe. 2026. *Is the DMA the Right Tool to Promote Competition in Cloud Computing?*

<https://ccianet.org/articles/is-the-dma-the-right-tool-to-promote-competition-in-cloud-computing/>

³⁶⁷ European Commission. (2024, March 7). *Designated gatekeepers must now comply with all obligations under the Digital Markets Act*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1342

³⁶⁸ 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

million (\$1.64 million)--*i.e.*, less than one-hundredth of CCIA's modeled annual compliance-cost estimate.³⁶⁹

The DMA represents a dramatic paradigm 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 is 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. In this approach, the burden of proof with respect to harms is reversed, with designated companies required to demonstrate compliance or justify any deviation, rather than the Commission bearing the burden of establishing harm.

The European Commission published its first review of the DMA on April 28, 2026, concluding that the regulation remains fit for purpose and failing to propose any meaningful reform.³⁷⁰ The review did not resolve industry concerns about disproportionate compliance costs, restrictions on integrated services, and compelled access to proprietary technology and data. The report noted the increased focus on enforcement in relation to AI, an area of leadership for the US and US companies. CCIA urges the U.S. government to continue engaging European counterparts on these concerns and to seek concrete improvements in the proportionality, predictability, and implementation of the DMA.

Subsequent enforcement has further demonstrated the implications for U.S. suppliers. On July 16, 2026, the Commission adopted specification decisions concerning interoperability with Google's Android services and access to Google Search data.³⁷¹ On July 23, it imposed fines totaling €890 million on Google for self-preferencing and anti-steering infringements.³⁷² The Commission decision in relation to Google search data has been imposed despite the ongoing concerns of experts, including European privacy regulations, about the nature of the proposed disclosures.³⁷³ These developments reinforce the importance of protecting confidential business

³⁶⁹ European Commission. (2020). *Impact assessment of the Digital Markets Act*.

<https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act>.

³⁷⁰ European Commission. (2026, April 28). *Review highlights Digital Markets Act remains fit for purpose and has positive impact*.

https://digital-markets-act.ec.europa.eu/review-highlights-digital-markets-act-remains-fit-purpose-and-has-positive-impact-2026-04-28_en.

³⁷¹ European Commission. (2026, July 16). *Commission provides guidance to Google for AI interoperability on Android and sharing of Google Search data under the Digital Markets Act*.

https://digital-markets-act.ec.europa.eu/commission-provides-guidance-google-ai-interoperability-android-and-sharing-google-search-data-under-2026-07-16_en.

³⁷² European Commission. (2026, July 23). *Commission fines Google €890 million for breaches of the Digital Markets Act*.

https://digital-markets-act.ec.europa.eu/commission-fines-google-eur890-million-breaches-digital-markets-act-2026-07-23_en.

³⁷³ D'Acquisto, G. (2026, September 18). Google query anonymization: what are the hidden risks for data. Agenda Digitale. <https://www.agendadigitale.eu/sicurezza/anonimizzazione-query-google-quali-rischi-nascosti-per-i-dati>.

information, intellectual property, privacy, and cybersecurity when implementing access and interoperability obligations.

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 to foster innovation, increase competition, and support more tailored financial products.³⁷⁴ 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.³⁷⁵ The proposed exclusion would restrict access based on gatekeeper designation rather than an assessment of a provider's conduct, including where customers expressly authorize access to their financial data. The Financial Data Access framework remains a legislative proposal, and the final scope of any gatekeeper exclusion remains subject to negotiations. CCIA urges the U.S. government to oppose categorical exclusions that prevent U.S. suppliers from competing to provide financial data services on equal terms.

Barriers to the Deployment and Operation of Network Infrastructure

The European Commission published a draft EU Space Act (EUSA) in June 2025.³⁷⁶ Under the Commission's proposal, third-country operators would require Commission approval for registration, based on the space agency EUSPA's technical assessment. EU operators would generally obtain national authorization, with a separate regime for Union-owned assets. The proposed Compliance Board is supposed to act independently and is subject to nominal conflict-of-interest safeguards but it is unclear whether these safeguards adequately address the inherent tension in EUSPA's combined regulatory and program-management responsibilities. The additional procedural hurdles for foreign firms combined with the risks to fairness and impartiality poses potential barriers to U.S. firms' market access.

One key feature of the proposal is definitions and regulatory mandates based on the size of constellations, an approach that appears targeted at U.S. suppliers—defining a giga-constellation

³⁷⁴ European Parliament and Council of the European Union. (2023, December 13). *Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act)*. <https://eur-lex.europa.eu/eli/reg/2023/2854/oj>; European Commission. (2023, June 28). *Proposal for a regulation 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 (COM(2023) 360 final)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0360>

³⁷⁵ Flinders, K. (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>

³⁷⁶ *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> .

as containing at least 1,000 operational spacecraft. Additional requirements applicable to this category would disproportionately affect U.S. operators of large constellations—a form of *de facto* discrimination, since EU operators do not operate such services. The EU Space Act remains under negotiation, seeking to address third-country operators, regulatory equivalence arrangements, and the allocation of supervisory responsibilities.³⁷⁷ CCIA urges the U.S. government to seek recognition from the EU of comparable U.S. regulatory requirements and to oppose duplicative or discriminatory conditions impeding U.S. satellite operators’ access to the EU market.

In a related but separate action, on May 27, 2026, the European Commission proposed a new framework for authorizing systems providing mobile satellite services in the harmonized 2 GHz frequency band.³⁷⁸ The proposal prioritizes new entrants for two of the four paired 5 MHz blocks available for commercial mobile satellite services, but restricts eligibility to EU firms, based on specious cybersecurity grounds.³⁷⁹ These conditions would restrict participation by U.S. satellite providers and could require changes to globally integrated network architectures. Given likely inconsistency with respect to the EU’s GATS commitments that cover satellite services, CCIA urges the U.S. government to seek transparent, proportionate authorization requirements that recognize equivalent safeguards and do not use corporate nationality or jurisdiction as a substitute for assessing actual security risks.

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.

Over the past several years, the European Union Agency for Cybersecurity (ENISA) has been developing the EU Cybersecurity Certification Scheme for Cloud Services (EUCS), an initiative that initially incorporated a protectionist certification scheme currently in force in

³⁷⁷ Council of the European Union. (2026, May 8). *Regulation on the safety, resilience and sustainability of space activities in the Union (EU Space Act) – Progress report* (8861/26).

<https://data.consilium.europa.eu/doc/document/ST-8861-2026-INIT/en/pdf>

³⁷⁸ European Commission. (2026, May 27). *Proposal for a regulation on the procedure for authorisation of systems providing mobile satellite services using the harmonised 2 GHz frequency band and repealing Decision No 626/2008/EC* (COM(2026) 311 final).

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52026PC0311>

³⁷⁹ CCIA. (2026, June). *CCIA Explainer on EU 2 GHz Mobile Satellite Services Regulation*. <https://ccianet.org/library/ccia-explainer-on-eu-2-ghz-mobile-satellite-services-regulation/>.

France—eligibility requirements that explicitly discriminated against non-EU companies.³⁸⁰ The latest draft no longer contains such requirements.

On January 20, 2026, the European Commission proposed a revised Cybersecurity Act that would amend the European cybersecurity certification framework and establish a framework for addressing non-technical risks in ICT supply chains.³⁸¹ The proposal would enable restrictions involving suppliers designated as high risk, creating potential market-access consequences across critical sectors. CCIA is concerned that assessments based on ownership, control, or exposure to third-country laws would disadvantage U.S. suppliers even where they meet rigorous technical and operational security standards.³⁸² CCIA urges USTR to ensure that the proposed framework distinguishes demonstrable security risks from nationality-based assumptions and provides transparent designation criteria, proportionate mitigation options, and effective opportunities for review.

On June 3, 2026, the European Commission proposed the Cloud and AI Development Act (CADA), including an EU-wide framework for assessing the sovereignty of cloud and AI services.³⁸³ The proposal establishes four assurance levels and a mechanism linking public-sector adoption to assessments of the sensitivity and criticality of relevant uses. Higher assurance requirements address matters including ownership, control, jurisdiction, and the location of operations. The proposal also provides for the possible extension of requirements to specified private-sector uses in highly critical sectors.

These provisions could disadvantage U.S. providers and restrict European customers' access to globally competitive cloud and AI services, particularly where eligibility depends on corporate structure rather than demonstrable security and operational safeguards. Of particular concern are the broad data localization requirements which apply in differing degrees across all risk levels. CCIA urges the U.S. government to seek risk-based, technology-neutral requirements that recognize equivalent protections and preserve opportunities for trusted U.S. suppliers. The proposal should not impose ownership-based exclusions where contractual, technical, and operational safeguards can address the identified risks.

³⁸⁰ 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>

³⁸¹ European Commission. (2026, January 20). *Proposal for a regulation on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)* (COM(2026) 11 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52026PC0011>

³⁸² ECIPE. (2026). *The Real-World Economic Impact of the Cloud and AI Development Act (CADA): What CADA Could Mean for Cloud Prices, Migration, Digitalisation and Europe's Technology Supply Chain*. <https://ecipe.org/publications/economic-impact-of-cada/>.

³⁸³ European Commission. (2026, June 3). *Proposal for the Cloud and AI Development Act (CADA)*. <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>

Furthermore, high-assurance requirements under legislative proposals such as CADA (including Union assurance level 3 and above under Article 18.1) should not be tied solely to the existence of a GDPR adequacy decision, which creates supply-chain fragility; instead, EU legislation incorporates appropriate flexibilities by explicitly recognizing the full menu of GDPR Chapter V transfer mechanisms (such as Standard Contractual Clauses and Binding Corporate Rules) alongside advanced technical and cryptographic controls like External Key Management. Policymakers should also recognize that measures under CADA or sector-specific frameworks like DORA that incentivize or compel the localization of customer data, operational telemetry, and diagnostic metadata within the EU disrupt globally integrated threat intelligence networks, creating blind spots that undermine real-time, edge-based cybersecurity defense.

The European Commission has also begun applying cloud-sovereignty criteria through procurement. On April 17, 2026, it announced awards under a tender allowing EU institutions, bodies, offices, and agencies to procure up to €180 million in “sovereign” cloud services over six years.³⁸⁴ The tender used the Commission’s Cloud Sovereignty Framework and required a minimum Sovereignty Effectiveness Assurance Level of SEAL-2, demonstrating that sovereignty criteria are already influencing purchasing decisions independently of the proposed CADA legislation. Such criteria can increase compliance costs and constrain the commercial structures through which U.S. suppliers serve European public-sector customers. The framework does not categorically exclude U.S. technology and one successful offering combines European operational arrangements with technology and services of a U.S. supplier. CCIA urges the use of objective security and resilience requirements that permit competing suppliers, including American, to demonstrate equivalent safeguards.

Implementation of the Digital Operational Resilience Act (DORA) has introduced direct oversight of major technology suppliers serving the financial sector. On November 18, 2025, the European Supervisory Authorities published their first list of 19 critical ICT third-party service providers, including entities within the Amazon, Google, and Microsoft groups.³⁸⁵ Designated providers face information requests, investigations, inspections, and oversight fees. For a designated critical provider established in a third country, Article 31(12) conditions continued use of its services by EU financial entities on establishment of an EU subsidiary within 12 months of designation. These requirements create additional establishment and supervisory burdens for affected U.S. suppliers, although DORA does not impose a general requirement to store all financial-sector data in the EU.

³⁸⁴ European Commission, Directorate-General for Digital Services. (2026, April 17). *Commission advances cloud sovereignty through strategic procurement*. https://commission.europa.eu/news-and-media/news/commission-advances-cloud-sovereignty-through-strategic-procurement-2026-04-17_en

³⁸⁵ European Supervisory Authorities. (2025, November 18). *The European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act*. <https://www.esma.europa.eu/press-news/esma-news/european-supervisory-authorities-designate-critical-ict-third-party-providers>

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.”³⁸⁶ Many of those ICT products are currently supplied by U.S. companies,³⁸⁷ 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. The European Commission has been working with national governments to complete the first round of risk assessments since the fall of 2023.

On September 9, 2026, the European Commission proposed a Public Procurement Act that includes a framework for European preferences and requirements addressing security, resilience, and supply-chain dependencies.³⁸⁸ These provisions could affect U.S. technology suppliers’ access to public contracts. The proposal does distinguish suppliers, goods, and services covered by the WTO Government Procurement Agreement or other procurement agreements from those that are not covered, but products and services supplied by U.S. firms from outside a GPA or FTA territory would be put at a disadvantage.³⁸⁹ CCIA urges the U.S. government to preserve negotiated procurement access and seek transparent, proportionate requirements that recognize equivalent security and operational safeguards.

Forced Revenue Transfers for Digital News

Article 15 of the EU Copyright Directive creates a press publishers’ right that can require authorization for covered online uses of press publications by search engines, aggregators, and platforms. Hyperlinks, individual words, and very short extracts are nominally excluded, and applicable copyright exceptions remain relevant. As evidenced by outcomes in France and the Czech Republic, the narrow “short excerpts” exemption offers little legal certainty, given varying

³⁸⁶ 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

³⁸⁷ 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 here: European Commission. (2023, October 3). *Annex to the Commission recommendation on critical technology areas for the EU’s economic security for further risk assessment with Member States* (C(2023) 6689 final). https://defence-industry-space.ec.europa.eu/system/files/2023-10/C_2023_6689_1_EN_annexe_acte_autonome_part_1_v9.pdf

³⁸⁸ European Commission. (2026, September 9). *Proposal for a regulation on public contracts and concessions (Public Procurement Act)* (COM(2026) 590 final).

https://single-market-economy.ec.europa.eu/publications/proposal-regulation-public-contracts-and-concessions_en

³⁸⁹ HSF. (2026). *The European Public Procurement Act*.

<https://www.hsfrkramer.com/notes/crt/2026-09/the-eu-public-procurement-act-the-commission-proposes-a-european-preference-framework>.

interpretations as to what qualifies. Compounding the complexity, Article 15(5) requires Member States to ensure that authors receive an appropriate share of revenues received by press publishers for the relevant uses.

The Directive does not comprehensively harmonize copyright exceptions, including freedom of panorama. However, it does establish two text and data mining exceptions: Article 3 covers scientific research by qualifying research organizations and cultural heritage institutions, while Article 4 permits text and data mining more broadly, including for commercial purposes, where access is lawful and rightsholders have not expressly reserved the relevant rights in an appropriate manner. The conditions governing reservations, acceptable standards for exclusion protocols, and their practical implementation can create uncertainty for U.S. developers seeking to rely on Article 4. This uncertainty is compounded by far-reaching policy proposals put forward by the European Commission in a new ‘targeted’ legislative consultation concerning rights reservation methods, transparency or licensing obligations for AI developers, as well as other aspects of the current EU copyright regime.

National implementation of the Copyright Directive 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.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

The European Media Freedom Act (EMFA), most of which became applicable on August 8, 2025, introduces special procedures governing very large online platforms’ treatment of content from qualifying media service providers.³⁹⁰ Article 18 generally requires platforms to provide reasons and an opportunity to respond before certain restrictions based on incompatibility with their terms and conditions take effect, including a 24-hour response period in ordinary circumstances. On February 6, 2026, the Commission published implementation guidelines addressing media-provider declarations and related platform procedures. These requirements add complexity to content moderation and may impede timely enforcement of platform policies. Since the EMFA does not exempt suppliers from obligations to address illegal content under the DSA, suppliers risk being subject to conflicting mandates.³⁹¹ CCIA urges implementation that

³⁹⁰ European Parliament and Council of the European Union. (2024, April 11). *Regulation (EU) 2024/1083 (European Media Freedom Act)*, Articles 18 and 29.

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32024R1083>

³⁹¹ European Commission. (2026, February 6). *Guidelines under Article 18 of the European Media Freedom Act (EMFA)*.

<https://digital-strategy.ec.europa.eu/en/library/guidelines-under-article-18-european-media-freedom-act-emfa>

preserves platforms' ability to protect users while avoiding conflicting obligations across the EU's digital rulebook.

The "Digital Services Act" (DSA), setting EU norms for content liability, entered into force generally on November 16, 2022.³⁹² Specific obligations for designated "very large online platforms" and "very large online search engines" have been in effect since 2023, with the European Commission having designated the first 19 services: 17 very large online platforms and two very large online search engines.³⁹³ Most of the 19 initially designated services were operated by U.S. companies. DSA VLOPS and VLOSEs are designated based on size alone, and note a separate determination of risk. This 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.

DSA enforcement and designation have continued to expand. In December 2025, the Commission imposed a €120 million fine on X for breaches of transparency obligations.³⁹⁴ On August 31, 2026, it designated ChatGPT as a very large online search engine and Reddit and Roblox as very large online platforms, bringing additional U.S. services within the enhanced framework for systemic-risk assessment, mitigation, audits, and data access.³⁹⁵ These developments increase the importance of proportionate implementation and effective protections for confidential information, user privacy, and cybersecurity.

These new rules police how providers moderate for illegal content, counterfeiting, collaborative economy services, or product safety. The DSA incorporates a range of obligations including notice & takedown systems for hosting services, 'know your business customer', transparency of content moderation, and cooperation with authorities. Platforms with 45 million or more active users, including a large number of U.S. companies, have to comply with additional obligations such as strict transparency and reporting obligations, risk assessments, yearly audits,³⁹⁶ 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

³⁹² European Parliament and Council of the European Union. (2022, October 19). *Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act)*. <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

³⁹³ European Commission. (2023, April 25). *Digital Services Act: Commission designates first set of very large online platforms and search engines*. <https://digital-strategy.ec.europa.eu/en/news/digital-services-act-commission-designates-first-set-very-large-online-platforms-and-search-engines>

³⁹⁴ European Commission. (2025, December 5). *Commission fines X €120 million under the Digital Services Act*. <https://digital-strategy.ec.europa.eu/en/news/commission-fines-x-eu120-million-under-digital-services-act>

³⁹⁵ European Commission. (2026, August 31). *Commission designates ChatGPT, Reddit, Roblox under Digital Services Act*. <https://digital-strategy.ec.europa.eu/en/news/commission-designates-chatgpt-reddit-roblox-under-digital-services-act>

³⁹⁶ 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/>

content regulation, an often overly burdensome mechanism that fails 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.

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 personalized targeted advertising undermined the horizontal normative purpose of the DSA proposal.

Throughout implementation, the European Commission continues to use the DSA to further regulate online services beyond the scope of the legislation.³⁹⁷ As the Commission was building a database containing platforms' statements of reasons for content-moderation decisions, information beyond what was required by the DSA was solicited from online service suppliers.³⁹⁸

In 2025, the Commission also worked on guidelines on protection of minors under the DSA, which were published in July 2025.³⁹⁹ CCIA contributed to the work of the Commission in this respect and provided comments to the draft.⁴⁰⁰ 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.⁴⁰¹

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 2021 General Product Safety Regulation (GPSR)

³⁹⁷ 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/>

³⁹⁸ 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/>

³⁹⁹ European Commission. (2025, July 14). *Commission publishes guidelines on the protection of minors*.

<https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>

⁴⁰⁰ CCIA. (2025, June 16). *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/>

⁴⁰¹ CCIA. (2025, July 11). *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/>

proposal.⁴⁰² The GPSR was published in the Official Journal of the European Union on May 23, 2023⁴⁰³ and took effect on December 13, 2024. This regulation updates the existing Product Safety Directive to respond to new challenges related to online purchases including via marketplaces.⁴⁰⁴ The GPSR also permits market-surveillance authorities to order online marketplaces, for a specified period, to remove identical content referring to offers of a dangerous product, disable access to it, or display an explicit warning. These obligations add to marketplaces' compliance burdens, but should be distinguished from an unrestricted duty to monitor for every previously flagged product.

The EU is progressively introducing Digital Product Passport⁴⁰⁵ requirements under the Ecodesign for Sustainable Products Regulation, with requirements expanding over time across product groups. While these requirements are primarily designed around newly manufactured goods, they may create particular barriers for U.S. sellers of second-hand, refurbished and legacy products, who may have no access to information held by the original manufacturer or to an existing DPP, particularly for goods manufactured before the requirements applied. Requiring such information as a condition of sale could therefore restrict access to the EU market for legitimate downstream sellers.

The European Commission's May 2022 proposal to prevent and combat child sexual abuse online remains under negotiation. The Council agreed its negotiating position on November 26, 2025, providing for risk assessment and mitigation, removal and blocking measures, and an EU Centre on Child Sexual Abuse.⁴⁰⁶ Its position supports making voluntary detection activities permanent, rather than carrying forward the Commission proposal's mandatory detection-order framework. Voluntary detection is currently authorized until April 3, 2028.⁴⁰⁷ CCIA continues to

⁴⁰² 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

⁴⁰³ European Parliament and Council of the European Union. (2023, May 10). *Regulation (EU) 2023/988 on general product safety, amending Regulation (EU) No 1025/2012 and Directive (EU) 2020/1828, and repealing Directive 2001/95/EC and Council Directive 87/357/EEC*.

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R0988>

⁴⁰⁴ European Parliament and Council of the European Union. (2001, December 3). *Directive 2001/95/EC on general product safety*. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0095>

⁴⁰⁵ EU Internal Market. (2025). *What is a Digital Product Passport?*

https://single-market-economy.ec.europa.eu/single-market/digital-product-passport_en.

⁴⁰⁶ Council of the European Union. (2026, July 27). *Preventing child sexual abuse*.

<https://www.consilium.europa.eu/en/policies/prevent-child-sexual-abuse/>; Council of the European Union. (2025, November 26). *Child sexual abuse: Council reaches position on law protecting children from online abuse*.

<https://www.consilium.europa.eu/en/press/press-releases/2025/11/26/child-sexual-abuse-council-reaches-position-on-law-protecting-children-from-online-abuse/>

⁴⁰⁷ Council of the European Union. (2026, July 23). *Fighting child sexual abuse online: Interim measure protecting children now reinstated*.

<https://www.consilium.europa.eu/en/press/press-releases/2026/07/23/fighting-child-sexual-abuse-online-interim-measure-protecting-children-now-reinstated/>

support effective child-protection measures while opposing requirements that undermine encryption, privacy, or the security of users' communications.

The European Commission will be releasing its proposal for a Digital Fairness Act (DFA) on 11 November 2026. This proposal will address practices online deemed harmful to consumers of all ages across all types of B2C platforms. Specifically, it will likely address dark patterns, influencer marketing, digital contracts, unfair pricing, addictive design and personalization. The overlaps between the KIDS Act (introduced September 17) the DFA and DSA, as well as other existing EU legislation, is likely to create significant compliance burden and legal uncertainty for U.S. platforms and thus warrants careful monitoring.

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.⁴⁰⁸ Regulation (EU) 2024/900 was adopted on March 13, 2024, published in the Official Journal on March 20, 2024,⁴⁰⁹ and became generally applicable on October 10, 2025. 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 requirements of this legislative regime prompted several U.S. companies to withdraw their political advertising services from the European market.⁴¹⁰

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.⁴¹¹ 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. Article 17 applies to online content-sharing service providers as specifically defined in the Directive. Where authorization is unavailable, covered providers may avoid liability by satisfying applicable best-efforts licensing and content-unavailability requirements and acting expeditiously on sufficiently substantiated notices, subject to proportionality, safeguards for lawful uses, and a modified regime for qualifying new providers. 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

⁴⁰⁸ European Commission. (2021, November 25). *European democracy: Commission sets out new laws on political advertising, electoral rights and party funding*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6118

⁴⁰⁹ European Parliament and Council of the European Union. (2024).

Regulation (EU) 2024/900 on the transparency and targeting of political advertising.
<https://eur-lex.europa.eu/eli/reg/2024/900/oj/eng>

⁴¹⁰ Chee, F. Y. (2025). *Meta to halt political advertising in EU from October, blames EU rules*. Reuters.
<https://www.reuters.com/sustainability/meta-halt-political-advertising-eu-october-blames-eu-rules-2025-07-25/>

⁴¹¹ European Parliament and Council of the European Union. (2019). *Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC*.
<https://eur-lex.europa.eu/eli/dir/2019/790/oj>

lead to a general monitoring obligation,⁴¹² 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.⁴¹³ 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.

In 2024, the EU adopted a revised Product Liability Directive, Directive (EU) 2024/2853, replacing its earlier product-liability framework.⁴¹⁴ The directive expressly includes software within the definition of products and provides for rebuttable presumptions concerning defectiveness or causation in specified circumstances, including cases involving excessive technical or scientific complexity. It also creates potential liability for certain online marketplaces where the conditions in Article 6(3) of the DSA are met and the marketplace fails, within one month of a request, to identify the relevant EU-established economic operator or its own supplier. Member States must transpose the directive by December 9, 2026; it applies to products placed on the market or put into service after that date. These changes may increase litigation exposure and compliance costs for U.S. software developers and online marketplaces.

In late 2026 or the beginning 2027, the European Commission is also expected to propose a new legislation – the EU Product Act – that would overhaul product and market surveillance policy. While not yet a formal legislation, the leaked direction of travel may warrant the USTR attention on possible measures that may create further barriers for free trade and non-EU platforms.

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 deployment and maintenance.⁴¹⁵ The incumbent telco association, the European Telecommunications Network Operators (formerly ETNO, now Connect Europe) proposed that large content and applications providers, mainly

⁴¹² Court of Justice of the European Union. (2022). *Republic of Poland v. European Parliament and Council of the European Union* (Case C-401/19). <https://curia.europa.eu/juris/document/document.jsf?docid=258261&doclang=en>

⁴¹³ Moody, G. (2024). *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/>

⁴¹⁴ European Parliament and Council of the European Union. (2024). *Directive (EU) 2024/2853 on liability for defective products and repealing Council Directive 85/374/EEC*, Articles 2, 4, 10, 21 and 22. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32024L2853>

⁴¹⁵ 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>

U.S. firms, should be required to pay fees to European ISPs to facilitate the delivery of content demanded by the ISPs' customers—analogue 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.⁴¹⁶ 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. Numerous member states have questioned a rush to institute new fees.⁴¹⁷ 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 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).”⁴¹⁸

The white paper's consultation results were published in September 2024 and showcase similar widespread opposition against proposals for introducing network fees. A CCIA analysis found that 67% of respondents in the most recent consultation voiced opposition to regulatory intervention in the IP interconnection market.⁴¹⁹

On January 21, 2026, the European Commission proposed the Digital Networks Act.⁴²⁰ Article 9 of the proposed DNA risks capturing private network operators, content and application providers (CAPs), and CDNs under interconnection rules and mandatory dispute resolution, functioning as a backdoor to network fees, by extending the scope of the General Authorization

⁴¹⁶ 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>

⁴¹⁷ 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/>

⁴¹⁸ 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>

⁴¹⁹ Stecher, M. T. (2024, September 23). *Consultation on EU's future connectivity networks: (Again) no support for regulatory intervention*. Disruptive Competition Project.
<https://project-disco.org/european-union/consultation-on-eus-future-connectivity/>

⁴²⁰ European Commission. (2026, January 21). *The Digital Networks Act*.
<https://digital-strategy.ec.europa.eu/en/policies/digital-networks-act>

(GA) regime and capturing those providers under mandatory dispute resolution frameworks. CCIA is concerned that the framework proposed under the DNA could create pressure for payments in otherwise competitive interconnection markets and provide a basis for future intervention without demonstrated market failure.

In addition, Articles 191-193 would establish a new framework for relations among network participants. The articles foresee guidance on cooperation between network operators and other digital-sector participants issued by the BEREC (a body of European telecom regulators), a voluntary conciliation facility involving national regulators, and a subsequent review of the framework, three years after its entry into force. These provisions could bring commercial and technical arrangements involving cloud providers, content and application providers and content delivery networks within a new process of regulatory scrutiny.

While the proposal does not directly mandate network usage fees, the effect could be the same: it could enable binding payment awards, if arbitration is deemed mandatory. Parliamentary groups are pushing to convert the ‘voluntary’ mechanism into mandatory arbitration, or, failing that, to impose new funding levies (effectively a ‘digital tax’) on U.S. providers designated under the DMA and DSA. This momentum is extending to the national level. Spain and France are receptive, and as noted above, Italy's regulator (AGCOM) has already moved to bring CDNs under its general authorization regime. CCIA is concerned that the framework proposed under the DNA could create pressure for payments in otherwise competitive interconnection markets and provide a basis for future intervention without demonstrated market failure. Since the EU, as part of the 2025 trade agreement with the United States, agreed not to introduce network usage fees,⁴²¹ further clarifying this in the DNA should be a priority. CCIA urges USTR to seek safeguards preserving the non-regulated status of IP interconnection, as a functioning market based on market practices and standard commercial arrangements, consistent with the EU’s commitment not to adopt or maintain network usage fees.

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,⁴²² and welcomes efforts to date,⁴²³ which appears to have materially helped resist the adoption of this policy so far.

⁴²¹ The White House. (2025, August 21). Article 17 *United States-European Union Framework Agreement*. <https://www.whitehouse.gov/briefings-statements/2025/08/joint-statement-on-a-united-states-european-union-framework-on-an-agreement-on-reciprocal-fair-and-balanced-trade/>.

⁴²² Arts, P., & Conlow, M. (2023, May 8). *The European Network Usage Fees proposal is about much more than a fight between Big Tech and Big European telcos*. Cloudflare. <https://blog.cloudflare.com/eu-network-usage-fees/>

⁴²³ 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>

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 AI Act entered into force on August 1, 2024,⁴²⁴ with phased application, some of which have been subsequently extended based on inadequate preparation. Prohibited-practice rules began applying in February 2025, and general-purpose AI obligations in August 2025. Following the AI Omnibus amendments, which entered into force on July 27, 2026,⁴²⁵ requirements for Annex III high-risk uses are set to apply from December 2, 2027, and those for high-risk systems embedded in regulated products from August 2, 2028. Other requirements, including specified transparency obligations, became applicable in August 2026. The revised schedule provides additional implementation time, but alignment of EU standards with international standards remains unresolved, and critical to avoiding duplicative compliance burdens. For example, it remains uncertain whether EU standards will fully align with ISO standards (e.g., ISO 42001); if not, firms will face dual compliance burdens. Standardization work being developed by CEN-CENELEC to support the Act is well behind schedule, with the first batch of harmonized standards not expected until 2027, leaving model providers very limited time to prepare for compliance. CEN-CENELEC has also streamlined its standardization process to shorten the time needed to finalize standards, which correspondingly reduces opportunities for stakeholder input and for ensuring alignment between EU and international standards.

The Act also imposes training data transparency obligations for general-purpose AI models, requiring providers to publish a sufficiently detailed summary of the content used to train their models using a Commission-developed template finalized in July 2025.⁴²⁶ U.S. and global industry stakeholders have raised concerns about the commercial sensitivity of such disclosures, including potential exposure of trade secrets and the reach of the AI Act's copyright-policy obligation. Article 53(1)(c) requires providers placing general-purpose AI models on the EU market to maintain a policy for compliance with EU copyright law, including applicable reservations of text-and-data-mining rights. However, standards for what constitutes an acceptable mechanism for such reservations remain undeveloped. Recital 106 states that this obligation applies regardless of where the copyright-relevant training activities occurred, raising

⁴²⁴ European Commission. (2024, August 1). *European Artificial Intelligence Act comes into force* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4123; European Parliament and Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, Article 113. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

⁴²⁵ European Parliament and Council of the European Union. (2026, July 8). *Regulation (EU) 2026/1744 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)*, Article 4. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32026R1744>

⁴²⁶ European Commission. (2025, July 24). *Explanatory notice and template for the public summary of training content for general-purpose AI models*. <https://digital-strategy.ec.europa.eu/en/library/explanatory-notice-and-template-public-summary-training-content-general-purpose-ai-models>

significant challenges relating to the extra-territorial application of EU law and the prospects of jurisdictional conflicts.

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: specified systems are subject to transparency obligations, while minimal-risk systems generally face no additional AI Act requirements, 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 general-purpose AI models, with stricter requirements for those posing systemic risks. A voluntary Code of Practice for such models was released in July 2025 and updated in 2026, endorsed by many providers.⁴²⁷ 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.⁴²⁸ CCIA is concerned that the AI Act’s compliance burdens and legal uncertainty could discourage the introduction of AI products in Europe.

Restrictions on Cross-Border Data Flows

The EU’s evolving privacy framework, anchored in the General Data Protection Regulation (GDPR), which became applicable on May 25, 2018,⁴²⁹ 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.⁴³⁰ This foundational regulation has been layered with additional obligations, including DMA restrictions on specified combinations and cross-use of personal data without consent; the Data Act’s exclusion of designated gatekeepers from eligibility as third-party

⁴²⁷ European Commission. (2026, July 31). *The General-Purpose AI Code of Practice*.

<https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>

⁴²⁸ 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>

⁴²⁹ European Parliament and Council of the European Union. (2016, April 27). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*.

<https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

⁴³⁰ Janßen, R., Kesler, R., Kummer, M. E., & Waldfogel, J. (2022). *GDPR and the lost generation of innovative apps*. National Bureau of Economic Research. <https://www.nber.org/papers/w30028>

recipients of connected-product and related-service data under its access regime; and DSA restrictions on advertising based on special categories of personal data. These overlapping obligations exacerbate regulatory fragmentation, driving up compliance costs and creating uncertainty for transatlantic operators.

Compounding these challenges, transatlantic data transfers have faced prolonged instability following the 2020 CJEU Schrems II decision. The 2023 EU-U.S. Data Privacy Framework provided a new transfer basis for participating organizations but did not resolve liability for earlier transfers.⁴³¹ In May 2023, Ireland’s Data Protection Commission, acting following an EDPB binding decision, imposed a €1.2 billion fine on Meta Ireland.⁴³² In August 2024, the Dutch Data Protection Authority announced a €290 million fine on Uber concerning transfers to the United States.⁴³³ Standard contractual clauses remained legally available after Schrems II, but their adequacy depended on the circumstances and any necessary supplementary safeguards; the Irish authority found Meta’s arrangements insufficient. These cases illustrate substantial compliance uncertainty and enforcement exposure for transatlantic transfers. 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.⁴³⁴ Philippe Latombe appealed that judgment on October 31, 2025, in Case C-703/25 P, which remains pending.⁴³⁵ The adequacy decision remains in effect, but the continuing litigation underscores the importance of maintaining a durable legal basis for transatlantic data transfers.

Beyond the ongoing litigation surrounding the EU-U.S. Data Privacy Framework, the European Commission’s 2026 targeted consultation on ‘Safeguarding the EU’s Data Sovereignty’ highlights the urgent need to modernize and simplify the EU’s broader GDPR Chapter V transfer toolkit, as bilateral adequacy decisions alone cannot scale to support the global digital and AI economy. In practice, standard transfer mechanisms remain hampered by an unpragmatic

⁴³¹ European Commission. (2023, July 10). *Commission Implementing Decision (EU) 2023/1795 on the adequate level of protection of personal data under the EU–US Data Privacy Framework*.

https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj/eng

⁴³² Data Protection Commission. (2023, May 22). *Data Protection Commission announces conclusion of inquiry into Meta Ireland* [Press release].

<https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland>

⁴³³ Dutch Data Protection Authority. (2024, August 26). *Dutch DPA imposes a fine of 290 million euro on Uber because of transfers of drivers’ data to the US*.

<https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-of-290-million-euro-on-uber-because-of-transfers-of-drivers-data-to-the-us>

⁴³⁴ Court of Justice of the European Union. (2025, September 3). *Data protection: The General Court dismisses an action for annulment of the new framework for the transfer of personal data between the European Union and the United States* [Press release No. 106/25, Case T-553/23, Latombe v. Commission].

<https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-09/cp250106en.pdf>

⁴³⁵ Court of Justice of the European Union. (2025, December 22). *Case C-703/25 P: Appeal brought on 31 October 2025 by Philippe Latombe against the judgment delivered on 3 September 2025 in Case T-553/23, Latombe v Commission*. <https://eur-lex.europa.eu/eli/C/2025/6610/oj/eng>

‘zero-risk’ enforcement approach by Data Protection Authorities (DPAs) that penalizes companies based on the theoretical possibility of foreign government access rather than practical likelihood—an approach exacerbated by mass complaints from activist organizations. Furthermore, the requirement to conduct complex, case-by-case Transfer Impact Assessments (TIAs) imposes disproportionate compliance costs (often exceeding €100,000 in legal fees for initial multi-country assessments) that particularly harm SMEs and public-sector entities, while the proliferation of uncoordinated foreign Standard Contractual Clauses (SCCs) increasingly subjects cloud providers to conflicting ‘dual-SCC’ obligations on the exact same dataset. CCIA urges USTR to encourage the European Commission to simplify GDPR Chapter V transfer mechanisms—including by replacing ‘zero-risk’ Transfer Impact Assessments with a practical risk-based standard, streamlining Standard Contractual Clauses and Binding Corporate Rules, and recognizing Privacy-Enhancing Technologies (PETs) as valid safeguards. The EU should also build interoperability bridges with multilateral frameworks such as the OECD’s Data Free Flow with Trust (DFFT) initiative and the Global Cross-Border Privacy Rules (CBPR) System.

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.⁴³⁶ 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.

In its July 4, 2023 judgment in Case C-252/21, *Meta Platforms v. Bundeskartellamt*, the CJEU held that a national competition authority may assess compliance with the GDPR when examining an alleged abuse of a dominant position, subject to cooperation with the competent data-protection authorities.⁴³⁷ The interaction between competition and data-protection enforcement can increase procedural complexity and compliance uncertainty for U.S. firms.

The EU Data Act, adopted in December 2023 and generally applicable from September 12, 2025, 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.⁴³⁸ 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

⁴³⁶ 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>

⁴³⁷ Court of Justice of the European Union. (2023, July 4). *Judgment in Case C-252/21, Meta Platforms and Others v. Bundeskartellamt*, operative part, point 1. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021CJ0252>

⁴³⁸ European Parliament and Council of the European Union. (2023, December 13). *Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act)*. <https://eur-lex.europa.eu/eli/reg/2023/2854>

EU Internet-of-Things data;⁴³⁹ 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. For connected products and related services placed on the market after September 12, 2026, Article 3(1) additionally requires design and provision that make relevant data accessible to users by default, subject to the provision's conditions. This adds product-development and data-access compliance obligations for suppliers serving the EU market.

The Data Governance Act (DGA), applicable since September 24, 2023, establishes conditions for reusing certain protected data held by public-sector bodies, alongside rules for data-intermediation services and data altruism.⁴⁴⁰ Its international-transfer provisions include safeguards for protected non-personal data and measures addressing third-country governmental access that conflicts with EU or Member State law. These requirements add compliance obligations and potential legal conflicts for providers operating across jurisdictions.

On November 19, 2025, the Commission proposed a Digital Omnibus that would consolidate elements of the DGA and other data legislation into the Data Act.⁴⁴¹ The proposal remains subject to the legislative process. CCIA supports simplification that reduces overlapping obligations while preserving predictable, non-discriminatory conditions for cross-border data services.

The EU's e-evidence Regulation, Regulation (EU) 2023/1543, became applicable on August 18, 2026.⁴⁴² It enables competent authorities to issue cross-border European Production and Preservation Orders directly to covered service providers' designated establishments or legal representatives, and can require production of data stored outside the EU. Production orders generally require a supplier to respond within 10 days, or eight hours in emergencies. The accompanying framework requires covered providers offering services in the EU to designate an establishment or appoint an EU legal representative. These obligations create additional

⁴³⁹ 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

⁴⁴⁰ European Parliament and Council of the European Union. (2022, May 30). *Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)*, Articles 1 and 38.
<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0868>

⁴⁴¹ European Commission. (2025, November 19). *Proposal for a regulation as regards the simplification of the digital legislative framework (Digital Omnibus)*, COM(2025) 837 final.
<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025PC0837>

⁴⁴² European Parliament and Council of the European Union. (2023, July 12). *Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings*, Article 34(2).
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1543>

operational and representation costs for U.S. suppliers and can raise conflicts with third-country disclosure restrictions, although the Regulation provides a judicial review procedure for conflicting legal obligations. CCIA urges predictable implementation, workable emergency procedures, and effective safeguards for conflicts of law.

Threats to the Security of Devices and Services

The EU cybersecurity directive (‘NIS2’) is an economy-wide measure that 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). Member States were required to transpose NIS2 by October 17, 2024, but implementation has remained uneven.⁴⁴³ Transposition and implementation of the Network and Information Security (NIS2) Directive is creating significant challenges for multinational companies operating across multiple Member States. For services that do not fall under the main establishment principle, including those that do not depend on Member States’s infrastructure like Number Independent Interpersonal Communication Services (NI-ICS) service providers face significant burdens: duplicative audits across 27 Member States, varying incident reporting thresholds, and diverging cybersecurity safeguards. As a result, these impede a company’s ability to centralize compliance programs, and diverts resources from strengthening its security posture. There is an urgent need for simplification and harmonisation in the context of NIS2, including establishment of the single audit principle and the expansion of the main establishment principle for NI-ICS.

In October 2024 the EU adopted the Cyber Resilience Act (CRA), establishing cybersecurity requirements for products with digital elements, including software and connected devices.⁴⁴⁴ Its principal requirements apply from December 11, 2027, while reporting obligations began on September 11, 2026. The framework requires conformity assessment, although not every covered product requires third-party approval. Applicability to cloud services remains unclear: to the extent that a cloud service is categorized as remote data processing solutions (RDP) on which “product with digital elements” (PDE) depends to perform its functions, coverage under the CRA appears possible. CCIA is concerned that some cloud services could be covered by both NIS2 Directive and CRA, which would create duplicative, overlapping requirements and unnecessary burden for cloud services. It should be clear that if a service is already compliant with NIS2, they do not need to also comply with the CRA.

Manufacturers must provide an early warning within 24 hours after becoming aware of an actively exploited vulnerability or a severe incident affecting a product’s security, followed by

⁴⁴³ European Cyber Security Organisation. (n.d.). *NIS2 Directive transposition tracker*. <https://ecs-org.eu/activities/nis2-directive-transposition-tracker/>

⁴⁴⁴ European Parliament and Council of the European Union. (2024, October 23). *Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*, Articles 1–3. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32024R2847>

further notification generally within 72 hours. The vulnerability-reporting trigger concerns active exploitation, rather than every known vulnerability. Nevertheless, reporting before remediation raises serious concerns about the handling of sensitive security information, especially in the context of developments in AI. CCIA urges proportionate implementation, secure reporting arrangements, and alignment with established vulnerability-management practices to avoid unnecessary risks and market-access delays. CCIA urges the EU to ensure that there is no requirement to report unpatched vulnerabilities before remediation is available.

Other Barriers to Digital Trade

The EU's Foreign Subsidies Regulation (FSR), including an investigative framework and mandatory notification requirements took effect in 2023.⁴⁴⁵ The measure is intended to combat the trade-distortive effect of significant foreign subsidies on the EU market. For mergers and acquisitions, notification generally requires both an EU turnover threshold of at least €500 million for the relevant acquired undertaking, merging undertaking, or joint venture, and combined foreign financial contributions exceeding €50 million over the preceding three years. For public procurement, the principal thresholds are an estimated contract value of at least €250 million and foreign financial contributions of at least €4 million from an individual third country over that period.

The distinction between foreign financial contributions and foreign subsidies is central to industry concerns. Companies may need to identify and track broad categories of government-related transactions to assess notification obligations even where those transactions do not confer a selective benefit or distort competition. Although reporting exemptions and waivers exist, U.S. firms continue to face substantial group-wide information-gathering costs, repeated information requests, confidentiality concerns, and transaction uncertainty.

The Commission adopted final FSR guidelines on January 9, 2026, and published its implementation review on July 14, 2026.⁴⁴⁶ The guidelines address distortion, the balancing test, and the calling-in of below-threshold transactions and procurement procedures, but do not eliminate the underlying notification framework. CCIA urges the U.S. government to seek meaningful simplification, proportionate information requests, clearer materiality thresholds and exemptions, protection of confidential information, and reduced duplication for companies making repeated filings.

⁴⁴⁵ European Parliament and Council of the European Union. (2022, December 14). *Regulation (EU) 2022/2560 on foreign subsidies distorting the internal market*, Article 54.

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2560>

⁴⁴⁶ European Commission. (2026, July 14). *Review finds Foreign Subsidies Regulation fit for purpose, Commission considers targeted changes* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1606

The EU adopted the Corporate Sustainability Due Diligence Directive (CS3D) in 2024 and substantially amended it through the Omnibus I package in 2026.⁴⁴⁷ The amendments narrowed its scope, including by establishing a €1.5 billion EU-turnover threshold for large non-EU companies, subject to the directive's detailed scope rules. Member States must transpose the amended requirements by July 26, 2028, with the main company obligations applying from July 26, 2029.

Companies within scope must still address adverse human-rights and environmental impacts in their operations, subsidiaries, and chains of activities, including outside the EU. These obligations can require substantial changes to global compliance systems and business relationships. The amendments capped pecuniary penalties at 3% of net worldwide turnover and removed the harmonized EU civil-liability regime, although liability under national law remains relevant. CCIA urges the U.S. government to seek proportionate implementation, clear limits on information requests and value-chain obligations, and coordination that reduces conflicting requirements for U.S. businesses.

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, adopted in May 2025, establishes a €150 billion loan instrument supporting defense procurement.⁴⁴⁸ Its eligibility rules generally require contractors and covered subcontractors to be established and have executive management in the EU, an EEA EFTA state, or Ukraine, and not be subject to third-country control. Components originating outside those territories generally may not exceed 35% of the estimated cost of the end product's components. These establishment, control, and content requirements can restrict participation by U.S. defense and dual-use technology suppliers. The European Defence Industry Programme (EDIP) received final Council approval on December 8, 2025, providing €1.5 billion in grants for 2025–2027.⁴⁴⁹ The adopted framework includes restrictions on the origin of components, generally limiting components from outside the EU and associated countries to 35% of total component costs, with specific provisions for the Ukraine Support Instrument. These requirements further constrain opportunities for U.S. suppliers to participate in EU-supported defense procurement. 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

⁴⁴⁷ European Parliament and Council of the European Union. (2026, February 24). *Directive (EU) 2026/470 amending Directives 2006/43/EC, 2013/34/EU, (EU) 2022/2464 and (EU) 2024/1760 as regards certain corporate sustainability reporting requirements and certain corporate sustainability due diligence requirements*. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32026L0470>

⁴⁴⁸ Council of the European Union. (2025, May 27). *Council Regulation (EU) 2025/1106 establishing the Security Action for Europe (SAFE) through the Reinforcement of the European Defence Industry Instrument*, Articles 1 and 4–6. <https://eur-lex.europa.eu/eli/reg/2025/1106/oj/eng>

⁴⁴⁹ Council of the European Union. (2025, December 8). *European Defence Industry Programme: Council gives final approval* [Press release]. <https://www.consilium.europa.eu/en/press/press-releases/2025/12/08/european-defence-industry-programme-council-gives-final-approval/>

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 Commission's proposed 2028-2034 Multiannual Financial Framework would provide €131 billion for defense, security, and space through the European Competitiveness Fund.⁴⁵⁰ The final allocation and associated eligibility conditions remain subject to negotiations. 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.

The EU is preparing a full revision of its Defense Procurement Directive, with a legislative proposal scheduled for Q4 2026. In November 2025, the EC launched a call for evidence and public consultation on the proposal, with the direction pointing towards stronger 'European preference' provisions. The revision is widely expected to align the Directive with the preference logic already embedded in the EU's defense funding instruments, such as SAFE and EDIP. Carrying this logic into the general procurement rulebook would extend conditions that currently apply only to EU-funded contracts across the wider defense market. For U.S. providers, this could mean several structural barriers. Preference criteria modelled on SAFE and EDIP would favor entities from eligible countries, and require U.S.-owned suppliers and their EU subsidiaries to demonstrate freedom from foreign control to qualify.

U.S. small businesses selling goods into the EU face extended producer responsibility requirements that vary across Member States and product categories, including separate registration, reporting and compliance obligations. This model originated in the 2019 Market Surveillance Regulation, was subsequently extended to a much broader range of consumer products under the General Product Safety Regulation, and could be expanded or reinforced further through the European Product Act. Some national regimes also require producers established outside the EU to appoint a locally established authorised representative, creating significant fixed costs even for SMEs selling only small volumes cross-border. While the EU is pursuing simplification of EPR requirements, current proposals may preserve greater burdens for third-country producers. For U.S. SMEs selling directly to EU consumers, particularly sellers of second-hand, refurbished, collectible or low-volume goods, appointing an authorised representative or otherwise securing an EU-based responsible operator can create significant fixed costs and administrative barriers disproportionate to their level of trade.

The European Commission is preparing a European Product Act to update EU product compliance and market surveillance rules. Early Commission drafting raises particular concerns for U.S. sellers of second-hand and refurbished goods, which could continue to be treated

⁴⁵⁰ European Commission. (n.d.). *EU budget 2028–2034*.
https://commission.europa.eu/strategy-and-policy/eu-budget/long-term-eu-budget/eu-budget-2028-2034_en

similarly to newly manufactured products entering the EU despite sellers often lacking access to original technical documentation or the manufacturer. The approach could also make marketplace distribution dependent on manufacturer-controlled credentials, potentially giving manufacturers significant influence over downstream and secondary-market circulation. Proposed systematic pre-listing verification requirements could create additional barriers for U.S. SMEs using marketplaces to reach EU consumers and risk undermining the intermediary limited-liability framework established by the Digital Services Act. The draft also envisages a new EU market surveillance fee on products imported from third countries, adding a further cost specifically to cross-border trade.

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 (e.g., recycling) 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.”⁴⁵¹ 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.⁴⁵²

EU changes to customs procedures have introduced additional costs and responsibilities for cross-border e-commerce. The EU intends to abandon its duty exemption for low-value parcels, with implementation targeting 2028. In the meantime (since July 1, 2026), qualifying low-value consignments worth up to €150 are subject to a temporary €3 customs duty applied to each item or set of items falling within a specific tariff line classification.⁴⁵³ Separately, the new Union Customs Code adopted on September 20, 2026 provides for an EU-wide handling fee by November 1, 2026, with its amount expected at €2 per line item.⁴⁵⁴ The reform also establishes a

⁴⁵¹ von der Leyen, U. (2025, September 10). *2025 State of the Union address by President von der Leyen* [Speech]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/speech_25_2053

⁴⁵² World Trade Organization. (2012, March 30). *Agreement on Government Procurement (as amended)*. https://www.wto.org/english/docs_e/legal_e/rev-gpr-94_01_e.htm

⁴⁵³ Council of the European Union. (2026, February 11). *Council gives final green light to new customs duty rules for small parcels*. <https://www.consilium.europa.eu/en/press/press-releases/2026/02/11/council-gives-final-green-light-to-new-customs-duty-rules-for-small-parcels/>

⁴⁵⁴ Council of the European Union. (2026, September 22). COMMISSION DELEGATED REGULATION (EU) .../... of 21.9.2026 supplementing Regulation (EU) 2026/2108 of the European Parliament and of the Council by establishing the amount of the Union handling fee. <https://data.consilium.europa.eu/doc/document/ST-13480-2026-INIT/en/pdf>

new “importer for distance sales” framework, under which either the seller or the platform facilitating the sale may assume the importer role, entailing extensive importer responsibilities for covered online platforms, such as customs formalities and duty payments, alongside a phased transition to an EU Customs Data Hub.

These measures increase costs and administrative burdens for U.S. exporters and online marketplaces, particularly smaller sellers relying on low-value shipments of second-hand, vintage, collectible, or other unique goods. Considerable uncertainty remains around the implementation of several provisions, most notably customs warehousing for distance sales, leaving compliance obligations unclear and creating legal risks for affected businesses. CCIA urges transparent and proportionate implementation, avoidance of duplicative charges, and platform obligations that reflect the information and control platforms possess over individual transactions.

France

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In March 2022, ANSSI, the French cybersecurity authority, updated its SecNumCloud qualification framework to include restrictions on non-EU ownership and control of qualifying cloud service providers. These requirements discriminate against U.S. suppliers seeking to serve customers that require SecNumCloud-qualified services, including covered French public-sector customers.⁴⁵⁵ 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).⁴⁵⁶ The certification standard is no longer voluntary—tenders have been published with SecNumCloud verification as a requirement.⁴⁵⁷ The only companies verified to date under SecNumCloud have been French.⁴⁵⁸ 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

⁴⁵⁵ ANSSI. (2022, March 9). *L'ANSSI actualise le référentiel SecNumCloud*.

<https://cyber.gouv.fr/actualites/lanssi-actualise-le-referentiel-secnumcloud>

⁴⁵⁶ ITIF. (2021). *SecNumCloud 3.2.a*. <https://www2.itif.org/2021-secnumcloud-3.2.a-english-version.pdf>

⁴⁵⁷ Official Journal of the European Union. (n.d.). 399127-2022 – *Competition*.

<https://ted.europa.eu/udl?uri=TED:NOTICE:399127-2022:TEXT:EN:HTML>

⁴⁵⁸ ANSSI. (2025). *Liste des produits et services qualifiés*.

<https://cyber.gouv.fr/prestataires-de-services-dinformatique-en-nuage-secnumcloud>

subsequently declaring when SecNumCloud would be required.⁴⁵⁹ Further, some legislators are trying to expand certification requirements in subsequent legislation to health data.⁴⁶⁰

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.⁴⁶¹ This justification is patently pretextual, given that the EU has also established a framework for cross-border access to electronic evidence. Regulation (EU) 2023/1543, applicable from August 18, 2026, enables competent judicial authorities to issue European Production and Preservation Orders to covered service providers through designated establishments or legal representatives in another participating Member State.⁴⁶² Its existence reinforces the need to assess government-access risks through the applicable legal protections rather than treating a provider’s nationality as a sufficient proxy for security.

France is bound by the EU’s applicable commitments under the WTO Government Procurement Agreement (GPA) and General Agreement on Trade in Services (GATS).⁴⁶³ For procurement covered by the GPA, Article IV prohibits less favorable treatment of a locally established supplier based on foreign affiliation or ownership, subject to the agreement’s coverage and exceptions. SecNumCloud’s ownership restrictions are facially inconsistent with that obligation, and it is unlikely that the relevant exception would justify France’s practices.⁴⁶⁴ In addition to the existing discrimination, legislative amendments that would extend SecNumCloud ownership requirements to private entities active in the healthcare and other critical 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.

⁴⁵⁹ French Ministry of the Economy, Finance, and Industrial and Digital Sovereignty. (2022, September 12). *Cloud : Cinq nouveaux dispositifs pour soutenir le développement du secteur*.

<https://www.economie.gouv.fr/cloud-cinq-nouveaux-dispositifs-soutenir-developpement-secteur>.

⁴⁶⁰ Assemblée nationale. (2023). *Amendement No. CS765*.

<https://www.assemblee-nationale.fr/dyn/16/amendements/1514/ESPNUM/765>.

⁴⁶¹ 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/>.

⁴⁶² European Parliament and Council of the European Union. (2023, July 12). *Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings*, Articles 1, 4, 7, and 34.

<https://eur-lex.europa.eu/legal-content/EN/TEXT/PDF/?uri=CELEX:32023R1543>.

⁴⁶³ World Trade Organization. (n.d.). *Agreement on Government Procurement: Parties and observers*.

https://www.wto.org/english/tratop_e/gproc_e/memobs_e.htm; European Communities and their Member States. (1994, April 15). *Schedule of specific commitments under the General Agreement on Trade in Services (GATS/SC/31)*. <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=O:/SCHD/GATS-SC/SC31.pdf>.

⁴⁶⁴ World Trade Organization. (2012, March 30). *Agreement on Government Procurement (as amended)*, Article IV(2)(b). https://www.wto.org/english/docs_e/legal_e/rev-gpr-94_01_e.pdf.

On May 24, 2024 France enacted Law No. 2024-449, a sweeping law to regulate multiple aspects of digital services (*Sécuriser et Réguler l'Espace Numérique* –SREN).⁴⁶⁵ Its cloud provisions regulate specified commercial practices and establish interoperability, data portability, and interface-access obligations, with enforcement powers assigned to its telecommunications regulator, Arcep. On September 25, 2025, Arcep issued a nonbinding recommendation on cloud interoperability and portability, expressly distinguishing that guidance from existing statutory obligations.⁴⁶⁶ The relevant national interoperability provisions apply only until January 12, 2027. The law includes certain provisions that would impose significant fines on a list of allegedly unfair practices by CSPs or mandate a certain level of interoperability between these services. Article 31 of the enacted SREN Law establishes security and protection requirements for particularly sensitive data entrusted to private cloud providers by State administrations, State operators, and specified public-interest groupings. Decree No. 2026-272 of April 14, 2026 implements this provision through requirements addressing data-hosting location, provider establishment, ownership and voting control, and protection against unauthorized access by third-country authorities.⁴⁶⁷ An August 12, 2026 order subsequently approved the applicable cloud-provider requirements framework.⁴⁶⁸ These requirements deepen market-access concerns for U.S. cloud suppliers by further extending SecNumCloud's restrictions of corporate ownership and jurisdiction as eligibility factors for handling covered public-sector data.

Discriminatory Local Content Quotas and Audiovisual Service Mandates

France requires covered subscription video-on-demand services, including foreign services targeting France, to contribute at least 20% of their annual net French revenues to European or original French-language cinematographic and audiovisual production.⁴⁶⁹ The minimum rises to 25% for services offering films less than 12 months after their French theatrical release. For example, in September 2025, Arcom approved an amendment allowing Disney+ to offer films nine months after theatrical release, with a contribution set at 25% of annual French revenues

⁴⁶⁵ 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>

⁴⁶⁶ Arcep. (2025, September 25). *Recommandation relative à l'interopérabilité et à la portabilité des services d'informatique en nuage*.

https://www.arcep.fr/uploads/tx_gspublication/recommandation-interoperabilite-portabilite-cloud_sept2025.pdf

⁴⁶⁷ French Government. (2026, April 14). *Décret n° 2026-272 du 14 avril 2026 relatif à la protection des données d'une sensibilité particulière des administrations, opérateurs et groupements d'intérêt public de l'Etat traitées par un service d'informatique en nuage fourni par un prestataire privé*, Article 2.

<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000053900789>

⁴⁶⁸ French Government. (2026, August 12). *Arrêté du 12 août 2026 portant approbation du référentiel d'exigences relatif aux prestataires de services d'informatique en nuage*, Article 1.

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000054678082>

⁴⁶⁹ French Government. (2021, June 22). *Décret n° 2021-793 du 22 juin 2021 relatif aux services de médias audiovisuels à la demande*, Articles 2, 10, and 14 (as amended).

<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000043688681/>

and a minimum investment of €205 million over three years.⁴⁷⁰ These requirements constrain investment allocation and release strategies for affected U.S. services.

Decree No. 2025-1421 of December 30, 2025 further constrains the allocation of audiovisual investment,⁴⁷¹ requiring at least 20% of the audiovisual production contribution to support animation, creative documentaries, or recordings or recreations of live performances. For services with annual net revenues exceeding €50 million, at least 75% of the allocation to each of those genres must support new works.

France separately imposes taxes on paid on-demand audiovisual service (TSV-P) and advertising and sponsorship associated with free or user-generated service (TSV-G), generally at a rate of 5.15%.⁴⁷² The measures cover services supplied to users in France, including by providers established abroad, and finance the National Center for Cinema and the Moving Image (CNC). For qualifying free services principally providing access to user-created audiovisual content, the TSV-G currently includes a 66% reduction in the relevant taxable revenues and a €100,000 allowance. The National Assembly's July 2026 report records 2025 receipts of €45.5 million from TSV-G and €155.1 million from TSV-P. Although the regimes cover French suppliers, CCIA identifies a disproportionate burden on U.S. platforms, who are also put at a competitive disadvantage vis-a-vis their competitors in linear TV, dominated by French suppliers.

The National Assembly report recommends eliminating the TSV-G's 66% reduction for qualifying free user-generated-content services. This would increase the share of qualifying revenues included in the tax base from 34% to 100%, while retaining the 5.15% statutory rate. The report estimates that removing the reduction would generate more than €70 million in additional annual revenue for the CNC. CCIA opposes this proposal because it would substantially increase the burden on predominantly U.S. platforms and shift additional financing of France's audiovisual sector onto digital services.⁴⁷³

Separately, Recommendation No. 7 proposes revising the definition of taxable audiovisual access services to expressly encompass distribution models including live streaming, continuous short-video feeds, and algorithmic recommendations. Although presented as a clarification, this could materially broaden the reach of both TSV-G and TSV-P. CCIA urges France to reject this

⁴⁷⁰ Arcom. (2025, September 19). *Arcom adopts amendment to Disney+ service agreement*. <https://www.arcom.fr/en/press/arcom-adopts-amendment-disney-service-agreement>

⁴⁷¹ French Government. (2025, December 30). *Décret n° 2025-1421 du 30 décembre 2025 modifiant le décret n° 2021-793 du 22 juin 2021 relatif aux services de médias audiovisuels à la demande*, Article 1. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000053228669>

⁴⁷² Masségli, D. (2026). *Communication en conclusion des travaux de la mission d'information flash sur les taxes sur les services vidéo*. Assemblée nationale. https://www.assemblee-nationale.fr/dyn/17/documents/tsv/117n462658460_document.pdf

⁴⁷³ CCIA. (2026, August 28). *France's Video-Sharing Platform Tax Risks Further Discriminatory Taxation of U.S. Digital Services*. <https://ccianet.org/library/frances-video-sharing-platform-tax-risks-further-discriminatory-taxation-of-u-s-digital-services/>

expansion or establish explicit exclusions for non-audiovisual transactions and clear allocation rules for mixed services. These recommendations remain proposals but merit close monitoring.

Proposals to increase video-platform taxation follow tax relief for traditional television broadcasters. Article 84 of the 2026 Finance Law excludes advertising-sales agency fees from the television-services tax base and extends a €30 million allowance to qualifying services.⁴⁷⁴ The parliamentary video-tax report expressly links broadcaster relief to the need to diversify CNC funding. CCIA is concerned that increasing platform taxes in this context would shift more of France's audiovisual financing burden onto predominantly foreign digital suppliers. USTR should oppose discriminatory funding arrangements that disadvantage U.S. platforms relative to domestic broadcasters.

The parliamentary report also recommends raising the TSV-P exemption threshold to €1 million, calculated using a three-year rolling average, aiming to support small French platforms. Although the proposed threshold is expressed in revenue terms rather than nationality, that stated objective warrants scrutiny alongside proposals increasing burdens on larger, predominantly U.S. suppliers. CCIA urges USTR to assess the combined competitive effects of these changes.⁴⁷⁵

Article 83 of the 2026 Finance Law separately changes TSV-P liability from January 1, 2027. Although these provisions seek to avoid taxing intermediaries on amounts passed onward, implementation must clearly identify liable parties and coordinate reporting across the payment chain. CCIA urges USTR to seek guidance preventing inconsistent allocations and duplicate assessments.

CCIA urges USTR to oppose the proposed expansion of video taxation to additional digital distribution models. Any implementing legislation should expressly exclude payments unrelated to audiovisual access, including genuine donations, tipping, virtual goods, messaging, gaming, and other non-audiovisual benefits. Any intermediary tax liability should be limited to consideration retained and attributable to that component, with coordinated reporting to prevent double counting. Merely processing a payment or distributing an application should not automatically make an intermediary liable for another supplier's audiovisual service.

France's Finance Law for 2024 introduced a tax on qualifying online music-streaming services effective January 1, 2024.⁴⁷⁶ The rate remains 1.2% for covered revenue exceeding €20 million. The base includes relevant payments by users in France, excluding VAT, and 34% of qualifying

⁴⁷⁴ French Government. (2026, February 19). *Loi n° 2026-103 du 19 février 2026 de finances pour 2026*, Article 84. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000053508155>

⁴⁷⁵ CCIA. (2026). *Changes to France's Video Streaming Tax Risks Exacerbating Discrimination on U.S. Digital Services*. <https://ccianet.org/wp-content/uploads/securepdfs/2026/08/Francis-Video-Sharing-Platform-Tax-Risks-Further-Discriminatory-Taxation-of-U.S.-Digital-Services.pdf>

⁴⁷⁶ French Government. (2023). *Loi n° 2023-1322 du 29 décembre 2023 de finances pour 2024*, Articles 1 and 53. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048727345>

advertising and sponsorship receipts. Covered providers may be established in France or abroad, and qualifying social-media services may also fall within scope.

The proceeds of this tax support the Centre National de la Musique, subject to an annual allocation ceiling (which some stakeholders are seeking to increase). In March 2024, Spotify announced that it would increase French subscription prices in response to the tax, illustrating its negative effect on consumers and the music industry.⁴⁷⁷ Even though collections this year are expected to be double the original 2024 amounts (*i.e.*, exceeding €20 M), the National Assembly Finance Committee recently initiated a study of the online music sector that appears designed to lay the groundwork for additional intervention, including higher taxes. CCIA urges USTR to engage with France on the cumulative burden on U.S. suppliers and assess whether the measure's design or application produces discriminatory effects, by targeting U.S. firms and excluding their French competitors.

During consideration of the 2025 and 2026 Finance Bills, French lawmakers proposed extending the existing tax on telecommunications to very large online platforms (including search services) designated under the EU's Digital Services Act.⁴⁷⁸ These proposals sought to extend the existing 1.3% levy, applicable to the taxable base exceeding €5 million, to additional digital suppliers.⁴⁷⁹ The Senate adopted an amendment during consideration of the 2025 Finance Bill despite government opposition but the amendment ultimately failed. Renewed proposals would risk adding overlapping turnover-based obligations for affected suppliers. The explanatory statement accompanying the Senate's 2025-budget amendment expressly identified Google, Apple, Facebook, Amazon, and Microsoft as intended targets.⁴⁸⁰

Forced Revenue Transfers for Digital News

In 2019, while in the process of implementing Article 15 of the EU Copyright Directive, 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.⁴⁸¹ In April 2020, the French competition authority ordered Google to negotiate in good faith with requesting press publishers and agencies over remuneration for the use of protected content, while maintaining

⁴⁷⁷ Spotify. (2024). <https://newsroom.spotify.com/2024-03-07/spotify-to-adjust-its-prices-over-new-tax-in-france/>.

⁴⁷⁸ Assemblée nationale. (2025, October 21). *Projet de loi de finances pour 2026 : Amendement n° I-1983*. <https://www.assemblee-nationale.fr/dyn/17/amendements/1906A/AN/1983>

⁴⁷⁹ *Projet de Loi de finances pour 2025* [France] No. 39. (2024). <https://www.senat.fr/petite-loi-ameli/2024-2025/143.html>.

⁴⁸⁰ 1stopVAT. (2024, November 26). *France – Increase of Digital Services Tax 2025*. <https://1stopvat.com/france-increase-of-digital-services-tax-2025/>

⁴⁸¹ Gingras, R. (2019, September 25). *How Google invests in news*. The Keyword. <https://www.blog.google/perspectives/richard-gingras/how-google-invests-news/>

the display of that content during negotiations.⁴⁸² In October 2020, Google and the “Alliance de la Presse d’Information Générale,” which represents newspapers such as Le Monde, announced agreement on a framework for payments linked to criteria such as the publisher’s audience, non-discrimination and the publisher’s contribution to political and general information.⁴⁸³ Notwithstanding this agreement, in July 2021, the French competition authority imposed a €500 million fine on Google asserting that the company did not negotiate in good faith with the press industry over licensing fees.⁴⁸⁴ Enforcement has continued beyond the 2021 penalty. In June 2022, the authority accepted binding commitments from Google governing negotiations with publishers and press agencies.⁴⁸⁵ In March 2024, it announced a further €250 million fine for non-compliance with certain commitments.⁴⁸⁶ In July 2026, the authority extended this enforcement approach to Meta, imposing interim measures requiring good-faith negotiations with press publishers and agencies.⁴⁸⁷ These proceedings extend the use of competition enforcement powers to compel negotiations over news remuneration across multiple U.S. platforms.

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.⁴⁸⁸ The directive told French Ministers and their staff to instead transition to

⁴⁸² 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>

⁴⁸³ 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>

⁴⁸⁴ Autorité de la concurrence. (2021, July 13). *Rémunération des droits voisins : l’Autorité sanctionne Google à hauteur de 500 millions d’euros pour le non-respect de plusieurs injonctions*.

<https://www.autoritedelaconcurrence.fr/fr/article/remuneration-des-droits-voisins-lautorite-sanctionne-google-hauteur-de-500-millions-deuros>

⁴⁸⁵ Autorité de la concurrence. (2022, June 21). *Décision n° 22-D-13 du 21 juin 2022 relative à des pratiques mises en œuvre par Google dans le secteur de la presse*.

https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2022-06/22d13.pdf

⁴⁸⁶ Autorité de la concurrence. (2024, March 20). *Related rights: the Autorité fines Google €250 million for non-compliance with some of its commitments made in June 2022*.

<https://www.autoritedelaconcurrence.fr/en/press-release/related-rights-autorite-fines-google-eu250-million-non-compliance-some-its>

⁴⁸⁷ Autorité de la concurrence. (2026, July 8). *Droits voisins : l’Autorité de la concurrence prononce des mesures conservatoires et enjoint Meta de négocier de bonne foi avec les éditeurs et agences de presse*.

<https://www.autoritedelaconcurrence.fr/fr/article/droits-voisins-lautorite-de-la-concurrence-prononce-des-mesures-conservatoires-et-enjoint>

⁴⁸⁸ 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/>

Olvid, a messaging application of a Paris-based startup, and Tchap, a government-developed messaging and collaboration app. The directive restricted government users from accessing foreign messaging suppliers, including U.S. providers WhatsApp and Signal, while favoring French alternatives. France expanded this approach to videoconferencing in January 2026, announcing plans to generalize the State-developed Visio service across State services by 2027.⁴⁸⁹ The government expressly identified ending the use of non-European solutions as an objective and named Teams, Zoom, GoTo Meeting, and Webex among the existing tools to be supplanted. Visio is hosted by Outscale using SecNumCloud-qualified infrastructure. This policy would displace commercial services supplied by U.S. firms and further reduce their opportunities to serve French government customers. USTR is urged to evaluate these bans in light of France's WTO GPA commitments.

Like many countries, France is actively implementing a range of measures banning minors from accessing specific services and mandating age verification. On August 14, 2026, France's Constitutional Council struck down the provision establishing a general prohibition on access to social networks for children under 15.⁴⁹⁰

Article L. 333-10 of the French Sports Code⁴⁹¹ (introduced late 2021 and amended in August 2026) gives sports rights holders a fast-track legal tool to combat live piracy. Courts can order "any proportionate measure" against "any person likely to contribute to remedying" the infringement. Rights holders have used the Code to obtain court orders to block access to content against ISPs, DNS providers, Content Delivery Network (CDN) providers, and VPN providers. The dynamic orders under the system impose continuous operational obligations on targeted intermediaries, many of whom are U.S. providers. The impact of blocking orders on global providers is disproportionate to the intended effect, in particular in the case of public DNS resolvers, where a block will have an extraterritorial effect, and creates risks of overblocking and impacts on freedom of expression online.

⁴⁸⁹ French Government. (2026, January 26). *Souveraineté numérique : l'État généralise « Visio », sa solution de visioconférence sécurisée et souveraine à destination des agents publics*. <https://presse.economie.gouv.fr/souverainete-numerique-letat-generalise-visio-sa-solution-de-visioconference-securisee-et-souveraine-a-destination-des-agents-publics/>

⁴⁹⁰ Conseil constitutionnel. (2026, August 14). *Décision n° 2026-911 DC du 14 août 2026*. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000054743009>

⁴⁹¹ France National Assembly. (2021) *Article L333-10, Modifié par LOI n°2026-725 du 3 août 2026 - art. 31*. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000045294025

Challenges to the Development of AI

On June 28, 2024, the French Competition Authority published Opinion No. 24-A-05 on competition in generative artificial intelligence.⁴⁹² The opinion identified risks involving computing resources, cloud services, and data access, and recommended considering whether providers of model-as-a-service offerings could be designated under the Digital Markets Act. In July 2026, the authority published a further opinion on AI agents, recommending implementation of existing regulatory frameworks, scrutiny of AI distribution channels, and greater interoperability and portability.⁴⁹³ These opinions are advisory and do not themselves establish new binding obligations but USTR should monitor their implementation for measures that impose disproportionate burdens on U.S. AI suppliers or restrict their ability to offer integrated services.

Separately, the French data protection authority, CNIL in June 2025 recommendations, articulated an interpretation of the privacy principle of a data controller's legitimate interest to support AI development, subject to necessity, a balancing of interests, and appropriate safeguards.⁴⁹⁴ They also identify circumstances in which collecting publicly accessible personal data for AI training may fall outside individuals' reasonable expectations, including where websites clearly oppose scraping through robots.txt or CAPTCHA restrictions. These interpretations affect access to training data and compliance requirements for AI developers operating in France.

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.⁴⁹⁵ The tax applies to covered services where annual revenues exceed both €750 million worldwide and €25 million attributable to France, assessed at group level where applicable. These thresholds disproportionately capture leading U.S. technology firms while excluding many smaller French suppliers of comparable services. French Finance Minister Bruno Le Maire regularly referred to

⁴⁹² Autorité de la concurrence. (2024, June 28). *Generative artificial intelligence: the Autorité issues its opinion on the competitive functioning of the sector.*
<https://www.autoritedelaconcurrence.fr/en/press-release/generative-artificial-intelligence-autorite-issues-its-opinion-competitive>

⁴⁹³ Autorité de la concurrence. (2026, July 17). *Agents d'IA : l'Autorité de la concurrence rend son avis sur le fonctionnement concurrentiel du secteur des agents d'intelligence artificielle.*
<https://www.autoritedelaconcurrence.fr/fr/communiqués-de-presse/agents-dia-lautorite-de-la-concurrence-rend-son-avis-sur-le-fonctionnement>

⁴⁹⁴ Commission nationale de l'informatique et des libertés (CNIL). (2025, June 19). *Développement des systèmes d'IA : la CNIL publie ses recommandations sur l'intérêt légitime.*
<https://www.cnil.fr/fr/recommandations-developpement-ia-interet-legitime>

⁴⁹⁵ French Government. (2019, July 24). *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.*
<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038811588>

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.⁴⁹⁶ 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.⁴⁹⁷ Based on French officials’ own statements, the majority of firms that pay the tax are American.⁴⁹⁸ France’s official budget documentation reports €785 million in DST receipts for 2024⁴⁹⁹ and forecasted €891 million for 2025 and €882 million for 2026.⁵⁰⁰ During consideration of the 2026 Finance Bill, the National Assembly’s Finance Committee adopted Amendment CF1827, proposing to raise the DST rate from 3% to 15% and the worldwide covered-services revenue threshold from €750 million to €2 billion, while leaving the €25 million French-revenue threshold unchanged.⁵⁰¹ Its explanatory statement identified the GAFAM companies as intended targets.⁵⁰² On September 12, 2025, the Constitutional Council upheld the challenged DST provisions in Decision No. 2025-1157 QPC. That decision addressed French constitutional objections; it did not address international trade concerns.⁵⁰³ CCIA supported USTR’s 2019 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. USTR initially suspended the additional duties associated with its French DST investigation and subsequently terminated that tariff action in November 2021 following the political agreement on transitional treatment of existing digital services taxes linked to OECD proposals.⁵⁰⁴ With France’s DST remaining in place, and uncertain prospects for a multilateral solution, CCIA urges USTR to assess whether renewed action under Section 301 is now warranted.

⁴⁹⁶ CCIA. (2020, July 14). *Comments of the Computer & Communications Industry Association in re Initiation of Section 301 Investigations of Digital Services Taxes*, Docket No. USTR-2020-0022. <https://ccianet.org/wp-content/uploads/2020/07/Comments-of-CCIA-USTR-2020-0022-Section-301-Digital-Service-s-Taxes-.pdf>

⁴⁹⁷ French Government. (n.d.). *Le projet de loi de finances 2019*. <https://www.gouvernement.fr/action/le-projet-de-loi-de-finances-2019>; Assemblée nationale. (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/15cion_fin1819064_compte-rendu

⁴⁹⁸ 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>

⁴⁹⁹ Direction du Budget. (2025). *Évaluation des voies et moyens : Annexe au projet de loi de finances pour 2026 — Tome I : Recettes*. <https://www.budget.gouv.fr/documentation/file-download/30583>

⁵⁰⁰ 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/>

⁵⁰¹ Assemblée nationale. (2025, October 18). *Projet de loi de finances pour 2026 : Amendement n° I-CF1827*. https://www.assemblee-nationale.fr/dyn/17/amendements/1906A/CION_FIN/CF1827

⁵⁰² Assemblée nationale. (2025). *Amendement n° I-CF1827*. https://www.assemblee-nationale.fr/dyn/17/amendements/1906A/CION_FIN/CF1827

⁵⁰³ Conseil constitutionnel. (2025, September 12). *Décision n° 2025-1157 QPC du 12 septembre 2025*. <https://www.conseil-constitutionnel.fr/decision/2025/20251157QPC.htm>

⁵⁰⁴ Office of the United States Trade Representative. (2021, November 18). *Termination of Actions in the Section 301 Digital Services Tax Investigations of Austria, France, Italy, Spain, and the United Kingdom and Further Monitoring*. <https://www.govinfo.gov/content/pkg/FR-2021-11-18/pdf/2021-25199.pdf>

Other Digital Trade Barriers

France’s private copying levy, established by law on July 3, 1985, compensates rights holders for the copyright exception that permits private, personal-use copying of protected works under Article L.122-5(2) of the French Intellectual Property Code; the levy is collected by Copie France on blank recording media and storage devices, with manufacturers, importers, and other entities placing covered products on the French market responsible for declaration and payment regardless of where the products originate. The costs are ultimately borne by consumers, including businesses acquiring such equipment for professional use. Of the amounts collected, 75% is distributed to rights holders and 25% funds cultural initiatives at rates set by an independent administrative commission.⁵⁰⁵ Although originally designed to address audio and video cassette recording, the scope of covered products has been periodically expanded without a corresponding reassessment of the underlying mechanism: extending in 2001 to DVD-R, CD-R, and printed works, in 2011 to external hard drives, USB drives, smartphones, and tablets, and in 2021 to refurbished smartphones and tablets—resulting in the levy being applied twice over the lifecycle of the same device. Based on the most recently available information (2022), the measure generates close to €300 million annually, three-quarters of which is from smartphones.⁵⁰⁶ As of 2026, proposals have emerged to further extend the levy to personal computers and cloud storage services that could increase the applicable levy by as much as 40%.⁵⁰⁷ Because the levy applies broadly to general-purpose consumer electronics and cloud services regardless of actual private-copying use, the proposed expansion raises concerns regarding its disproportionate impact on U.S. technology suppliers of the affected devices and services.

Germany

Asymmetric Platform Regulation

Under the 2021-amended Gesetz gegen Wettbewerbsbeschränkungen (GWB) addressing restraints of trade, there is a two-step procedure: the German Federal Cartel Office (FCO) first designates companies deemed to have “paramount importance for competition across markets” under Section 19(a)(1); and can then prohibit such companies, even as a preventive measure,

⁵⁰⁵ France National Assembly. (2023). *Code de la Propriété Intellectuelle*.

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000048603495

⁵⁰⁶ alloforfait.fr. 2023. *Copie Privée: un nouveau pactole empoché en 2022*.

<https://alloforfait.fr/actualites/118293-copie-privee-nouveau-pactole-empoché-2022.html>

⁵⁰⁷ Ifrro. (2016). *Proposal to extend Private Copying Levy to some Cloud Services*.

<https://ifrro.org/page/article-detail/france-government-and-senate-support-proposal-to-extend-private-copying-levies-to-some-cloud-services-2832/>.

from carrying out certain presumptively abusive actions (e.g., self-preferencing) under Section 19(a)(2).⁵⁰⁸ 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). While companies can seek to justify presumptively abusive 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.

The FCO has designated five U.S.-headquartered companies—Alphabet/Google,⁵⁰⁹ Amazon,⁵¹⁰ Meta,⁵¹¹ Apple,⁵¹² and Microsoft⁵¹³—as having paramount significance for competition across markets under Section 19a(1). No German or non-U.S. company has been designated. In addition to the questionable targeting of U.S. firms, CCIA is concerned that possible restrictions imposed on designated companies may prevent practices that benefit consumers and remain available to competitors. USTR should assess the competitive effects and justification of particular obligations and enforcement decisions affecting U.S. suppliers.

In January 2026, Germany completed the statutory evaluation of Section 19a.⁵¹⁴ CCIA has raised concerns that the evaluation proceeded without a formal consultation gathering input from

⁵⁰⁸ Federal Republic of Germany. (n.d.). *Gesetz gegen Wettbewerbsbeschränkungen (GWB), § 19a: Missbräuchliches Verhalten von Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb*.

https://www.gesetze-im-internet.de/gwb/_19a.html

⁵⁰⁹ German Federal Cartel Office. (2022, January 5). *Alphabet/Google subject to new abuse control applicable to large digital companies – Bundeskartellamt determines “paramount significance across markets”*.

https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/05_01_2022_Google_19a.html

⁵¹⁰ 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

⁵¹¹ 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

⁵¹² 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/>

⁵¹³ 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

⁵¹⁴ German Federal Ministry for Economic Affairs and Energy. (n.d.). Bericht gemäß § 19a Absatz 4 des Gesetzes gegen Wettbewerbsbeschränkungen.

https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Downloads/E/20260107-evaluation-19a-gwb.pdf?__blob=publicationFile.

affected companies and other stakeholders.⁵¹⁵ Given the overlapping application of Section 19a and the EU Digital Markets Act, a transparent assessment should examine duplicative compliance obligations, consistency between national and EU enforcement, and the effects on innovation and U.S. suppliers' competitive opportunities.

On February 5, 2026, the FCO prohibited Amazon from applying certain price-control mechanisms to third-party offers on its German marketplace and ordered the disgorgement of approximately €59 million in economic benefits.⁵¹⁶ CCIA is concerned that restrictions on tools used to identify competitive offers can impair the consumer experience and constrain a U.S. supplier's ability to compete through its marketplace services. Compounding these concerns is the fact that the EU's competition authority previously accepted such practices as legal, underscoring the unreasonableness of the FCO action.

Germany has also completed the statutory evaluation of Section 19a.⁵¹⁷ CCIA has raised concerns that the evaluation proceeded without a formal consultation gathering input from affected companies and other stakeholders.⁵¹⁸ Given the overlapping application of Section 19a and the EU Digital Markets Act, a transparent assessment should examine duplicative compliance obligations, consistency between national and EU enforcement, and the effects on innovation and U.S. suppliers' competitive opportunities.

On August 17, 2026, the FCO finalized enforcement action relating to Apple's App Tracking Transparency Framework.⁵¹⁹ As a result, closer alignment of advertising-consent prompts, Apple's own services, and third-party apps will be instituted, allowing greater flexibility for developers to combine consent requests. The proceeding illustrates how Germany's competition regime can require changes to a U.S. supplier's product design and privacy-related interfaces.

A further amendment to the GWB in November 2023, the 11th Amendment, significantly expanded the powers of the FCO in three key areas, heightening U.S. industry concerns over

⁵¹⁵ Computer & Communications Industry Association. (2026, March). Germany's barriers to U.S. digital services suppliers. <https://ccianet.org/wp-content/uploads/2026/03/2026-03-11-Germanys-Barriers-to-U.S.-Digital-Services-Suppliers-Caroline-Palmer.pdf>.

⁵¹⁶ German Federal Cartel Office. (2026, February 5). *Bundeskartellamt prohibits Amazon from applying so-called price control mechanisms and orders the disgorgement of 59 million euros in economic benefits.* https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2026/02_05_26_Amazon.html

⁵¹⁷ German Federal Ministry for Economic Affairs and Energy. (n.d.). Bericht gemäß § 19a Absatz 4 des Gesetzes gegen Wettbewerbsbeschränkungen. https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Downloads/E/20260107-evaluation-19a-gwb.pdf?__blob=publicationFile

⁵¹⁸ Computer & Communications Industry Association. (2026, March). Germany's barriers to U.S. digital services suppliers. <https://ccianet.org/wp-content/uploads/2026/03/2026-03-11-Germanys-Barriers-to-U.S.-Digital-Services-Suppliers-Caroline-Palmer.pdf>

⁵¹⁹ German Federal Cartel Office. (2026, August 17). *Apple changes its rules for personalised advertising in apps.* https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2026/08_17_2026_Apple_ATTF.html

Germany's competition regime.⁵²⁰ First, the FCO was granted authority to impose behavioral or structural remedies following a sector inquiry identifying a significant and continuing disturbance of competition, even without a specific antitrust violation, where its other competition-law powers would likely be insufficient. Second, the amendment introduced a rebuttable presumption that specified infringements generate an economic benefit of at least 1% of domestic sales of the products or services connected with the infringement during the disgorgement period, which may not exceed five years. The statute provides limited grounds for rebuttal and caps the amount payable at 10% of the undertaking's total turnover in the preceding financial year. 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.

Effective April 1, 2026, Germany further amended Section 32f through the Kraftstoffmaßnahmenpaket.⁵²¹ The amendment combines the finding of a competition disturbance and the imposition of remedies into a single decision, and removes the express requirement that an addressee's conduct substantially contribute to the disturbance. These changes apply across sectors, including digital markets, although enacted within a fuel-market package, and broaden the potential exposure of U.S. suppliers to remedies without a finding of an individual antitrust infringement.

Barriers to the Deployment and Operation of Network Infrastructure

U.S. digital suppliers face concerns about the cost and conditions of reaching Deutsche Telekom's internet subscribers. CCIA has identified Deutsche Telekom's paid-peering practices as a *de facto* network-usage-fee barrier.⁵²² In April 2025, consumer and digital-rights organizations submitted a complaint to the Bundesnetzagentur alleging that congestion at interconnection points controlled by DT was strategically enabled by DT to disadvantage firms that do not purchase direct connectivity⁵²³—resulting in either increased delivery costs or impaired quality of cross-border digital services (or both). CCIA urges German authorities to

⁵²⁰ German Federal Cartel Office. (2023, November 7). *Novelle des Gesetzes gegen Wettbewerbsbeschränkungen (11. GWB-Novelle)*. https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/07_11_2023_GWB-Novelle.html

⁵²¹ Federal Republic of Germany. (2026, March 31). *Gesetz zur Einführung eines Gesetzes zur Anpassung von Kraftstoffpreisen und zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen (Kraftstoffmaßnahmenpaket)*. Bundesgesetzblatt I, No. 82, Articles 2–3. https://www.recht.bund.de/bgbl/1/2026/82/regelungstext.pdf?__blob=publicationFile

⁵²² Computer & Communications Industry Association. (2026, March). *Germany's barriers to U.S. digital services suppliers*. <https://ccianet.org/wp-content/uploads/2026/03/2026-03-11-Germanys-Barriers-to-U.S.-Digital-Services-Suppliers-Caroline-Palmer.pdf>

⁵²³ epicenter.works. (2025, April 25). *Beschwerde gegen die Deutsche Telekom wegen Verletzung der Netzneutralität im Namen von Telekom-Kunden (Netzbremse.de)*. <https://epicenter.works/content/beschwerde-gegen-die-deutsche-telekom-wegen-verletzung-der-netzneutralitaet>

ensure effective oversight of interconnection practices and prevent discriminatory barriers from hindering end users' access to the internet.

Separately, on February 10, 2026, the Düsseldorf Higher Regional Court upheld Deutsche Telekom's contractual claim for more than €30 million against Meta subsidiary Edge Network Services for peering services.⁵²⁴ The court found that continued use of the connections constituted acceptance of an interim paid agreement and rejected the allegation of an abuse of dominance in that dispute. The judgment illustrates the financial exposure associated with interconnection arrangements, but did not establish a generally applicable right to impose network-usage fees.

Discriminatory Local Content Quotas and Audiovisual Service Mandates

On May 27, 2026, Germany's federal cabinet approved the draft Mediendienste-Investitionsverpflichtungs-Gesetz (MedienInvestVG), establishing a proposed investment obligation for audiovisual on-demand services targeting Germany, including foreign-established providers.⁵²⁵ The government submitted the bill to the Bundestag on September 2, 2026, with a first reading scheduled for September 24. The draft provides for entry into force as early as January 1, 2027. It would require covered commercial services to invest at least 8% of their relevant German net turnover from the penultimate calendar year in European audiovisual works. Commercial services generating less than €10 million in annual net turnover would be exempt.

Within the baseline investment obligation, at least 60% must support new European works, 80% must support European works produced in German original language, and 70% must support works made by independent producers. These overlapping sub-quotas direct spending toward specified production categories and constrain services' ability to allocate investment according to audience demand and commercial strategy.

The proposal also conditions qualifying investment in independent productions on restrictions on ownership of intellectual property. Depending on the producer's financial participation and contribution of underlying rights, qualifying agreements would limit IP ownership to three, five, or seven years, after which it would have to be transferred to a local entity. These requirements constrain the commercial negotiation of rights and may reduce the long-term value of productions financed by streaming services. Services could obtain departures from specified investment rules through qualifying arrangements with representative producer associations, subject to regulatory review, if they commit to investing at least 12% of relevant revenue. The

⁵²⁴ Oberlandesgericht Düsseldorf. (2026, February 10). *Telekom Deutschland GmbH kann von Meta-Tochterunternehmen Entgelt für Telekom-Leistungen verlangen*. <https://www.justiz.nrw/presse/2026-02-10-0>

⁵²⁵ Der Beauftragte der Bundesregierung für Kultur und Medien. (2026, May 27). *Investitionspakt und Filmbooster gehen an den Start*. <https://kulturstaatsminister.de/investitionspakt-und-filmbooster-gehen-an-den-start>

Filmförderungsanstalt would supervise compliance and could impose a compensatory levy equal to 75% of the unfulfilled investment obligation.

CCIA estimates that the 8% baseline obligation would require nearly \$2 billion in investment by major U.S. streaming services over 2027-2031.⁵²⁶ The combination of prescribed spending, content sub-quotas, and restrictions on rights allocation would constrain commercial decisions and disadvantage investment in U.S. content. In addition, the fact that predominantly U.S. streaming companies would be subject to a relinquishment of IP rights, whereas their major competitors, Germany's traditional broadcasters would not, appears inconsistent with Germany's national treatment obligations under the WTO's Trade-Related Intellectual Property Rights Agreement (TRIPS Article 3).

In August 2026 comments, the European Commission questioned aspects of the proposed investment framework, emphasizing the need for empirical evidence supporting the contribution levels and proportionality across the combined obligations.⁵²⁷ It observed that cumulative sub-quotas could significantly constrain providers' editorial and commercial choices, and that mandatory rights reversion could materially affect contractual arrangements and exploitation strategies. The Commission urged Germany to preserve sufficient commercial flexibility and ensure that the measures remain proportionate to promoting European works.

CCIA urges Germany to replace these prescriptive obligations with voluntary investment arrangements and preserve commercially negotiated rights terms. In the absence of such action, CCIA urges USTR to oppose this proposed measure and investigate it as a possible TRIPS violation.

Challenges to the Development of AI

German litigation has materially impacted copyright rules affecting U.S. generative-AI suppliers. On November 11, 2025, the Munich I Regional Court substantially upheld the German collecting society GEMA's claims against OpenAI concerning nine song lyrics, finding infringement through memorization in the models and reproduction in chatbot outputs and rejecting the text-and-data-mining defense for those uses (42 O 14139/24).⁵²⁸ On July 31, 2026, the same court substantially upheld GEMA's claims against the AI music platform Suno concerning six musical works (42 O 763/25).⁵²⁹ The Suno decision addressed infringement through models and

⁵²⁶ Computer & Communications Industry Association. (2026, June). *CCIA concerns with Germany's local investment obligation for streaming services*.

<https://ccianet.org/library/ccia-concerns-with-germanys-local-investment-obligation-for-streaming-services/>

⁵²⁷ European Commission. (2026, August 6). *Notification 2026/260/DE: Delivery of comments pursuant to Article 5(2) of Directive (EU) 2015/1535*. C(2026) 5785 final.

<https://technical-regulation-information-system.ec.europa.eu/en/notification/27977/message/116632/EN>

⁵²⁸ Landgericht München I. (2025, November 11). *Urteil GEMA gegen Open AI*. Pressemitteilung 11/2025.

<https://www.justiz.bayern.de/gerichte-und-behoerden/landgericht/muenchen-1/presse/2025/11.php>

⁵²⁹ Landgericht München I. (2026, July 31). *Urteil GEMA gegen SUNO*. Pressemitteilung 16/2026.

<https://www.justiz.bayern.de/gerichte-und-behoerden/landgericht/muenchen-1/presse/2026/16.php>

outputs in Germany and asserted jurisdiction over training-related acts conducted in the United States. Both judgments granted injunctive relief, information and damages claims and were announced as non-final. They create significant potential liability for U.S. AI suppliers, but do not establish that all AI training requires a license or that copyright enforcement can extend extraterritorially.

Other Barriers to Digital Trade

The Sixth Interstate Treaty Amending Media Law took effect on December 1, 2025, amending the Jugendmedienschutz-Staatsvertrag (JMStV) designed to protect minors.⁵³⁰ It requires providers of operating systems designated by the Commission for the Protection of Minors in the Media (KJM) to provide readily accessible parental controls. When activated, these controls must support age-based restrictions on app installation and use and support specified protections for browser and search services. The operating-system and related app requirements generally apply one year after a KJM's designation decision, with an extended transition of up to three years for evolving operating systems. These requirements can necessitate changes to operating systems, app distribution and service interfaces supplied by U.S. companies.

Germany's federal states are negotiating a treaty imposing sweeping obligations on U.S. streaming and platform services, including: (1) a media concentration regime with revenue thresholds triggering a presumption of "prevailing opinion power" that can lead to forced divestitures; (2) mandatory prominence rules requiring platforms to prioritize domestic public broadcasters over user preferences; (3) a new "AI editorial systems" category subjecting U.S. AI services to journalistic liability and domestic media input quotas; and (4) a digital advertising levy on regional online ads. The obligations are structurally designed to capture large cross-border digital services—in practice exclusively U.S. companies—while exempting competing domestic broadcasters and publishers.⁵³¹ USTR should closely monitor this initiative to ensure that U.S. suppliers are not unfairly targeted.

Taxation of Digital Products and Services

Germany continues to consider a digital services tax (DST). In May 2025, Culture Minister Wolfram Weimer proposed a "platform solidarity" levy, proposing a rate of 10% and identifying Austria's advertising-based digital services tax as a potential model.⁵³² Finance Minister Lars Klingbeil subsequently expressed support for a digital tax in January 2026.⁵³³ The proposed levy

⁵³⁰ German Länder. (2025, March 26). *Sechster Staatsvertrag zur Änderung medienrechtlicher Staatsverträge (Sechster Medienänderungsstaatsvertrag)*, Articles 1 and 3(2). <https://www.revosax.sachsen.de/vorschrift/21375>

⁵³¹ Hengel Mueller. 2025. *New Momentum for Reform of Media Concentration Control*. <https://hengeler-news.com/en/articles/new-momentum-for-reform-of-media-concentration-control>

⁵³² Deutsche Presse-Agentur. (2025, May 29). "Plattform-Soli": Weimer will Internetkonzerne zur Kasse bitten. ZDFheute. <https://www.zdfheute.de/politik/deutschland/weimer-internetkonzerne-plattform-soli-100.html>

⁵³³ Reuters. (2026, January 26). *Klingbeil fordert Digitalsteuer und Streamingdienst-Abgabe*. Handelsblatt. <https://www.handelsblatt.com/unternehmen/it-medien/streaming-klingbeil-fordert-digitalsteuer-und-streamingdienst-abgabe/100194739.html>

raises concerns about a selective revenue-based burden on major U.S. digital suppliers and potential cost increases for businesses purchasing digital advertising. This proposal has yet to be developed or formally introduced, but political pressure in favor of instituting the tax is building. The Social Democratic Party (SPD), the coalition partner that holds the Finance Ministry, has called for a broader digital services tax on "Big Tech" and has linked it to retaliation against U.S. tariffs.⁵³⁴

Ghana

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

Ghana's Ministry of Communications and National Communications Authority (NCA) introduced the 2025 Electronic Communications Bill, which would replace the Electronic Communications Act. The proposed bill would extend traditional telephone company licensing, operational reporting, and regulatory fees to Over-The-Top (OTT) internet messaging and video applications. Subjecting internet applications to legacy telecom licensing structures creates non-tariff market barriers and restricts access for foreign digital service suppliers.⁵³⁵ CCIA urges USTR to encourage Ghana to maintain a clear distinction between application-layer internet services and physical telecommunications networks.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Ghanaian Members of Parliament re-introduced the Human Sexual Rights and Family Values Bill, which contains provisions that eliminate intermediary safe harbor protections. By holding online platforms directly liable for user-generated content without clear notice-and-takedown safeguards, the bill threatens digital platform operations in the country.⁵³⁶ CCIA recommends that USTR engage Ghanaian policymakers to preserve platform safe harbor protections.

Greece

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Greece's Recovery and Resilience Plan requires data centers serving specified cloud investments to comply with the European Code of Conduct on Data Centre Energy Efficiency (EU CoC).

⁵³⁴ Politico. (2026). *Berlin weighs digital tax in response to Trump tariff threats*.

<https://www.politico.eu/article/germany-berlin-weighs-digital-tax-response-donald-trump-tariff-threats/>

⁵³⁵ National Communications Authority [Ghana]. (2025). Electronic Communications Bill, 2025, § 27. Business Regulatory Reform Portal, Government of Ghana.

<https://www.brr.gov.gh/acc/consultation/docs/NCA-Electronic-Communications-Bill-2025.pdf>.

⁵³⁶ Republic of Ghana. (2025, September 10). Human Sexual Rights and Family Values Bill, 2025, cls. 9(4)–(5), 10(3)–(5) [gazetted].

<https://www.ibanet.org/document?id=Ghana-Human-Sexual-Rights-and-Family-Values-Bill-2025>.

This requirement appeared in the original 2021 plan⁵³⁷ and remains in the August 2026 revision.⁵³⁸ Although the Code is voluntary at the EU level, the tender for Greece's central cloud infrastructure and services makes it mandatory. Conditioning eligibility on EU CoC participation can restrict competition where providers cannot demonstrate compliance through equivalent alternatives. Greece should accept objectively verified evidence of equivalent energy-efficiency performance to avoid unnecessarily excluding qualified U.S. suppliers.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

In April 2026, Greece announced plans to prohibit access to social media for children under 15, with implementation intended from January 1, 2027.⁵³⁹ The announced approach would require covered platforms to verify users' ages and prevent access by underage users. Greece continued advocating an EU-wide under-15 restriction in September 2026.⁵⁴⁰ National age-verification and access restrictions remain technically challenging and create additional compliance burdens for U.S. platforms serving Greece, particularly if requirements differ across EU Member States.

Guinea

Taxation of Digital Products and Services

Guinea introduced the Redevance de Conformité Numérique (Digital Compliance Fee) via presidential decree signed on May 21, 2026. The RCN applies to streaming platforms, cloud services, SaaS subscriptions, digital advertising and e-commerce. The decree sets a temporary flat 3% rate on applicable revenue for the first twelve months, after which tiered rates of 1.5% to 7% apply by service category. Providers with less than 250 million Guinean francs (about \$28,600) in annual taxable revenue are exempt, as are certain educational and non-profit services. The measure also creates a Digital Sovereignty Fund (FSN) financed primarily by the new fee's revenue.⁵⁴¹ This unilateral revenue tax explicitly targets foreign digital service exporters and creates severe double-taxation risks. CCIA urges USTR to request that Guinea withdraw its unilateral RCN tax in favor of multilateral consensus on international tax reform.

⁵³⁷ Council of the European Union. (2021, July 6). *Annex to the Council Implementing Decision on the approval of the assessment of the recovery and resilience plan for Greece* (10152/21 ADD 1). https://greece20.gov.gr/wp-content/uploads/2021/11/ST_10152_2021_ADD_1_en.pdf

⁵³⁸ Council of the European Union. (2026, August 20). *Annex to the Council Implementing Decision amending the Implementing Decision of 13 July 2021 on the approval of the assessment of the recovery and resilience plan for Greece* (12235/26 ADD 1 REV 1). https://greece20.gov.gr/wp-content/uploads/2026/08/CONSIL_ST_12235_2026_ADD_1_REV_1_EN.pdf

⁵³⁹ Reuters. (2026, April 8). *Greece to ban social media for under-15s from 2027, calls on EU action*. <https://www.reuters.com/business/media-telecom/greece-ban-social-media-under-15s-2027-pm-says-2026-04-08/>

⁵⁴⁰ Prime Minister of the Hellenic Republic. (2026, September 9). *Prime Minister Kyriakos Mitsotakis' meeting with the President of France Emmanuel Macron in Paris*. <https://www.primeminister.gr/en/2026/09/09/39226>

⁵⁴¹ Ecofin Agency. (2026, May 26). *Guinea Introduces 3% Tax on Foreign Digital Services*. <https://www.ecofinagency.com/news-digital/2605-55916-guinea-introduces-3-tax-on-foreign-digital-services> .

Hong Kong

Government-Imposed Restrictions on Internet Content and Related Access Barriers

In 2020, under pressure from China's mainland authorities, Hong Kong promulgated its National Security Law.⁵⁴² 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. Amendments to the National Security Law's Article 43 Implementation Rules took effect on March 23, 2026.⁵⁴³ Once an electronic message is specified for removal or disabling, designated officers may require action against its republication by other publishers or on other platforms. This expands the practical reach of content-removal demands across digital services. Hong Kong authorities have reportedly required internet service providers to block access to websites on national security grounds.⁵⁴⁴ Hundreds of people have reportedly been arrested under the law,⁵⁴⁵ as human rights experts have alerted world leaders to the harms of the law.⁵⁴⁶ 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, a measure which included concerning anti-doxing provisions.⁵⁴⁷ The provisions empower the Privacy Commissioner for Personal Data to issue cessation notices requiring removal of doxing content, restriction of access to messages or entire platforms, or discontinuation of hosting services. Notices may reach overseas service providers that provide or have provided services to a Hong Kong person, regardless of where the disclosure occurred,

⁵⁴² 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/>

⁵⁴³ Government of the Hong Kong Special Administrative Region. (2026, March 24). *2026 Implementation Rules for Amending the Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region*. <https://www.doi.gov.hk/en/legco/pdf/ajls20260324e1.pdf>

⁵⁴⁴ 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>; and 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>;

⁵⁴⁵ 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>

⁵⁴⁶ 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>

⁵⁴⁷ 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

provided the affected individual was a Hong Kong resident or present in Hong Kong when the disclosure occurred and the statutory consent and harm-related conditions are satisfied. Noncompliance is subject to statutory defenses, including technological impracticability and substantial prejudice to third parties. 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.

Hong Kong's Legislative Council passed the Safeguarding National Security Ordinance on March 19, 2024.⁵⁴⁸ The Ordinance criminalizes speech deemed to constitute treason, sabotage, sedition, theft of state secrets, external interference, and espionage, with some offenses carrying life imprisonment. Its broad provisions raise concerns about online expression and routine business communications. Section 43 also criminalizes collusion with an external force to publish false or misleading factual statements where the specified knowledge and national-security intent or recklessness requirements are met.

Threats to the Security of Devices and Services

Amendments effective March 23, 2026, empower police conducting legally authorized national-security searches of electronic equipment to compel specified persons, including owners, users, and persons believed to know the password, to provide passwords, decryption methods, or necessary assistance.⁵⁴⁹ Noncompliance without reasonable excuse is criminalized. These powers raise concerns about the confidentiality of business information accessible through employees' devices.

The Protection of Critical Infrastructures (Computer Systems) Ordinance, gazetted on March 28, 2025, took effect on January 1, 2026.⁵⁵⁰ It imposes cybersecurity obligations on designated critical infrastructure operators, including those in the separately listed information technology and telecommunications and broadcasting services sectors. Coverage depends on designation of operators and their critical computer systems, rather than sector membership alone. Designated operators must also maintain an office in Hong Kong for conducting business activities; a correspondence address alone is insufficient. The computer-system security management unit and its supervising employee, however, need not be based in Hong Kong. Industry concerns remain about the breadth of the information technology category and the predictability of

⁵⁴⁸ Government of the Hong Kong Special Administrative Region. (2024, March 19). *Address by CE to LegCo on passage of Safeguarding National Security Bill (with photos)*. <https://www.info.gov.hk/gia/general/202403/19/P2024031900717.htm>

⁵⁴⁹ Government of the Hong Kong Special Administrative Region. (2026, March 24). *2026 Implementation Rules for Amending the Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region*. <https://www.doj.gov.hk/en/legco/pdf/ajls20260324e1.pdf>

⁵⁵⁰ Government of the Hong Kong Special Administrative Region. (2025, June 27). *Protection of Critical Infrastructures (Computer Systems) Ordinance to come into effect on January 1, 2026*. <https://www.info.gov.hk/gia/general/202506/27/P2025062700238.htm>

designation for digital services providers. The Ordinance 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.⁵⁵¹ The measure's scope extends to critical computer systems located outside Hong Kong where designated operators can access them in or from Hong Kong. Although the government disclaims extraterritorial enforcement jurisdiction, these requirements raise concerns for cross-border cloud services operating in Hong Kong.

The Commissioner's Office may also seek a magistrate's warrant to exercise intrusive investigatory powers involving regulated systems. In its 2024 consultation submission, AmCham Hong Kong warned: "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."⁵⁵²

Other Barriers to Digital Trade

On January 9, 2026, Hong Kong's Law Reform Commission published its final report on Cyber-Dependent Crimes and Jurisdictional Issues, recommending bespoke legislation covering five categories of offenses, including making devices, programs, or data available for cybercrime.⁵⁵³ The report recommends a defense for providers acting as mere conduits and a separate defense for storage or dissemination services that promptly remove or disable access to illegal content—or report it to law enforcement where removal or disabling is not technically feasible or reasonably practicable. Any implementing legislation based on these recommendations should preserve these intermediary protections and provide clear, workable knowledge and response standards for digital services suppliers.

⁵⁵¹ 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>

⁵⁵² 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>

⁵⁵³ Law Reform Commission of Hong Kong. (2026, January 9). *LRC issues report on Cyber-Dependent Crimes and Jurisdictional Issues (with photo/video)*. <https://www.info.gov.hk/gia/general/202601/09/P2026010900205.htm>

Hungary

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Act 69 of 2024 on Hungary's Cybersecurity, effective January 1, 2025, replaced Act 50 of 2013.⁵⁵⁴ The new framework regulates cybersecurity across public administration and covered public- and private-sector entities, including restrictions on overseas data processing and cloud services.⁵⁵⁵ For entities subject to the Act's data-classification requirements, Government Decree 418/2024 imposes graduated geographic and cloud restrictions. Unless another law provides otherwise, F3-category data must remain within the EEA; use of an uncertified non-private cloud is limited to Hungary. F4-category data must be processed in Hungary and, where cloud services are used, in a third-party-certified private cloud or government cloud. Data classified as critical for integrity or availability (SR2) must be stored within the EEA and, if stored abroad, must also remain available in Hungary. Lower classifications permit broader overseas processing, subject to applicable conditions. Subject to the Act's jurisdictional rules, entities not registered in Hungary that operate covered electronic information systems must designate a representative operating in Hungary to ensure compliance.

Discriminatory Local Content Quotas and Audiovisual Services Mandates

Hungary's Act 79 of 2021 restricted minors' access to content depicting or promoting homosexuality or gender reassignment, including through audiovisual and information society services. On April 21, 2026, the Court of Justice of the European Union held in Case C-769/22 that these restrictions violated EU law, including rules governing cross-border services under the e-Commerce and Audiovisual Media Services Directives.⁵⁵⁶ On September 14, 2026, the government submitted legislation to remove the restrictions targeting LGBTQ+ content.⁵⁵⁷

India

⁵⁵⁴ Hungarian Parliament. (2024, December 20). 2024. évi LXIX. törvény Magyarország kiberbiztonságáról [Act LXIX of 2024 on Hungary's Cybersecurity], §§ 82(1), 116. <https://njt.jog.gov.hu/jogszabaly/2024-69-00-00.0>

⁵⁵⁵ 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.

⁵⁵⁶ Court of Justice of the European Union. (2026, April 21). *Values of the European Union: By adopting a law which stigmatises and marginalises LGBTI+ persons, Hungary has acted in breach of EU law* (Press Release No. 59/26, Case C-769/22). <https://curia.europa.eu/site/upload/docs/application/pdf/2026-04/cp260059en.pdf>

⁵⁵⁷ Reuters. (2026, September 15). *Hungary government submits bill to roll back Orban-era anti-LGBTQ+ rules*. <https://www.reuters.com/world/hungary-government-submits-bill-roll-back-orban-era-anti-lgbtq-rules-2026-09-15/>

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.”⁵⁵⁸ 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.⁵⁵⁹ While ostensibly seeking to address competition issues, the order, which is under appeal, may lead to a fragmented, more expensive, and less sustainable market for applications, introduce interoperability problems, and significantly increase cybersecurity risks in the mobile ecosystem.

In 2024, the Indian government released a draft Digital Competition Bill (DCB), an *ex-ante* regulatory framework modelled after the EU’s Digital Markets Act aimed at preventing Systemically Significant Digital Enterprises (SSDEs) from engaging in presumptively anticompetitive behavior.⁵⁶⁰ Following significant stakeholder opposition, the government withdrew the draft and commissioned a market study. That study, conducted by the Management Development Institute (MDI) Gurgaon, is now examining revised quantitative and qualitative thresholds for designating SSDEs. Recent stakeholder questionnaires and public reporting indicate that the government remains inclined to retain the core *ex-ante* framework, with substantially higher thresholds under consideration that could exclude major Indian platforms while capturing primarily large foreign, including U.S., firms.⁵⁶¹ A revised bill could emerge as early as the Winter Session in December 2026 or the Budget Session in February 2027. Such a discriminatory framework would raise serious national treatment and market access concerns while imposing prescriptive obligations without a demonstrated finding of anticompetitive harm. CCIA urges USTR to engage with Indian counterparts before a revised bill is introduced.

⁵⁵⁸ PRS Legislative Research. (2022, December 22). *Anti-Competitive Practices by Big Tech Companies: Standing Committee Report Summary*.

<https://prsindia.org/policy/report-summaries/anti-competitive-practices-by-big-tech-companies>

⁵⁵⁹ Competition Commission of India. (2018). *Umar Javeed et al. v. Google LLC & Google India Private Limited*. <https://www.cci.gov.in/antitrust/orders/details/1070/0>; Competition Commission of India. (2022). *XYZ (Confidential) v. Alphabet Inc. et al.* <https://www.cci.gov.in/antitrust/orders/details/1072/0>

⁵⁶⁰ Ministry of Corporate Affairs, Government of India. (2024, March 12). *Report of the Committee on Digital Competition Law and Draft Digital Competition Bill, 2024*.

<https://www.mca.gov.in/bin/dms/getdocument?mds=gzGtvSkE3zIVhAuBe2pbow%3D%3D&type=open>

⁵⁶¹ The Financial Express. (2026, July 27). *New Digital Competition Bill May Target Only Big Tech, Govt Likely to Retain Ex Ante Framework*.

<https://www.financialexpress.com/business/news/digital-competition-regulation-to-target-only-big-tech/4302951/>

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.⁵⁶² 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 “free” to “restricted” status.⁵⁶³ 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, 2023.⁵⁶⁴ 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

⁵⁶² 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>

⁵⁶³ Directorate General of Foreign Trade, Government of India. (2023, August 3). *Amendment in Import Policy of Items under HSN 8471 of Chapter 84 of Schedule-I (Import Policy) of ITC (HS), 2022 – reg.* Notification No. 23/2023. <https://content.dgft.gov.in/Website/dgftprod/ee5324b8-9a25-4c3a-908e-5af57e857634/Notification%20No.%2023%20dated%2003.08.2023%20Eng.pdf>

⁵⁶⁴ 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/>

totaling US\$8.4 billion in FY 2023–24 compared to authorized levels of about US\$9.5 billion.⁵⁶⁵ India has continued the Import Management System for restricted IT hardware through calendar year 2026. Under DGFT Policy Circular No. 08/2025-26, importers must obtain authorization through the IMS, with authorizations valid through December 31, 2026.⁵⁶⁶ Although the current framework does not impose a stated quota or hard cap, it preserves a possible midterm review and gives DGFT broad authority to amend, suspend, or withdraw the procedures based on policy requirements. The continuing authorization mandate creates regulatory uncertainty and adds an unnecessary administrative barrier to imports of critical ICT hardware.

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.

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,

⁵⁶⁵ 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>

⁵⁶⁶ Directorate General of Foreign Trade, Government of India. (2025, December 17). *Procedure for Implementation of Import Management System for Import of Restricted IT Hardware (viz. Laptops, Tablets, All-in-One Personal Computers, Ultra Small Form Factor Computers and Servers under HSN 8471) for the Calendar Year 2026 – reg.* Policy Circular No. 08/2025-26.

https://content.dgft.gov.in/Website/dgftprod/f78ef3ca-260e-44ce-bda6-7dde365c1144/Policy%20Circular%20No.%2008_0001.pdf

these requirements have been expanded to intermediate inputs and capital machinery, such as specialized copper products, electronic chemicals, and printed circuit board components, without prior consultation with impacted industry. While the stated objective is consumer safety, the surge in QCOs from 88 in 2019 to over 700 by late 2024⁵⁶⁷ is widely viewed as a protectionist measure. Because India's electronics manufacturing depends on 70–85% imported components,⁵⁶⁸ 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; and carve-outs for certain critical sectors such as electronics. Without greater transparency, stakeholder engagement, consideration of supply chain realities 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.

U.S. stakeholders report ongoing uncertainty in India's customs classification practices affecting imports of machinery, raw materials, and components used in electronics and smartphone manufacturing. Technical interpretations applied at individual ports frequently diverge from central government policy, particularly for high-technology inputs where product categories evolve rapidly. The resulting classification disputes are slow to resolve and have disrupted manufacturing operations for affected companies. In response, India has established a Joint Working Group between the Ministry of Electronics and Information Technology (MEITY) and the Central Board of Indirect Taxes and Customs (CBIC) to address classification issues at ports, though U.S. stakeholders continue to monitor whether this mechanism resolves the underlying inconsistencies.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

In 2020, the Ministry of Commerce and Industry's Department for Promotion of Industry and Internal Trade (DPIIT) extended local content requirements to the public procurement of software and services.⁵⁶⁹ Under this framework, suppliers must have more than 50% local

⁵⁶⁷ 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>

⁵⁶⁸ 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/>

⁵⁶⁹ Department for Promotion of Industry and Internal Trade, Government of India. (2020, September 16). *Public Procurement (Preference to Make in India), Order 2017 – Revision*. No. P-45021/2/2017-PP (BE-II). <https://dpiit.gov.in/sites/default/files/PPP%20MII%20Order%20dated%2016%2009%202020.pdf>

content to qualify as a “Class I local supplier,” while “Class II local suppliers” must have between 20% and 50% local content. However, the formula for calculating “local content” was not initially defined and was instead left to the discretion of individual procurement agencies. This created significant uncertainty for industry, particularly global software and cloud providers that operate through distributed R&D and supply chains and therefore cannot readily attribute product-development costs 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 the calculation of local content. The revised rules exclude certain imported components and services from counting toward applicable 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.

In March 2026, India's IT ministry, (MeitY), advised government ministries and departments to classify their data by sensitivity. The advisory sets out tiers, and the top tier, "Category A," covers the government's most critical systems. Examples include Aadhaar (India's national digital ID), UPI (Unified Payments Interface, India's instant payments network), tax systems, and land records. Category A systems may be hosted only on a government-run cloud or by an approved "Sovereign Cloud Provider," a vendor specifically cleared to host such data. Classification is left to each department, but most departments are likely to label their most important systems Category A to be safe. That behavior could pull a wide swath of government workloads behind these hosting limits. Under the proposed conditions, no U.S. cloud provider can currently qualify as a Sovereign Cloud Provider, because none are Indian-owned. As a result, a large share of Indian public procurement business may be closed to U.S. firms based on country-of-origin rather than the security of the technology.

In February 2021, guidelines regarding geospatial data and associated services were introduced with the goal of deregulation and liberalizing India’s mapping policy.⁵⁷⁰ 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

⁵⁷⁰ Department of Science and Technology, Government of India. (2021, February 15). *Guidelines for Acquiring and Producing Geospatial Data and Geospatial Data Services Including Maps*. <https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data.pdf>

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.⁵⁷¹ 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.

Starting in 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 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.⁵⁷² 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.⁵⁷³ 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

⁵⁷¹ 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/>

⁵⁷² Indian Computer Emergency Response Team (CERT-In). (2022, May 18). *Frequently Asked Questions on Cyber Security Directions of 28.04.2022*. 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/>

⁵⁷³ Bhatia, A. (2022, June 24). *India's New Cybersecurity Order Drives VPN Providers to Leave, Chilling Speech and Subjecting More Indians to Government Surveillance*. 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/>

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, and is 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 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.

India significantly restricts the use of public cloud technology involving overseas data transfers in the public sector and other regulated sectors. This is particularly burdensome in the financial services sector. The Securities and Exchange Board of India (SEBI), the country's financial sector regulator, passed multiple frameworks that now regulate significant portions of India's private financial sector, including stock brokers, asset management companies, and fintech companies. These regulations require American technology companies to be accredited and audited by the Ministry of Electronics and Information Technology (MEITY) in order to continue offering services to regulated entities in India's private financial sector. These certification requirements mandate onerous and technically infeasible data localization requirements for US tech companies (while advantageous to India technology companies that already have localized data). These protectionist regulations being extended to the private sector unfairly place restrictions on trade and cross-border data flows.

On March 6, 2023, the Securities and Exchange Board of India (SEBI) published a Circular for its Framework for Adoption of Cloud Services by SEBI Regulated entities,⁵⁷⁴ 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

⁵⁷⁴ Securities and Exchange Board of India. (2023, March 6). Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs), Circular No. SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033. https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-_68769.html.

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.⁵⁷⁵

Continued internet shutdowns have left widespread human rights impacts as well as economic losses. The U.S. International Trade Commission estimated global losses of US\$549.4 million incurred by Facebook, Instagram, YouTube, and Twitter between 2019-2021 due to repeated internet shutdowns.⁵⁷⁶ India has been the global leader in the number of internet shutdowns up to 2023, when it hit a record 113 incidents, and has been responsible for half of the recorded shutdowns since 2016.⁵⁷⁷ 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 2024.⁵⁷⁸

⁵⁷⁵ 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/>

⁵⁷⁶ 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>

⁵⁷⁷ Frontline Magazine. (2024). *Digital Darkness: India leads the world in internet shutdowns*. [youtube.com/watch?v=gSmcTRhu-zs&t=12](https://www.youtube.com/watch?v=gSmcTRhu-zs&t=12) ; and 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> .

⁵⁷⁸ 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

India's Sahyog portal, launched in 2024 by the Ministry of Home Affairs and managed by the Indian Cyber Crime Coordination Centre (I4C), represents a significant expansion of government content removal powers without adequate procedural safeguards.⁵⁷⁹ All intermediaries, including social media platforms, are being required to onboard to the portal and comply with takedown notices issued by the government. The portal enables content removal requests without prior judicial approval, bypassing established procedural safeguards. In 2025, X (formerly Twitter) challenged the portal's operations in Indian courts, alleging that it amounts to censorship. The majority of takedown notices issued through the portal are directed at U.S. technology companies. The lack of due process, transparency, or clear guidelines creates a highly unpredictable operating environment for digital service providers and constitutes an unpredictable trade barrier in the digital age. Further more the Indian Government is also considering an amendment to the Rule 3 (4) of the IT Rules mandating that Intermediaries must comply with all "clarifications, advisories, directions, SOPs, and codes of practice" issued by MeitY or the Ministry of Information and Broadcasting (MIB) to retain safe harbor protection.

India's current statutory framework for suspending telecommunications services is Section 20 of the Telecommunications Act, 2023 and the Telecommunications (Temporary Suspension of Services) Rules, 2024, which superseded the 2017 rules issued under the Indian Telegraph Act.⁵⁸⁰ The 2024 Rules require suspension orders to be issued by the Union Home Secretary or the relevant State Home Secretary, subject to limited emergency delegation, to state the reasons for suspension in writing, and to undergo review by a designated committee. They retain the 15-day maximum duration for individual suspension orders. Despite these procedural safeguards, India's continued use of internet shutdowns raises serious concerns regarding market access, economic losses, freedom of expression, and regulatory predictability for U.S. digital services suppliers.

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.⁵⁸¹ The Intermediary Guidelines and Digital Media

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. *Twitter*. <https://twitter.com/accessnow/status/1630772362294575106>

⁵⁷⁹ Pandey, K. (2025, April 1). Explained: What is the Sahyog Portal that X has called out for censorship? MediaNama.

<https://www.medianama.com/2025/04/223-explained-what-is-the-sahyog-portal-that-x-called-out-for-censorship>.

⁵⁸⁰ Ministry of Communications, Department of Telecommunications, Government of India. (2024, November 22).

Telecommunications (Temporary Suspension of Services) Rules, 2024. G.S.R. 724(E).

<https://egazette.gov.in/WriteReadData/2024/258840.pdf>

⁵⁸¹ Vadehra, S. (2021, May 28). An update on India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. *GALA*.

<https://blog.galalaw.com/post/102gzas/an-update-on-indias-information-technology-intermediary-guidelines-and-digital>

Ethics Code Rules, 2021 (IT Rules)⁵⁸² impose new obligations on intermediaries.⁵⁸³ 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 2023 amendments to the 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.⁵⁸⁴ 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.

⁵⁸² *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* [India]. (2021). Updated April 6, 2023.

<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>

⁵⁸³ *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* [India]. (2021). Updated April 6, 2023.

<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>

⁵⁸⁴ *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* [India]. (2021). Updated April 6, 2023, rules 3(1)(d), 3(2), 4(1), and 4(4).

<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>

On February 10, 2026, the Government of India notified further amendments to the IT Rules imposing extensive new obligations relating to “synthetically generated information” (SGI).⁵⁸⁵ Among other requirements, significant social media intermediaries must obtain user declarations concerning whether uploaded content is synthetic, undertake reasonable technical verification before publication, and ensure covered content carries prominent labeling and embedded provenance metadata. The amendments also require intermediaries to deploy technical tools, including automated mechanisms, to prevent the dissemination of unlawful synthetic content and sharply compress response timelines across the broader content-moderation framework, including requiring removal or disabling of specified information within as little as two or three hours following lawful notices. The amendments entered into force only ten days after notification and introduced substantial obligations beyond those contained in the preceding consultation draft. These requirements create significant operational burdens, legal uncertainty, and incentives for precautionary removal of lawful content, particularly because they apply across different layers of the technology stack without adequately distinguishing between infrastructure providers, model developers, and user-facing platforms.

In March 2026, MeitY proposed additional amendments that would further expand intermediary obligations.⁵⁸⁶ Proposed Rule 3(4) would require intermediaries to comply with Ministry-issued clarifications, advisories, directions, standard operating procedures, codes of practice, and guidelines and make such compliance part of intermediaries’ due diligence obligations under Section 79 of the IT Act. This could effectively transform non-binding sub-regulatory instruments into conditions for safe-harbor protection without formal rulemaking. Other proposed provisions would create overlapping data-retention obligations under multiple legal frameworks, while a subsequent April proposal would require continuous visible or audible labeling of synthetically generated content. These proposals risk incentivizing over-removal and over-retention, reducing legal certainty, and imposing prescriptive requirements that do not account for significant differences among intermediary services. CCIA urges USTR to press India to ensure that binding obligations on commercial actors are established through transparent rulemaking with clear statutory authority, adequate notice, and meaningful procedural safeguards.

India’s government often issues issue-specific interventions to supplement broader regulatory pressures. In November 2023, India’s IT ministry issued an advisory to social media companies

⁵⁸⁵ TOI Tech Desk. (2026, February 20). Explained: What are government’s new IT rules that go into effect starting today and what they mean for you. *The Times of India*.
<https://timesofindia.indiatimes.com/technology/tech-news/explained-what-are-governments-new-it-rules-that-go-into-effect-starting-today-and-what-they-mean-for-you/articleshow/128605381.cms>

⁵⁸⁶ ETtech. (2026, April 7). IT rule tweaks only clarificatory, don’t expand govt power: MeitY Secretary. *The Economic Times*.
<https://economictimes.indiatimes.com/tech/technology/it-rule-tweaks-only-clarificatory-dont-expand-govt-power-meit-secretary/articleshow/130092109.cms>

directing them to identify and remove “deepfakes” within 36 hours of receiving a complaint.⁵⁸⁷ 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 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.⁵⁸⁸ 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.⁵⁸⁹ X Corp appealed the decision in November 2025, and the Karnataka High Court subsequently sought the Union government’s response.⁵⁹⁰ On September 8, 2026, the Supreme Court stayed proceedings in a related Gujarat High Court case while considering the Union government’s petition to transfer that case.⁵⁹¹ The continuing litigation underscores the unresolved legal and procedural concerns surrounding the portal. 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.

⁵⁸⁷ 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>

⁵⁸⁸ 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/>

⁵⁸⁹ *X Corp. v. Union of India & Ors.*, W.P. No. 7405 of 2025 (September 24, 2025) [High Court of Karnataka, India]. <https://drive.google.com/file/d/1woknI67KZw5u8wWfVnANkutmKA2P9LvL/view>

⁵⁹⁰ ETtech. (2025, November 16). X appeals Karnataka HC order upholding Sahyog portal. *The Economic Times*. <https://economictimes.indiatimes.com/tech/technology/x-appeals-karnataka-hc-order-upholding-sahyog-portal/articleeshow/125364846.cms>

⁵⁹¹ Raja, A. (2026, September 11). ‘Backdoor’ push to join portal? X Corp accuses Centre of hiding facts from court. *The Indian Express*. <https://indianexpress.com/article/legal-news/x-corp-sahyog-portal-centre-gujarat-high-court-10873498/>

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

In December 2023, the Telecommunications Act, 2023 was enacted, replacing older statutes such as the Indian Telegraph Act and potentially providing a new legal basis for telecom regulation authorities to regulate OTT services; however, as of 2026, 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.

India's Telecommunications Act, 2023 provides for central-government authorization of telecommunications services and networks and grants the government substantial authority over authorization conditions and implementation.⁵⁹² It also contains provisions concerning biometric identification of users, interception of communications, suspension of telecommunications services, and government possession of telecommunications infrastructure during public emergencies or in the interest of public safety.¹ These provisions raise concerns about compliance burdens, privacy, freedom of expression, and regulatory predictability for U.S. suppliers. CCIA urges USTR to monitor implementation of the Act and press India to maintain a clear distinction between telecommunications infrastructure and services and the applications and digital services delivered over them.

In 2025, India's Department of Telecommunications considered subjecting content delivery networks (CDNs) to a new authorization or registration framework under the Telecommunications Act, potentially including disclosure of confidential CDN-ISP peering and interconnection agreements. Following opposition from TRAI and industry, however, India did not include a CDN authorization category in the final Telecommunications (Authorisation for Telecommunication Network) Rules, 2026.⁵⁹³ CCIA welcomes this outcome and urges India to maintain CDNs outside telecommunications licensing, registration, and authorization regimes and to refrain from imposing requirements to disclose commercially sensitive peering arrangements.

Restrictions on Cross-Border Data Flows

In November 2025, the government notified the final Digital Personal Data Protection Rules, 2025, implementing the DPDP Act.⁵⁹⁴ The final Rules retain provisions of significant concern regarding data localization and cross-border data transfers. Rule 13 empowers the Central Government, based on recommendations from a government-appointed committee, to specify

⁵⁹² *The Telecommunications Act, 2023* [India], Act No. 44 of 2023, sections 3 and 20. (2023).

<https://www.indiacode.nic.in/handle/123456789/20101>

⁵⁹³ TeamLease RegTech Legal Research Team. (2026, July 23). *Telecommunications (Authorisation for Telecommunication Network) Rules, 2026*.

<https://teamleaseregtech.com/updates/article/58054/telecommunications-authorisation-for-telecommunication-network-rules-2/>

⁵⁹⁴ *Digital Personal Data Protection Rules, 2025* [India], G.S.R. 846(E). (2025, November 13).

<https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtOWa>

categories of personal data processed by Significant Data Fiduciaries that, together with traffic data pertaining to their flow, may not be transferred outside India. Rule 15 generally permits cross-border transfers but subjects them to requirements that the Central Government may impose by general or special order regarding the availability of personal data to foreign governments or entities under their control. These substantive provisions are subject to an 18-month transition period and are scheduled to take effect in May 2027. The framework therefore continues to give the government broad discretion to impose company- or data-specific localization and transfer restrictions without clear substantive criteria, creating significant uncertainty for globally integrated U.S. digital services providers. CCIA urges USTR to press India to ensure that cross-border transfers remain permitted by default, to eliminate localization requirements, and to establish transparent, objective, and proportionate safeguards for any restrictions on data transfers.

Taxation of Digital Products and Services

India's income tax laws⁵⁹⁵ 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 business in India)⁵⁹⁶ 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).⁵⁹⁷ 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.

Challenges to the Development of AI

In December 2025, India's Department for Promotion of Industry and Internal Trade (DPIIT) released a Working Paper on Generative AI and Copyright proposing a mandatory blanket licensing regime for copyrighted works used in commercial AI training.⁵⁹⁸ Under the proposed "One Nation, One License, One Payment" framework, India would reject a text-and-data-mining

⁵⁹⁵ *Income-tax Act, 1961* [India]. (1961). <https://www.incometaxindia.gov.in/income-tax-act>; *Income-tax Rules, 1962* [India]. (1962). <https://www.incometaxindia.gov.in/income-tax-rules>

⁵⁹⁶ Income Tax Department. (n.d.). *Double taxation avoidance agreements*. <https://www.incometaxindia.gov.in/dtaa>

⁵⁹⁷ *Income-tax Act, 1961* [India], § 9(1)(i). (1961). <https://www.indiacode.nic.in/bitstream/123456789/2435/1/a1961-43.pdf>

⁵⁹⁸ Department for Promotion of Industry and Internal Trade. (2025, December). *Working paper on generative AI and copyright, Part 1: One nation one license one payment—Balancing AI innovation and copyright*. <https://www.dpiit.gov.in/static/uploads/2025/12/ff266bbeed10c48e3479c941484f3525.pdf>

exception and instead permit AI developers to train on qualifying Indian copyrighted works subject to mandatory, government-set royalty payments. Rightsholders would not be able to withhold covered works from AI training, while a centralized, government-designated entity would collect and distribute royalties and a government-appointed committee would establish royalty rates. Of particular concern, the contemplated royalty methodology could be tied to an AI developer's global revenue rather than its actual use of Indian copyrighted works, disproportionately burdening U.S. technology companies and functioning similarly to a revenue-based levy on digital services. The framework could also discourage investment in Indian digital infrastructure, undermine voluntary licensing markets, create retroactive liabilities, and restrict lawful access to information. CCIA urges USTR to press India not to adopt the proposed mandatory licensing framework and instead preserve lawful access to training data, adopt a flexible text-and-data-mining exception, avoid extraterritorial or retroactive obligations, protect trade secrets, and allow market-based licensing arrangements to develop.

Other Barriers to Digital Trade

India maintains discriminatory restrictions on foreign-invested retail and e-commerce providers. Under India's separate multi-brand retail trading regime, foreign investment is capped at 51% under the government approval route and is subject to a minimum investment of \$100 million, back-end infrastructure requirements, and domestic sourcing obligations; companies with foreign investment engaged in multi-brand retail trading are also prohibited from conducting retail sales through e-commerce.⁵⁹⁹ Separately, India permits 100% foreign investment in the marketplace model of e-commerce but generally prohibits foreign-invested companies from operating an inventory-based model for domestic business-to-consumer sales. Foreign-invested marketplace operators are also subject to restrictions on ownership or control of seller inventory, influencing sale prices, and seller exclusivity that do not constrain domestic firms operating without foreign investment in the same manner. In July 2026, India created a limited exception allowing foreign-invested e-commerce entities to operate an inventory-based model exclusively for exports of goods manufactured or produced in India, and the government operationalized that framework in August 2026.⁶⁰⁰ While a welcome liberalization for exports, the change does not address the underlying asymmetry in the domestic Indian market, where foreign-invested platforms remain unable to operate inventory-based B2C models available to domestic competitors. CCIA urges USTR to press India to provide non-discriminatory treatment for U.S. e-commerce suppliers and remove FDI-based restrictions on business models, inventory management, pricing, and seller relationships.

⁵⁹⁹ Department for Promotion of Industry and Internal Trade. (2020, October 15). *Consolidated FDI policy circular of 2020*, § 5.2.15.4, pp. 53–55.

<https://www.dpiit.gov.in/static/uploads/2025/07/6457fc2703ee6082366c4a958b6473a8.pdf>

⁶⁰⁰ ET Online. (2026, July 23). Govt opens inventory-based e-commerce to foreign direct investment for exports only. *The Economic Times*.

<https://economictimes.indiatimes.com/news/economy/foreign-trade/govt-opens-inventory-based-e-commerce-to-foreign-direct-investment-for-exports-only/articleshow/132578576.cms>

India has also imposed a new comprehensive regulatory framework on online video gaming. The Promotion and Regulation of Online Gaming Act, 2025 prohibits the offering or operation of online money games, regardless of whether they are games of skill or chance, as well as their advertising, promotion, facilitation, and associated financial transactions.⁶⁰¹ The Promotion and Regulation of Online Gaming Rules, 2026,⁶⁰² which took effect on May 1, 2026, established the Online Gaming Authority of India and a centralized framework for determining, registering, and regulating online games. Of particular trade concern, Rule 17 permits the government to require online social-game and e-sports providers to retain and store traffic data, metadata, and related information on computer resources located in India for prescribed periods. These localization requirements increase the cost of supplying services on a cross-border basis, fragment globally integrated infrastructure, and may disproportionately burden foreign digital services providers. CCIA urges USTR to press India to eliminate mandatory localization requirements for gaming data and to ensure that classification, registration, and other regulatory requirements are transparent, proportionate, and applied on a non-discriminatory basis.

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.⁶⁰³ 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.⁶⁰⁴ Amendments to these corridor and landing-point restrictions are currently under review by Indonesia's National Team for the Acceleration of Digital Infrastructure Development (TIMNAS), with industry input under consideration. USTR should encourage Indonesia to use this process to expand permissible cable routes and landing points, provide operators greater route flexibility, and establish a transparent mechanism for proposing new corridors.

⁶⁰¹ *Promotion and Regulation of Online Gaming Act, 2025* [India], Act No. 32 of 2025, §§ 2(1)(g), 5–7. (2025). <https://www.meity.gov.in/static/uploads/2025/10/8a7f103cefc68ed8aaa2ebc9a2ed7c13.pdf>

⁶⁰² *Promotion and Regulation of Online Gaming Rules, 2026* [India]. (2026, April 22). <https://egazette.gov.in/WriteReadData/2026/271974.pdf>

⁶⁰³ 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>.

⁶⁰⁴ 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>.

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. 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 under Law No. 17 of 2008 on Shipping, which generally require Indonesian-flagged vessels to conduct subsea cable survey, installation, and repair operations.⁶⁰⁵ The U.S.-Indonesia Agreement on Reciprocal Trade (ART), signed in February 2026, commits Indonesia to grant cabotage exemptions for foreign-flagged vessels installing telecommunications cables. This is an important step, but the commitment does not extend to maintenance and repair, where rapid vessel mobilization is most critical. Moreover, the underlying exemption process continues to require applicants to obtain confirmation from the Indonesian National Shipowners' Association (INSA) that no domestic vessel is available, effectively giving domestic vessel owners a veto over access to foreign vessels. Indonesia's standard subsea cable repair time exceeds 30 days, and only four cable ships are Indonesian-flagged, of which only three are capable of repairs. The Third Amendment to the Shipping Law, Law No. 66 of 2024, further raised the vessel-ownership threshold applicable to certain venture companies from 5,000 to 50,000 gross tons, even though specialized subsea cable vessels generally fall below 20,000 tons. USTR should press Indonesia to adopt a standing, sector-wide cabotage waiver covering installation, maintenance, and repair, or at minimum extend the ART commitment to repair and reform the exemption process so that technical suitability and mobilization time—not the existence of any Indonesian-flagged vessel—determine eligibility. CCIA estimates that maintaining the current cabotage and permitting regime could impose approximately \$100 billion in foregone economic activity on Indonesia through 2030.

In Indonesia, new entrants seeking to offer satellite services must complete radiofrequency coordination with one or more national operators before the satellite authorization application can proceed. Coordination between two operators to avoid interference is a reasonable requirement but can be concluded only where both are willing to engage in good faith. Where regulation makes the new entrant's authorization dependent on the agreement of an incumbent operator but provides the regulator with no mechanism to resolve the matter if that operator

⁶⁰⁵ Republik Indonesia. (2008, May 7). Undang-Undang Nomor 17 Tahun 2008 tentang Pelayaran [Law No. 17 of 2008 on Shipping]. Jaringan Dokumentasi dan Informasi Hukum, Badan Pemeriksa Keuangan. <https://peraturan.bpk.go.id/Details/39060>.

declines to coordinate, the new satellite service entrant can be delayed indefinitely through no fault of its own. There is currently no procedural backstop — a defined timeframe, best practice for protection criteria, a dispute-resolution step, or a regulator-led determination — so that the obligation to protect national service becomes, in effect, a veto on market access in a country. USTR should consider engaging with Indonesia to explore mechanisms to address what could constitute a nullification of market access for a service Indonesia liberalized in the WTO (*i.e.*, cross-border internet access services). In addition, requiring such coordination without an effective dispute-resolution mechanism could be considered a condition inconsistent with Article VI.4 (c) of the GATS, designed to ensure that licensing procedures are not themselves a restriction on the supply of a service.

Customs-Related Restrictions and Import Barriers for Goods

Industry reports that Indonesia has failed to implement 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, Indonesia only introduced ITA commitments for five categories of goods/HS codes (Semiconductors, Semiconductors Equipment, Computers, Telecommunications Equipment and Software, and Electronic Consumer Goods).⁶⁰⁶ Even within those categories 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.⁶⁰⁷ 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

⁶⁰⁶ Consumer Technology Association. (2025, October 30). Comments of the Consumer Technology Association to Ambassador Jamieson Greer, United States Trade Representative [Docket No. USTR-2025-0016]. Regulations.gov. https://downloads.regulations.gov/USTR-2025-0016-0101/attachment_1.pdf.

⁶⁰⁷ Kementerian Perdagangan Republik Indonesia [Ministry of Trade of the Republic of Indonesia]. (2015, October 15). Peraturan Menteri Perdagangan Nomor 87/M-DAG/PER/10/2015 tentang Ketentuan Impor Produk Tertentu [Minister of Trade Regulation No. 87/M-DAG/PER/10/2015 on Provisions for the Import of Certain Products]. Jaringan Dokumentasi dan Informasi Hukum, Badan Pemeriksa Keuangan. <https://peraturan.bpk.go.id/Details/143170/permendag-no-87m-dagper102015-tahun-2015>.

2021”), which went into effect on November 19, 2021, and implemented new HS codes.⁶⁰⁸ 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 exemptions for certain capital goods, industry continues to report insufficient transparency and predictability regarding the process and timeline for obtaining them. The February 2026 U.S.-Indonesia ART now commits Indonesia to reform its pre-shipment inspection mechanism to address U.S. exporters’ concerns no later than three months after the Agreement enters into force, including through regular engagement with USTR.⁶⁰⁹ USTR should closely monitor implementation to ensure that the resulting reforms eliminate duplicative inspection requirements and provide transparent and predictable procedures for U.S. technology exporters.

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.⁶¹⁰ 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 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) which relaxed data localization requirements. GR71 still requires data localization for public sector ESOs, and does not govern financial services, which retains broad localization mandates.

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

⁶⁰⁸ 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.

⁶⁰⁹ Office of the United States Trade Representative. (2026, February 19). Agreement Between the United States of America and the Republic of Indonesia on Reciprocal Trade, art. 2.43.

<https://ustr.gov/sites/default/files/files/Press/Releases/2026/02.19.26%20US-IDN%20ART%20Full%20Agreement%20-%20US%20Final%20for%20Website%20sanitized.pdf>.

⁶¹⁰ 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.

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.⁶¹¹

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.⁶¹²

GR71 is, however, now subject to revision. Based on the 2024 draft, revisions potentially include the expansion of data localization mandate to include five broadly defined categories of data: civil registration, immigration, health, financial and ‘other’ data as determined by relevant ministries or institutions. The ‘other’ category is intentionally vaguely defined to allow for practically unlimited scope of data that must be stored in Indonesia. Data localization requirements limit the ability of international service providers to serve Indonesian customers with features and services that may not be available locally.

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.⁶¹³ 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 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.⁶¹⁴ This is particularly burdensome in

⁶¹¹ 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-foreign-private-electronic-system-operators11122020/>.

⁶¹² 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>.

⁶¹³ 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.

⁶¹⁴ 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/>.

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.⁶¹⁵ 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.

Additional Bank Indonesia regulations effective as of March 31, 2026 threaten to cut U.S. cloud companies off from providing services to Indonesian payment service providers. Bank Indonesia (BI) Regulation No. 10/2025 (PBI 10/2025) and implementing Board of Governors Regulation No. 32/2025 (PADG 32/2025), effective March 31, 2026, transform the oversight model for Supporting Operators, or third-party service providers, including cloud service providers, that support payment system participants. While this category existed under BI's previous regulatory regime, Supporting Operators were supervised only indirectly through the payment service providers they served. The new framework shifts to a hybrid model in which BI designates Supporting Operators as direct objects of supervision, asserts authority to impose administrative

⁶¹⁵ 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>

sanctions directly on them, and establishes a mandatory tiered classification (Critical, Important, Standard) with registration required for Critical and Important operators by March 31, 2029. Operators that fail to register will be barred from collaborating with payment service providers. The regulations also introduce new obligations across operational resilience, governance, data reporting, and cooperation agreements. Based on article 122 of BI Regulation No. 10/2025,⁶¹⁶ all domestic payment transaction processing, from initiation to settlement, be conducted within the territory of Indonesia—thus effectively precluding use of cloud providers located outside Indonesia for such purposes.⁶¹⁷

Meanwhile, the Financial Services Authority (OJK) has gradually allowed certain financial services entities, such as insurance companies and non-bank financial institutions with specific asset thresholds, to use offshore electronic systems and data centers. Commercial banks may also use offshore electronic systems and data centers for non-core workloads, such as for risk and internal management purposes, but core banking workloads must still be stored and processed in Indonesia unless approved by OJK.

Through various regulations, the government has been requiring service providers to possess Indonesian National Standard (SNI) certificates to participate in public procurement, while not 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.⁶¹⁸ The standards listed are SNI ISO 9001, SNI ISO/IEC 27001, SNI ISO/IEC 27017, and SNI ISO/IEC 27018 – and they do not acknowledge the international ISO equivalent. The requirements are designed to provide preferences to local providers, including by requiring a local presence and local content (neither of which are technically relevant to technical competence), effectively discriminating against international providers. Furthermore, some requirements are listed without further implementing guidelines, resulting in local certifiers incapable of issuing such certificates. The recent draft cybersecurity law (see below) 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

⁶¹⁶ Bank Indonesia, (2025) *Regulation No. 10 (2025)*

<https://www.bi.go.id/id/publikasi/peraturan/Documents/PBI-102025.pdf>

⁶¹⁷ Veritask. (2026). *Bank Indonesi Regulation No. 10.*

<https://veritask.ai/en/artikel/bank-indonesia-regulation-number-10-of-2025-reorganizing-the-payment-system-industry>

⁶¹⁸ *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

regulatory authority.⁶¹⁹ 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.⁶²⁰ Digital 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.⁶²¹ 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 oversees 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

⁶¹⁹ *Naskah Akademik Rancangan Undang-Undang Keamanan Ketahanan Siber* [Indonesia]. (2025). <https://berkas.dpr.go.id/akd/dokumen/RJI-20190617-025848-5506.pdf>.

⁶²⁰ *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/>.

⁶²¹ 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>.

does not clearly mandate disclosure of algorithmic changes or user behavior data to news publishers.

Since the adoption of Presidential Regulation No. 32/2024, the United States secured a significant commitment addressing these concerns in the U.S.-Indonesia Agreement on Reciprocal Trade. Annex III, Article 3.3 provides that Indonesia shall refrain from requiring U.S. digital services providers to support domestic news organizations through paid licenses, user data sharing, or profit-sharing models.⁶²² The Agreement was signed on February 19, 2026 but has not yet entered into force. USTR should ensure that Indonesia implements this commitment fully, including by bringing the operation of Presidential Regulation No. 32/2024 and any implementing measures into conformity with the ART and preventing the creation of functionally equivalent mandatory payment obligations through other legislation.

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 2019-2021.⁶²³ 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 2022.⁶²⁴

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 internet website or internet-enabled service.⁶²⁵ Under the new framework, local and foreign ESPs

⁶²² Office of the United States Trade Representative. (2026, February 19). Agreement Between the United States of America and the Republic of Indonesia on Reciprocal Trade, annex III, art. 3.3.

https://ustr.gov/sites/default/files/files/Press/Releases/2026/02_19_26%20US-IDN%20ART%20Full%20Agreement%20-%20US%20Final%20for%20Website%20sanitized.pdf.

⁶²³ 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>.

⁶²⁴ 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 Tough New Curbs for Online Platforms. *Reuters*.

<https://www.reuters.com/world/asia-pacific/exclusive-indonesia-preparing-tough-new-curbs-online-platforms-source-s-2022-03-23/>

⁶²⁵ 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.

are required to register with the government and appoint local representatives to respond to government demands for access to systems and data, regardless of whether the company has a legal entity, employees, or other meaningful presence in Indonesia. Indonesia's Ministry of Communication and Digital Affairs (MOCDA or Komdigi) has notified at least 36 global companies (including US-based companies such as Cloudflare, Dropbox, OpenAI, and Shopify) to register as electronic system operators (ESOs) with Komdigi. Several companies have had to block access to users due to a lack of ESO registration; some have restored access following consultations with the Indonesian government, while some may be required to establish a local entity in Indonesia.

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 for failing to comply with granular user data request from Komdigi.⁶²⁶ 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 20.⁶²⁷ 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.⁶²⁸ 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.

Registration is also the gateway to the broader set of obligations, including mandatory government access to systems and data for "supervision," law enforcement data demands that bypass the Mutual Legal Assistance Treaty (MLAT) process, expedited content removal, and a

<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/>.

⁶²⁶ 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>.

⁶²⁷ 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.globalcompliancencews.com/2022/07/05/indonesia-deadline-for-registration-of-electronic-system-operators-is-now-set-for-20-july-2022-01072022/>.

⁶²⁸ 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/>

range of administrative and risk-assessment requirements. Taken together, these obligations impose significant costs and legal conflicts on U.S. companies of all types, and there have been reports of Indonesian authorities using the registration requirement and the threat of blocking to pressure companies to depart from their global policies on customer privacy and content moderation.

Komdigi has pursued enforcement of the registration requirement through recurring waves of notices to foreign companies, each demanding registration within short deadlines, in some cases as little as five business days, under threat of being blocked.⁶²⁹ These notices have targeted a growing range of sectors over time, extending well beyond the consumer-facing platforms the framework was originally designed to include. Many of the companies receiving notices offer globally available services that are not specifically directed at the Indonesian market. The steady expansion of the regime, combined with the unpredictability of enforcement and the severity of the penalty, has created substantial uncertainty for U.S. companies and deterred investment in Indonesia.

The expansion of the regime to B2B and infrastructure providers compounds these concerns, because the obligations that flow from registration were written with a different set of services in mind. Infrastructure and B2B providers typically have no visibility into or control over the content of their customers' end users, so takedown mandates applied at the infrastructure layer are technically disproportionate and raise serious freedom of expression concerns. The compliance frameworks that attach to registration, drawn from laws written for social media and consumer applications, have little relevance to these business models and provide no corresponding regulatory benefit. And because infrastructure providers underpin large portions of the global Internet, blocking a single provider would cut Indonesian users and businesses off from a significant share of global websites and online services, harming Indonesia's own digital economy as much as the targeted company.

Indonesia's Ministry of Communication and Digital Affairs (MOCDA or Komdigi) has notified at least 36 global companies (including US-based companies such as Cloudflare, Dropbox, OpenAI, and Shopify) to register as electronic system operators (ESOs) with Komdigi. Several companies have had to block access to users due to a lack of ESO registration; some have restored access following consultations with the Indonesian government, while some may be required to establish a local entity in Indonesia.

⁶²⁹ Kementerian Komunikasi dan Digital [Indonesian Ministry of Communication and Digital]. (2026, July 1). Komdigi tegaskan kewajiban pendaftaran, 25 PSE lingkup privat terima pemberitahuan [Komdigi affirms registration obligation; 25 private-scope electronic system operators receive notices]. <https://portal.komdigi.go.id/kanal-publik/berita-kini/10354>.

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.⁶³⁰ Civil society groups have also raised concerns with aspects of the Regulation.⁶³¹ Recently, X was fined for failure to comply with a content takedown request within the prescribed 24 hours turn-around-time.⁶³² 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.⁶³³ 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 PP Tunas) establishes a broad online child-safety framework that imposes significant new obligations on digital service providers.⁶³⁴ On March 6, 2026, the Ministry of Communication and Digital

⁶³⁰ GR 43/2023 [Indonesia]. (2023).

<https://peraturan.bpk.go.id/Download/321932/PP%20Nomor%2043%20Tahun%202023.pdf>

⁶³¹ 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>.

⁶³² 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>.

⁶³³ 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>.

⁶³⁴ Republik Indonesia. (2025, March 27). Peraturan Pemerintah Nomor 17 Tahun 2025 tentang Tata Kelola Penyelenggaraan Sistem Elektronik dalam Pelindungan Anak [Government Regulation No. 17 of 2025 on the Governance of Electronic System Operations in Child Protection]. Jaringan Dokumentasi dan Informasi Hukum, Badan Pemeriksa Keuangan. <https://peraturan.bpk.go.id/Details/316698/pp-no-17-tahun-2025>.

Affairs issued implementing Regulation No. 9 of 2026, which entered into force the same day and requires providers to assess and report the risk profiles of products, services, and features that are designed for, or may be used or accessed by, children. The framework divides minors into five separate age bands and assesses services across factors including contact with unknown persons, harmful content, commercial exploitation, data protection, addiction, and psychological and physiological harms. A high-risk finding in any one category results in the service receiving an overall high-risk profile. Children ages 13 through 15 may maintain accounts only on services classified as low-risk and with parental consent, while social-networking and social-media services are presumptively categorized as high-risk unless otherwise determined through the assessment process.

The framework creates substantial compliance uncertainty because of its exceptionally broad scope, granular age-assurance requirements, subjective risk criteria, and significant regulatory discretion over platform classifications. These requirements can restrict access to otherwise responsible services despite the use of effective safety and privacy mitigations and impose particularly significant burdens on general-purpose U.S. digital services that are not designed specifically for children. Furthermore, failure to comply with the regulation may lead to fines worth as much as 6% of a platform's global revenue. USTR should encourage Indonesia to adopt objective, harm-based risk criteria; recognize effective platform-level mitigations before classifying an entire service as high-risk; permit proportionate and privacy-preserving age-assurance mechanisms; and ensure that enforcement and sanctions provide adequate due process.

In May 2026, Indonesia's Ministry of Law released a proposed revision to Law No. 28 of 2014 on Copyright that would impose significant new obligations on U.S. digital service providers.⁶³⁵ Among other provisions, the draft would require digital platforms to compensate collective management organizations for broad uses of journalistic works, including indexing, aggregation, snippets, links, algorithmic recommendations, and use for machine learning or artificial intelligence. It would also impose licensing requirements for the use of both copyrighted works and publicly available information to train AI models; broad AI labeling and disclosure requirements; royalty obligations relating to AI-generated content; expansive protections for an individual's likeness and a creator's "unique style;" and proactive copyright-monitoring obligations without a clear intermediary safe harbor. Multiple provisions authorize the closure of a digital platform as a sanction for non-compliance.

These obligations would create substantial compliance and market-access barriers for U.S. search, social media, cloud, streaming, and AI providers. In particular, the proposed mandatory compensation for journalistic content appears inconsistent with Indonesia's commitment under

⁶³⁵ Pujari, R., SSEK Law Firm. (2026, May 20). Indonesia Proposes Overhaul of Copyright Law with Focus on Digital Content and Emerging Technologies. Conventus Law. <https://conventuslaw.com/report/indonesia-proposes-overhaul-of-copyright-law-with-focus-on-digital-content-and-emerging-technologies>.

Annex III, Article 3.3 of the U.S.-Indonesia ART not to require U.S. digital services providers to support domestic news organizations through paid licenses, user data sharing, or profit-sharing models.⁶³⁶ USTR should urge Indonesia to remove mandatory payment and collective-licensing requirements; preserve a notice-and-action framework for intermediary liability; establish a meaningful text-and-data-mining exception for AI development; narrowly tailor any AI-transparency obligations to material risks; and remove disproportionate platform-closure sanctions. Furthermore, USTR should engage Komdigi on the ESO registration regime and its associated obligations, and in particular to press Indonesia to narrow the scope of MR 5/2020 so that it does not apply to B2B services and digital infrastructure providers, using the U.S.-Indonesia Agreement on Reciprocal Trade or other tools as appropriate.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

Indonesia is advancing a third amendment to Law No. 32 of 2002 on Broadcasting that could extend legacy broadcasting regulation to internet-based audiovisual and over-the-top (OTT) services. During legislative deliberations in August 2026, lawmakers continued to consider provisions governing OTT platforms, including potential oversight of digital content and advertising. On September 8, 2026, the DPR formally approved the draft as a DPR initiative, advancing it to the next stage of the legislative process. Although the precise obligations applicable to OTT services remain under development, subjecting on-demand and internet-based services to regulatory frameworks designed for traditional broadcasters could impose licensing, content-control, and other burdens that do not reflect the fundamentally different business models and user relationships of digital services. USTR should urge Indonesia to maintain a clear distinction between traditional broadcasting and internet-delivered services and avoid extending legacy broadcasting requirements to U.S. streaming and digital-content providers.

Restrictions on Cross-Border Data Flows

The Indonesian Government enacted GR 33/2026⁶³⁷ on July 16, 2026, implementing the Personal Data Protection (PDP) Law, with enforcement from January 16, 2027. While its substantive requirements are broadly comparable to international frameworks such as the EU's GDPR, GR 33/2026 does not recognize international certifications, foreign standard contractual clauses (SCCs), or binding corporate rules approved in other jurisdictions — requiring instead Indonesian-specific instruments that do not yet exist. Every viable cross-border transfer mechanism is gated on the PDP Authority, which has not been established, creating a regulatory vacuum in which U.S. providers face enforcement risk but lack the legal tools to lawfully transfer data out of Indonesia. This compounds existing localization pressures under GR71 and

⁶³⁶ Office of the United States Trade Representative. (2026, February 19). Agreement Between the United States of America and the Republic of Indonesia on Reciprocal Trade, annex III, art. 3.3. <https://ustr.gov/sites/default/files/files/Press/Releases/2026/02.19.26%20US-IDN%20ART%20Full%20Agreement%20-%20US%20Final%20for%20Website%20sanitized.pdf>.

⁶³⁷ Nusantara DFDL. (2026). *Indonesia's Personal Data Protection Law*. <https://www.nusantaradfdl.com/insights/indonesia-personal-data-protection-law-gr-33-2026/>

sectoral financial data rules. The Law is now implemented via Government Regulation No. 33 of 2026 ("PP 33/2026"), effective January 16, 2027, which requires appointment of a data protection officer, completion of data protection impact assessments, strict breach- and data-subject-request response windows, and documented safeguards for cross-border data transfers, with fines of up to 2 percent of relevant business-variable revenue for non-compliance

Indonesia's Government Regulation No. 80/2019 (GR80) on E-Commerce draws a clear distinction between domestic and foreign e-commerce business actors, and prohibits personal data from being sent offshore unless otherwise approved by the Ministry of Trade through a list of countries which can store Indonesian e-commerce data. This effectively requires e-commerce business actors to store personal data for e-commerce customers locally. GR80 poses *de facto* data localization measures and local content requirements, which increase overhead costs for foreign entities and create undue market barriers. For SMEs seeking to serve the Indonesian market, such requirements may pose an insuperable barrier.

Indonesia's One Data Indonesia Bill (RUU Satu Data Indonesia or "RUU SDI") became law on October 6, 2026.⁶³⁸ The law establishes a national data governance framework requiring government ministries and agencies to share interoperable data on shared infrastructure. Several provisions pose significant market access barriers. The bill requires parliamentary approval for all cross-border data transfers — a requirement with no global equivalent and incompatible with real-time cloud operations. It prohibits inputting "strategic" data into AI systems "not under Indonesian legal sovereignty," an undefined term that effectively creates a national-origin restriction on AI capabilities regardless of security posture. The bill also includes discriminatory provisions including mandates for prioritization of domestic technology in security standards, and imposes data sovereignty audits without defined scope or methodology.

Taxation of Digital Products and Services

Indonesia issued Regulation No.17/PMK.010/2018 (Regulation 17) in 2018 to revise its tariff schedule.⁶³⁹ 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 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

⁶³⁸ Kompas. (2026). *Key points to Know about One Data Law*.

<https://go.kompas.com/read/2026/10/13/022147474/key-points-to-know-about-the-one-data-indonesia-law>

⁶³⁹ *Regulation No.17/PMK.010/2018* [Indonesia]. (2018).

<http://www.jdih.kemenkeu.go.id/fullText/2018/17~PMK.010~2018Per.pdf>.

back to 1998⁶⁴⁰ and most recently reaffirmed in June 2022.⁶⁴¹ In February 2026, the United States and Indonesia signed the Agreement on Reciprocal Trade (ART), under which Indonesia committed to eliminate existing tariff lines on “intangible products” and suspend related import-declaration requirements. USTR should ensure that Indonesia fully removes the relevant Chapter 99 tariff lines and associated import-declaration requirements and continues to support a permanent prohibition on customs duties on electronic transmissions at the WTO.

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.⁶⁴² 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 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 the 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.

In July 2025, Indonesia issued Ministry of Finance Regulation No. 37 of 2025 (PMK 37/2025), which requires designated online marketplaces to collect and remit income tax on transactions

⁶⁴⁰ WTO. (1998, May 25). *The Geneva ministerial declaration on global electronic commerce*. https://www.wto.org/english/tratop_e/ecom_e/mindecl_e.htm

⁶⁴¹ 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

⁶⁴² EY. (2020, March 19). *Indonesian Government proposes key tax changes*. <https://taxnews.ey.com/news/2020-0604-indonesian-government-proposes-key-tax-changes>.

conducted by domestic sellers through their platforms.⁶⁴³ After initially postponing implementation, the Directorate General of Taxes began implementing the regime on July 1, 2026, designating Blibli, Shopee, Tokopedia, and Lazada as collectors. Under the framework, marketplaces generally collect 0.5 percent of transaction value from qualifying domestic sellers, while individual sellers with annual gross turnover of Rp 500 million or less may claim an exemption by providing the required declaration. Although the government characterizes PMK 37/2025 as a collection mechanism for existing tax obligations rather than a new tax, shifting tax-collection, verification, recordkeeping, and reporting responsibilities onto online marketplaces creates additional operational and compliance burdens that do not apply in the same manner to traditional sales channels. USTR should monitor implementation to ensure that the regime does not discriminate against digital distribution channels, impose disproportionate liability on marketplace operators, or create unnecessary barriers to participation in Indonesia's e-commerce market.

Other Barriers to Digital Trade

Indonesia continues to maintain extensive local content requirements that restrict the ability of U.S. technology suppliers to compete on equal terms. Ministry of Industry Regulation No. 35 of 2025, which entered into force in December 2025 and replaced the previous framework under Regulation No. 16/M-IND/PER/2/2011, establishes revised methodologies for calculating domestic content.⁶⁴⁴ Of particular concern, the framework extends local-content obligations to "Industry 4.0 Support Services," including software, cloud, and related digital services. The calculation methodologies do not adequately account for the cross-border and intangible nature of these services, creating uncertainty regarding compliance and eligibility for government procurement. These requirements operate alongside broader domestic-product preferences, including Presidential Instruction No. 2 of 2022, and unclear e-catalogue classifications and implementing guidance continue to complicate participation by international cloud and technology suppliers.

⁶⁴³ Kementerian Keuangan Republik Indonesia [Ministry of Finance of the Republic of Indonesia]. (2025, July 14). Peraturan Menteri Keuangan Nomor 37 Tahun 2025 tentang Penunjukan Pihak Lain sebagai Pemungut Pajak Penghasilan serta Tata Cara Pemungutan, Penyetoran, dan Pelaporan Pajak Penghasilan yang Dipungut oleh Pihak Lain atas Penghasilan yang Diterima atau Diperoleh Pedagang Dalam Negeri dengan Mekanisme Perdagangan melalui Sistem Elektronik [Minister of Finance Regulation No. 37 of 2025 on the Designation of Other Parties as Income Tax Collectors and Procedures for the Collection, Remittance, and Reporting of Income Tax Collected by Other Parties on Income Received or Obtained by Domestic Sellers through Electronic Commerce]. Jaringan Dokumentasi dan Informasi Hukum, Badan Pemeriksa Keuangan. <https://peraturan.bpk.go.id/Details/322300/pmk-no-37-tahun-2025>.

⁶⁴⁴ Kementerian Perindustrian Republik Indonesia [Ministry of Industry of the Republic of Indonesia]. (2025, September 11). Peraturan Menteri Perindustrian Nomor 35 Tahun 2025 tentang Ketentuan dan Tata Cara Sertifikasi Tingkat Komponen Dalam Negeri dan Bobot Manfaat Perusahaan [Minister of Industry Regulation No. 35 of 2025 on Provisions and Procedures for Certification of Domestic Component Level and Company Benefit Weight]. Jaringan Dokumentasi dan Informasi Hukum, Badan Pemeriksa Keuangan. <https://peraturan.bpk.go.id/Details/333003/permenperin-no-35-tahun-2025>.

The February 2026 U.S.-Indonesia Agreement on Reciprocal Trade provides an important pathway for resolving these barriers. Annex III, Article 2.2 commits Indonesia to exempt U.S. companies and U.S. goods from local content requirements and to remove forced domestic specification and processing requirements.⁶⁴⁵ Because the Agreement remains pending, and has not entered into force, USTR should closely monitor implementation and ensure that the exemption is applied comprehensively, including to U.S. software, cloud, data-center, telecommunications, and other technology suppliers participating in Indonesian public procurement. Indonesia should also ensure that implementing regulations under Regulation No. 35 of 2025 do not recreate equivalent preferences through certification, scoring, procurement eligibility, or other indirect requirements.

In June 2026, Indonesia issued Minister of Trade Regulation No. 19 of 2026 on Electronic Commerce, replacing Regulation No. 31/2023 and maintaining significant restrictions on foreign e-commerce providers.⁶⁴⁶ Foreign electronic commerce operators that meet specified thresholds—including at least 1,000 transactions or 1,000 shipments to Indonesian consumers annually, or traffic equivalent to at least 1% of domestic internet users—must appoint a representative in Indonesia through a Foreign Trading Company Representative Office (KP3A). The regulation also maintains a minimum price of \$100 per unit for finished goods sold directly from abroad to Indonesian consumers through electronic commerce platforms. In addition, social-commerce providers are prohibited from facilitating payment transactions directly through their electronic systems, and marketplace and social-commerce providers may not act as producers.

Regulation No. 19/2026 also strengthens requirements favoring domestic products. Covered platforms must configure search, recommendation, and ranking systems to prioritize Indonesian products, including by displaying domestic products in the first row of the first page of results, and must provide dedicated promotional space for domestically produced goods and services.⁶⁴⁷ These requirements constrain the ability of U.S. e-commerce suppliers to structure their services and recommendation systems according to commercial considerations and disadvantage foreign

⁶⁴⁵ Office of the United States Trade Representative. (2026, February 19). Agreement Between the United States of America and the Republic of Indonesia on Reciprocal Trade, annex III, art. 3.2. <https://ustr.gov/sites/default/files/files/Press/Releases/2026/02.19.26%20US-IDN%20ART%20Full%20Agreement%20-%20US%20Final%20for%20Website%20sanitized.pdf>.

⁶⁴⁶ Ministry of Trade of the Republic of Indonesia. (2026, June 8). Minister of Trade Regulation No. 19 of 2026 on the Conduct of Trading Business through Electronic Systems. <https://peraturan.bpk.go.id/Details/351720/permendag-no-19-tahun-2026>.

⁶⁴⁷ Kementerian Perdagangan Republik Indonesia [Ministry of Trade of the Republic of Indonesia]. (2026, June 8). Peraturan Menteri Perdagangan Nomor 19 Tahun 2026 tentang Penyelenggaraan Usaha Perdagangan melalui Sistem Elektronik [Minister of Trade Regulation No. 19 of 2026 on the Conduct of Trading Business through Electronic Systems], art. 40(3). Jaringan Dokumentasi dan Informasi Hukum, Badan Pemeriksa Keuangan. <https://peraturan.bpk.go.id/Details/351720/permendag-no-19-tahun-2026>.

products and suppliers in the Indonesian market. USTR should urge Indonesia to eliminate discriminatory local-presence, product-prioritization, and cross-border e-commerce restrictions.

Iraq

Government-Imposed Content Restrictions and Related Access Barriers

On July 16, 2026, Iraq’s Communications and Media Commission (CMC) approved Board Decision Annex 2 to the 2025 Framework Regulation for Digital Platforms. Annex 2 establishes a rigid notice-and-takedown regime requiring online platforms to execute content removal and geo-blocking within 3 days for non-live content and immediately (within hours) for live-streaming content upon administrative notice. Crucially, the regulation makes safe harbor conditional, allowing the CMC to revoke liability protections if a platform receives indirect revenue benefits or fails to prevent content re-uploads. Non-compliant platforms face graduated fines of up to 150 million IQD (~USD \$115,000) and mandatory account blocking. Requiring near-instant removals on live streams is technically unfeasible. CCIA urges USTR to push for the restoration of unconditional intermediary safe harbors and the removal of unfeasible live-stream takedown mandates.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The CMC’s Framework Regulations for Registration of Smart Phone Apps mandate that foreign application developers and digital service providers store user data locally within Iraqi data centers and appoint a local legal representative as a condition of market entry. CCIA urges USTR to press Iraq to eliminate mandatory local presence and data localization requirements.

Ireland

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Ireland’s restrictions on new data center grid connections have constrained infrastructure expansion, particularly around Dublin. On December 12, 2025, the Commission for Regulation of Utilities finalized its Large Energy Users Connection Policy, and EirGrid has since published its implementing connection process.⁶⁴⁸ Under the new policy, data centers seeking connections of at least 1 MVA must meet at least 80% of annual electricity demand with additional renewable electricity generated in Ireland within six years of energization. Connection approval remains subject to location-specific network constraints. These requirements provide a route to new connections while imposing additional infrastructure costs and development dependencies on

⁶⁴⁸ Philip Lee LLP. (2026, July 10). *EirGrid DCCOPP Version 3: What Data Centre Operators Need to Know*. <https://www.philiplee.ie/eirgrid-dccopp-version-3-what-data-centre-operators-need-to-know/>; EirGrid. (2026, May 20). *Data Centre Connection Offer Process and Policy: Version 3*. <https://cms.eirgrid.ie/sites/default/files/publications/Data-Centre-Connection-Offer-Process-and-Policy-V3-May-2026.pdf>

U.S. cloud providers. In April 2026, Friends of the Earth Ireland, ClientEarth, and Friends of the Irish Environment announced a High Court challenge to the policy, alleging incompatibility with climate and environmental-assessment obligations.⁶⁴⁹

In September 2023, Ireland's Office of Government Procurement launched a €60 million public-sector cloud infrastructure tender.⁶⁵⁰ By January 2024, the competition had been canceled because too few compliant tenders were received. Technology Ireland, whose members include major U.S. cloud providers, had warned that the proposed terms created fundamental obstacles to participation and risked undermining public-sector cloud procurement. Ireland published updated cloud-computing and procurement guidance in May 2025 to support public-sector cloud adoption.⁶⁵¹ Procurement uncertainty nevertheless continued: in July 2026, the government confirmed cancellation of a separate proposed framework for Microsoft software and services following concerns raised by an interested party, while indicating that a revised competition would be issued.⁶⁵² Ireland should ensure that cloud procurement terms are commercially workable and that security requirements are proportionate and applied without discrimination against U.S. providers.

Ireland's electricity regulator, the Commission for the Regulation of Utilities (CRU), has approved grid-connection rules that unfairly penalize U.S. cloud providers that invested in Ireland in good faith under the connection agreements and grid standards in force at the time. In September 2026, the CRU approved EirGrid Grid Code Modification MPID 345 (Fault Ride Through, Rate of Change of Frequency, and Post-Fault Active Power Recovery for Demand Facilities), taking legal effect in October 2026. The modification requires large demand facilities — predominantly U.S.-operated data centers — to remain connected to the grid during transmission faults and to restore pre-fault demand within milliseconds, behaving like electricity generators. Critically, these obligations are imposed retrospectively on existing facilities. Every operational U.S. data center in Ireland was designed, built and connected in full compliance with the Grid Code standards and connection agreements applicable at the time, when Fault Ride Through obligations applied only to generators on the supply side and demand-side backup systems were specifically engineered — and approved by the grid operator — to disconnect safely during voltage disturbances to protect sensitive IT equipment. Applying generation-style

⁶⁴⁹ James, N. (2026, April 27). *Friends of the Earth is suing Ireland's energy regulator*. Friends of the Earth Ireland. <https://www.friendsoftheearth.ie/news/friends-of-the-earth-is-suing-irelands-energy-regulator/>

⁶⁵⁰ Butler, G. (2024, January 16). *Ireland cancels €60m public sector cloud computing tender*. Data Center Dynamics. <https://www.datacenterdynamics.com/en/news/ireland-cancels-60m-public-sector-cloud-computing-tender/>

⁶⁵¹ Office of Government Procurement. (2025, May 21). *Cloud Services Procurement Guidance Note 2025 Update*. <https://www.gov.ie/en/office-of-government-procurement/publications/cloud-services-procurement-guidance-note-2025-update/>

⁶⁵² Clark, L. (2026, July 22). *Ireland stalls €1B Microsoft tender amid digital sovereignty questions*. The Register. <https://www.theregister.com/public-sector/2026/07/22/ireland-stalls-1b-microsoft-tender-amid-digital-sovereignty-questions/5276149>

FRT duties retrospectively to demand customers is, to the industry's knowledge, without international precedent in any other jurisdiction, and reverses the very design parameters operators were previously required to meet. USTR should press for the revision of these rules.

Other Barriers - Firm-specific Regulatory Fees

As the predominant regulatory hub for many U.S. multinational companies entering the EU market, Ireland exercises regulatory supervision over numerous platforms and services operating in the country. Irish regulatory authorities have increasingly moved toward funding this supervision through per-service levies on supervised companies rather than through exchequer appropriations, creating new compliance costs for U.S. companies based in Ireland. For example, Ireland's media and online safety regulator, Coimisiún na Meán (CnaM), receives no exchequer funding and calculated an operating budget of approximately €55 million for 2025, funded entirely through supervisory levies.⁶⁵³ The scope of these levies continues to expand alongside Ireland's growing regulatory responsibilities under multiple EU regimes, including the Digital Services Act (DSA), the Data Act, and the AI Act. U.S. stakeholders report that the resulting levies are duplicative, lack transparency, and are not subject to any caps.⁶⁵⁴ This levy structure disadvantages U.S. companies based in Ireland relative to competitors based in other EU member states with lower comparable supervisory fees, and represents a significant outlier relative to supervisory-fee regimes in other markets. As with similar levies imposed at the EU level (e.g., for the DSA), USTR should evaluate the consistency of such fees with Ireland's obligations under Article 9 of the GATS Reference Paper on Domestic Regulation.⁶⁵⁵

⁶⁵³ Coimisiún na Meán. (2025). *2025 Estimates and Levy Calculation Table*.
<https://www.cnam.ie/app/uploads/2025/05/2025-Estimates-and-Levy-Calculation-Table.pdf>.

⁶⁵⁴ Technology Ireland (2026, July), *Reducing frictions, optimizing interplay: Exploring the digital regulatory landscape*, p. 44, <https://www.ibec.ie/technologyireland/influence/reducing-frictions-optimising-interplay>.

⁶⁵⁵ World Trade Organization. (2021). *Reference Paper on Services Domestic Regulation*.
<https://docs.wto.org/dol2fe/Pages/SS/directdoc2.aspx?filename=q%3a%2fWT%2fL%2f1129.pdf&Open=True>.

Italy

Asymmetric Platform Regulation

In 2022, Law No. 118, the “2021 Annual Competition Law,” went into effect,⁶⁵⁶ including the digital-platform amendments.⁶⁵⁷ The latter creates a rebuttable presumption of economic dependency where a business uses intermediation services provided by a digital platform that plays a “determining role” in reaching end users or suppliers, including through network effects or data availability. The law identifies possible abuses, including insufficient information about the service’s scope or quality, unjustified unilateral obligations, and practices that inhibit or obstruct the use of alternative providers, including unilateral conditions or additional costs not provided for in existing contracts or licenses. Based on these changes, the Italian Competition Authority now has the power to demand information from specific digital platforms even without launching a formal proceeding.⁶⁵⁸

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Italy’s AI Law No. 132/2025, effective October 10, 2025, introduces localization concerns.⁶⁵⁹ Article 5(1)(d) directs public e-procurement platforms to allow preferences for AI solutions that store and process strategic data in Italy and maintain disaster-recovery and business-continuity infrastructure domestically. This preference could disadvantage U.S. suppliers relying on infrastructure outside Italy.

The Ministry of Culture's current interpretation of the Italian Cultural Heritage Code (D.Lgs. 42/2004) categorizes public archives (including school records and educational documentation) as “cultural heritage” under Italian law and effectively restricts the storage and transfer of digitalized public documents outside Italian territory. The lack of clear harmonization between cultural heritage protection requirements and modern cloud computing needs creates an obstacle to digital trade, particularly impacting non-EU cloud providers seeking to serve Italian schools and educational institutions. USTR should evaluate whether this restriction is consistent with Italy’s obligations under the WTO GPA.

⁶⁵⁶ 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/>

⁶⁵⁷ Gazzetta Ufficiale. (2022, August 12). *Legge 5 agosto 2022, n. 118—Legge annuale per il mercato e la concorrenza 2021*, Article 33(2). <https://www.gazzettaufficiale.it/eli/id/2022/08/12/22G00126/SG>

⁶⁵⁸ 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/>

⁶⁵⁹ Gazzetta Ufficiale. (2025, September 25). *Legge 23 settembre 2025, n. 132—Disposizioni e deleghe al Governo in materia di intelligenza artificiale*, Article 5(1)(d).

<https://www.gazzettaufficiale.it/eli/id/2025/09/25/25G00143/SG>

Discriminatory Local Content Quotas and Audiovisual Services Mandates

Italy's Legislative Decree No. 208/2021, as amended by Legislative Decree No. 50/2024, requires covered on-demand audiovisual providers to invest 16% of their annual net revenues in Italy in European works produced by independent producers.⁶⁶⁰ Of that investment, 70% is reserved for works of original Italian expression produced by independent producers within the preceding five years, equivalent to 11.2% of relevant revenues. Although the 2024 amendment reduced the overall investment requirement from 20%, it increased the Italian sub-quota from 50% to 70%, further constraining providers' allocation of production investment.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Italy launched its Piracy Shield on February 1, 2024, initially to combat unauthorized broadcasts of live sporting events.⁶⁶¹ Following an initial order from the Italian Communications Regulatory Authority (AGCOM), rightsholders can submit additional domain names and IP addresses through the platform, triggering obligations to block access within 30 minutes of notification. CCIA has warned about the over blocking effects of such a platform,⁶⁶² leading to serious disruptions of legitimate services, which are now well documented.⁶⁶³

AGCOM adopted Resolution No. 209/25/CONS on July 30, 2025, effective September 15, 2025, extending Piracy Shield's expedited blocking mechanism to all live audiovisual content and to intermediaries other than ISPs, including VPN providers and public DNS resolvers.⁶⁶⁴ Industry concerns about overblocking and procedural safeguards persisted following adoption. On January 8, 2026, AGCOM announced a fine exceeding €14 million against Cloudflare, equivalent to 1% of its global turnover, for failing to register under Privacy Shield, despite an outstanding legal challenge regarding the scope of the measure.⁶⁶⁵ Cloudflare appealed the fine on March 8, 2026, arguing that the system lacks adequate transparency, safeguards, and effective

⁶⁶⁰ Gazzetta Ufficiale. (2024, April 17). *Decreto legislativo 25 marzo 2024, n. 50—Disposizioni integrative e correttive del decreto legislativo 8 novembre 2021, n. 208*, Article 1 (replacing Article 55 of Legislative Decree No. 208/2021). <https://www.gazzettaufficiale.it/eli/id/2024/04/17/24G00067/SG>

⁶⁶¹ AGCOM. (n.d.). *Piattaforma Piracy Shield*.

<https://www.agcom.it/competenze/antipirateria-e-piracy-shield/piattaforma-piracy-shield>

⁶⁶² 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/>

⁶⁶³ Sommesse, 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/>

⁶⁶⁴ AGCOM. (2025, July 30). *Delibera n. 209/25/CONS—Modifiche al regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70 di cui alla delibera n. 680/13/CONS*. <https://www.agcom.it/provvedimenti/delibera-209-25-cons>

⁶⁶⁵ AGCOM. (2026, January 8). *Sanzione di oltre 14 milioni di euro a Cloudflare per violazione delle norme antipirateria*. <https://www.agcom.it/comunicazione/comunicati-stampa/comunicato-stampa-71>

redress against erroneous blocking.⁶⁶⁶ In judgment No. 13201/2026, published July 17, 2026, the Lazio Regional Administrative Court rejected Cloudflare’s challenges, leaving the blocking order and fine in place.⁶⁶⁷ The court also rejected the overblocking challenge for lack of proof concerning the resources covered by the contested order.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

AGCOM’s Resolution No. 207/25/CONS, adopted July 30, 2025, and published August 5, extends the general authorization regime for telecommunications networks to CDN providers and content and application providers that own, operate, or control CDN infrastructure in Italy.⁶⁶⁸ Telecommunications networks (ECNs, or electronic communications networks in EU parlance) are a regulated service subject to binding arbitration in the event of a dispute between market participants. Exposure to AGCOM’s dispute-resolution powers raise concerns that ISPs could seek regulated payments for content delivery, treating internet traffic exchange like traditional carrier-to-carrier interconnection. Although the resolution does not itself establish a network usage fee, a dispute resolution process could result in a mandatory fee, undermining the principle of settlement-free peering that has governed internet traffic exchange globally for the past 30 years. Such an outcome would be inconsistent with the EU’s bilateral commitment to the United States not to impose such changes. Accordingly, implementation of this measure warrants careful monitoring. Several U.S. firms have filed appeals in Italian court against the AGCOM resolution; these cases are still pending.

Other Barriers to Digital Trade

The EU’s 2001 InfoSoc Directive requires Member States to ensure “fair compensation” to rightsholders for private copies of copyright-protected content. As a result, most Member States impose a surcharge on electronic devices and recording media to compensate rightsholders for personal copies of their work, under the assumption these devices and media will be used to reproduce copyright-protected content for private use. While Italy’s private copy compensation system (*compenso per copia privata*) was originally designed for cassette recorders, CDs, hard drives and smartphones capable of storing copyrighted works, the Government adopted a decree extending this system to cloud storage services, introducing recurring charges for remote digital storage. The revised compensation system is being subject to judicial review, and has not yet been implemented. USTR should advocate for the removal of this obsolete measure.

⁶⁶⁶ Nemeroff, P., & Terrell, E. (2026, March 16). *Standing up for the open Internet: why we appealed Italy’s “Piracy Shield” fine*. Cloudflare. <https://blog.cloudflare.com/standing-up-for-the-open-internet/>

⁶⁶⁷ Tribunale Amministrativo Regionale per il Lazio, Sezione Quarta. (2026, July 17). *Sentenza n. 13201/2026, Cloudflare Inc. c. AGCOM*. https://www.previdi.it/storage/app/media/Documenti%20da%20condividere/202613201_01.pdf

⁶⁶⁸ AGCOM. (2025, July 30). *Delibera 207/25/CONS—Riconoscimento delle condizioni di applicabilità del regime di autorizzazione generale previsto dal Codice delle comunicazioni elettroniche alle Content Delivery Network (CDN)*. <https://www.agcom.it/provvedimenti/delibera-207-25-cons>

Taxation of Digital Products and Services

Italy's 2020 Budget introduced a 3% digital services tax closely aligned with the EU's original proposal. The tax took effect on January 1, 2020.⁶⁶⁹ Effective January 1, 2025, Italy eliminated the €5.5 million domestic digital-services revenue threshold while retaining the €750 million worldwide revenue threshold, expanding coverage to qualifying businesses regardless of the amount of their taxable Italian digital-services revenues.⁶⁷⁰ The tax applies to revenue derived from the specified 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 goods and services);” and the “transmission of data collected from users and generated by the use of a digital interface.”⁶⁷¹ USTR's Section 301 investigation concluded that Italy's DST discriminates against U.S. companies and burdens U.S. commerce.⁶⁷² According to CCIA's analysis, Italy collected approximately \$720 million in DST receipts in 2025 and \$2.23 billion cumulatively from 2021-2025.⁶⁷³ U.S. officials should continue pressing Italy to repeal the discriminatory tax. USTR should consider refreshing the record on its Section 301 finding and consider use of trade tools to incentivize the removal of this measure..

Effective January 1, 2026, Law No. 199/2025 reformed AGCOM's funding contributions, expressly classifying them as taxes.⁶⁷⁴ Covered digital services and intermediaries—including e-commerce services, hosting services, and online platforms—are subject to an annual contribution of 0.2% of their Italian revenues, including revenues booked by companies abroad. Separately, on July 27, 2026, the Lazio Regional Administrative Court annulled the earlier 2023 contribution measures as applied to Meta Platforms Ireland on country-of-origin grounds; but

⁶⁶⁹ Office of the United States Trade Representative. (2021, January 6). *Section 301 Investigation: Report on Italy's Digital Services Tax*.

<https://ustr.gov/sites/default/files/enforcement/301Investigations/Report%20on%20Italy%E2%80%99s%20Digital%20Services%20Tax.pdf>

⁶⁷⁰ Gazzetta Ufficiale. (2024, December 31). *Legge 30 dicembre 2024, n. 207—Bilancio di previsione dello Stato per l'anno finanziario 2025 e bilancio pluriennale per il triennio 2025–2027*, Article 1(21)(a).

<https://www.gazzettaufficiale.it/eli/id/2024/12/31/24G00229/SG>

⁶⁷¹ 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>.

⁶⁷² Office of the United States Trade Representative. (2021, January 6). *Section 301 Investigation: Report on Italy's Digital Services Tax*.

<https://ustr.gov/sites/default/files/enforcement/301Investigations/Report%20on%20Italy%E2%80%99s%20Digital%20Services%20Tax.pdf>

⁶⁷³ CCIA. (2026, July 23). *2026 Status of Key Digital Services Taxes*.

<https://ccianet.org/library/2026-status-of-key-digital-services-taxes/>

⁶⁷⁴ Gazzetta Ufficiale. (2025, December 30). *Legge 30 dicembre 2025, n. 199—Bilancio di previsione dello Stato per l'anno finanziario 2026 e bilancio pluriennale per il triennio 2026–2028*, Article 1(273).

<https://www.gazzettaufficiale.it/eli/id/2025/12/30/25G00212/SG>

that judgment was based on the pre-2026 framework.⁶⁷⁵ Although regulators’ reliance on funding from entities they regulate is not uncommon, the fact that companies not subject to explicit regulation must pay this tax raises fundamental questions of fairness and good regulatory policy.

Italy has pursued VAT assessments against Meta, X, and LinkedIn on the novel theory that access to free social-media services constitutes a taxable exchange for users’ personal data—despite the fact that no monetary exchange occurs.⁶⁷⁶ The companies appealed this decision in July 2025. In November 2025, a European Commission working paper prepared for the VAT Committee emphasized that taxation requires a direct link between the service and the data supplied, with case-specific analysis where service levels vary.⁶⁷⁷ This disputed approach creates substantial tax uncertainty for U.S. providers offering advertising-supported services and merits close monitoring, given its global implications.

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.”⁶⁷⁸ It 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 periodical review to account for changes in market and technological conditions. The Act can impose significant compliance burdens on U.S. firms through detailed reporting requirements, recurring ministerial evaluations, and opaque supervisory processes. Although U.S. firms remain heavily represented among designated providers, Japan has also designated Japanese and other non-U.S. providers, and the concern is therefore more appropriately framed around disproportionate regulatory burdens and the manner in which the regime is implemented. USTR should urge Japan to align implementation of the TFDPA with its legislative mandate of “minimum necessary measures” and ensure that oversight

⁶⁷⁵ Tribunale Amministrativo Regionale per il Lazio. (2026, July 27). *Sentenza n. 13720/2026, Meta Platforms Ireland c. AGCOM*. https://mdp.giustizia-amministrativa.it/visualizza/?nomeFile=202613720_01.docx&nrg=202306657&schema=tar_r m&subDir=Provvedimenti

⁶⁷⁶ Parodi, E. (2025, July 21). *Meta, X and LinkedIn appeal unprecedented VAT claim by Italy*. Reuters. <https://www.reuters.com/world/europe/meta-x-linkedin-appeal-unprecedented-vat-claim-by-italy-2025-07-21/>

⁶⁷⁷ European Commission, Directorate-General for Taxation and Customs Union. (2025, November 11). *Working Paper No. 1118: VAT treatment of IT services provided in exchange for the provision of users’ personal data*. <https://www.vatupdate.com/wp-content/uploads/2025/11/WP-1118-Italian-question-on-IT-services-in-exchange-for-users-personal-data.pdf>

⁶⁷⁸ *Act on Improving Transparency and Fairness of Digital Platforms* [Japan], Act No. 38. (2020). <https://www.japaneselawtranslation.go.jp/ja/laws/view/4532/en>

is transparent, proportionate, and nondiscriminatory, avoiding unnecessary administrative burdens and overly prescriptive ministerial evaluations.

On July 5, 2022, METI released a Cabinet Order stipulating that the digital advertising sector would be regulated under the TFDPA.⁶⁷⁹ 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.⁶⁸⁰ METI has continued to conduct recurring evaluations under the TFDPA. In June 2025, TikTok Pte. Ltd. was added as a Specified Digital Platform Provider in the media-integrated digital advertising category.⁶⁸¹ In December 2025, METI published its fourth evaluation of comprehensive online shopping malls and app stores and its third evaluation of digital advertising,⁶⁸² and the Ministry continued its monitoring process in 2026. These recurring reporting and evaluation processes reinforce the need for predictable, transparent, and proportionate administration of the TFDPA, particularly where ministerial assessments can generate additional compliance expectations beyond the statute's express requirements.

In June 2024, Japan's Diet enacted the Act on Promotion of Competition for Specified Software Used in Smartphones, commonly referred to by the JFTC as the Mobile Software Competition Act (MSCA).⁶⁸³ The law was promulgated on June 19, 2024 and entered fully into force on December 18, 2025. In March 2025, the JFTC designated Apple Inc., iTunes K.K., and Google LLC, bringing two U.S.-headquartered corporate groups within the regime across specified mobile operating systems, app stores, browsers, and search engines.⁶⁸⁴ No Japanese or other

⁶⁷⁹ 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

⁶⁸⁰ 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

⁶⁸¹ METI. (2025, June 27). *TikTok Pte. Ltd.*を「特定デジタルプラットフォームの透明性及び公正性の向上に関する法律」の規制対象事業者として指定しました [TikTok Pte. Ltd. designated as a regulated business operator under the Act on Improving Transparency and Fairness of Digital Platforms]. <https://www.meti.go.jp/press/2025/06/20250627002/20250627002.html>

⁶⁸² METI. (2025, December 17). *Evaluation of Transparency and Fairness for Specified Digital Platforms Compiled*. https://www.meti.go.jp/english/press/2025/1217_003.html

⁶⁸³ Japan Fair Trade Commission. (2024, June 12). *Regarding the Passage of the Act on Promotion of Competition for Specified Smartphone Software*. <https://www.jftc.go.jp/en/pressreleases/yearly-2024/June/240612.html>

⁶⁸⁴ Japan Fair Trade Commission. (2025, March 31). *Designation of Specified Software Operators under the Act on Promotion of Competition for Specified Smartphone Software*. <https://www.jftc.go.jp/en/pressreleases/yearly-2025/March/250331.html>

competing provider met the applicable designation thresholds, despite evidence that they should have been, demonstrating how the quantitative designation threshold targets only U.S.-based firms. The JFTC finalized implementing regulations and guidelines in July 2025⁶⁸⁵ and has since begun active administration of the law, including publication of designated providers' compliance reports in 2026.⁶⁸⁶

For designated companies, the MSCA 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 MSCA 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 MSCA seeks to prohibit. For example, two companies, Nintendo and Sony, control 99% of the console gaming market in Japan (approximately 70% and 29%, respectively).⁶⁸⁷ 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.⁶⁸⁸ 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, as

⁶⁸⁵ Japan Fair Trade Commission. (2025, July 29). *Subordinate Legislations and Guidelines of the Act on the Promotion of Competition for Specified Smartphone Software (Mobile Software Competition Act (MSCA))*. <https://www.jftc.go.jp/en/pressreleases/yearly-2025/July/250729.html>

⁶⁸⁶ Japan Fair Trade Commission. (2026, July 27). スマホソフトウェア競争促進法に基づく遵守報告書の公表について [Publication of compliance reports under the Mobile Software Competition Act]. https://www.jftc.go.jp/houdou/pressrelease/2026/jul/260727_sumaho_junshuhoukoku.html

⁶⁸⁷ Knezovic, A. (2025, August 29). *Japanese Gaming Market*. Udonis. <https://www.blog.udonis.co/mobile-marketing/mobile-games/japanese-gaming-market>

⁶⁸⁸ Statista. (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/>

well as Japan’s commitment under the 2025 U.S. Japan Framework Agreement to implement the MSCA in a way that does not discriminate against U.S. companies, balances the need for fair and free competition with user safety and convenience, and respects the legitimate exercise of intellectual property rights.⁶⁸⁹

Customs-related Restrictions and Import Barriers for Goods

Japan is considering changes to its customs duty exemption for low-value imports. Eliminating the customs de minimis threshold could impose disproportionate administrative and compliance costs on low-value cross-border shipments, particularly affecting U.S. small businesses and individual exporters. Japan should preserve an appropriate customs de minimis threshold and ensure that any reforms facilitate legitimate low-value trade without creating unnecessary customs burdens.

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.⁶⁹⁰ 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, METI approved up to ¥72.5 billion in subsidies across five projects under the Economic Security Promotion Act to expand domestic GPU cloud computing resources for generative AI. The recipients included Sakura Internet, GMO Internet Group, KDDI, RUTILEA and AI Fukushima, and Highreso and Highreso Kagawa. In May 2024, METI separately approved up to ¥42.1 billion in support for SoftBank. Japan subsequently established its AI and Semiconductor Industrial Infrastructure Strengthening Framework, under which the government plans to provide more than ¥10 trillion in public support through Fiscal Year 2030. These initiatives are explicitly intended to expand domestically controlled computing capacity and reduce reliance on overseas cloud infrastructure. Given the scale and strategic importance of this support, USTR should encourage Japan to administer AI and cloud subsidies according to transparent, technology-neutral, and nondiscriminatory criteria that allow qualified U.S. suppliers to compete on equal terms.

In May 2024, Japan passed the Act on the Protection and Utilization of Important Economic Security Information (CESI Act),⁶⁹¹ establishing a new security clearance framework intended to protect sensitive government information tied to national security. The law, which came into

⁶⁸⁹ The White House. 2025. *Fact Sheet*. <https://www.whitehouse.gov/fact-sheets/2025/10/28195/>.

⁶⁹⁰ *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/jc>

⁶⁹¹ *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>

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 barrier for modern, highly secure cloud solutions offered by U.S. providers. 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.

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.⁶⁹² 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. Japan has taken steps toward modernizing defense information infrastructure, including updates to ATLA’s information-security requirements,⁶⁹³ expansion of the Defense Security Gateway for secure electronic information sharing,⁶⁹⁴ and development of the MOD Cloud.⁶⁹⁵ These initiatives represent progress away from exclusively stand-alone information environments. USTR should encourage Japan to move toward risk-based and technology-neutral requirements that evaluate security outcomes rather than

⁶⁹² 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

⁶⁹³ Acquisition, Technology & Logistics Agency, Ministry of Defense. (2025, June 3). 装備品等及び役務の調達における情報セキュリティ基準について [Information Security Standards for the Procurement of Equipment and Services]. <https://www.mod.go.jp/atla/cybersecurity.html>

⁶⁹⁴ Acquisition, Technology & Logistics Agency, Ministry of Defense. (2025, August 13). 防衛セキュリティゲートウェイ (DSG) [Defense Security Gateway (DSG)]. <https://www.mod.go.jp/atla/dsg.html>

⁶⁹⁵ Ministry of Defense. (2026). *FY2026 Budget: Major Projects*. https://www.mod.go.jp/en/d_act/d_budget/pdf/fy2026_20251226a.pdf

prescribing particular physical architectures, thereby enabling qualified U.S. cloud providers to compete for sensitive public-sector and defense workloads.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Japan's Act on Measures Against Rights Infringement, etc. Arising from Distribution of Information by Specified Telecommunications, commonly referred to as the Information Distribution Platform Act, establishes liability protections for internet and telecommunications service providers while providing mechanisms for individuals whose rights are infringed to seek disclosure of sender information.⁶⁹⁶ Formerly known as the Provider Liability Limitation Act, the law was substantially amended in 2024, with the amendments taking effect on April 1, 2025.⁶⁹⁷ In addition to retaining existing intermediary-liability protections and sender-identification disclosure procedures, the amended law imposes new obligations on designated large-scale service providers to establish and publicize procedures for removal requests, maintain systems for processing such requests, provide timely decisions and notifications, publish content-removal standards, and disclose information regarding their moderation practices. These requirements increase the compliance obligations applicable to large online platforms and bear monitoring to ensure that they preserve meaningful intermediary-liability protections and avoid excessive or disproportionate burdens on foreign providers.

Challenges to the Development of AI

On August 25, 2026, Japan's Intellectual Property Strategy Headquarters finalized the Principle-Code for Protection of Intellectual Property and Transparency for the Appropriate Use of Generative AI, a soft-law framework developed under the Act on Promotion of Research, Development and Utilization of Artificial Intelligence-Related Technologies.⁶⁹⁸ The Principle-Code follows a "comply-or-explain" model and applies to generative AI systems and services offered in Japan, including those provided by companies located outside Japan. It calls for public disclosures concerning AI models, training data, and intellectual property protection practices and establishes processes for responding to certain information requests from rightsholders and users concerning particular content or URLs. Japan clarified in the final framework that the Principle-Code is not legally binding and does not require disclosure of trade secrets or safety- and security-sensitive information. Nevertheless, its broad scope, detailed transparency expectations, and dispute-triggered disclosure mechanisms could impose

⁶⁹⁶ Information Distribution Platform Act (IDPA) (Partial Amendment of the Provider Liability Limitation Act) [Japan]. (2024). <https://www.japaneselawtranslation.go.jp/outline/120/905R620.pdf>

⁶⁹⁷ Act to Partially Amend the Act on the Limitation of Liability of Specified Telecommunications Service Providers for Damages and the Right to Demand Disclosure of Sender Identification Information [Japan], Act No. 25 of 2024. (2024). <https://www.japaneselawtranslation.go.jp/outline/120/905R620.pdf>

⁶⁹⁸ Intellectual Property Strategy Headquarters, Cabinet Secretariat, Japan. (2026, August 25). Principle-Code for Protection of Intellectual Property and Transparency for the Appropriate Use of Generative AI. https://www.cas.go.jp/jp/seisakukaigi/titeki2/ai_principle_code/index.html

substantial operational burdens on globally operating developers and providers. In particular, individualized requests concerning whether specific material was used in model training may be technically infeasible at scale, while Japan-specific disclosure requirements risk fragmenting globally interoperable AI governance. These mechanisms should also not undermine the legal certainty Japan has historically provided for lawful data analysis and machine learning under its Copyright Act.⁶⁹⁹ USTR should encourage Japan to implement the Principle-Code in a genuinely voluntary, technologically feasible, and proportionate manner; protect proprietary and security-sensitive information; recognize equivalent internationally aligned transparency practices; and avoid requirements for source-level attribution that providers cannot reasonably produce.

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).⁷⁰⁰ Japan's FY2026 tax reform expanded the platform taxation regime to certain cross-border e-commerce transactions involving goods, with the new requirements scheduled to take effect on April 1, 2028.⁷⁰¹ Under the revised framework, designated "Type II Platform Businesses" that facilitate covered sales and collect payment will be deemed to make the supply and will be responsible for filing and remitting consumption tax. The designation threshold is ¥5 billion in covered transactions. The reform also subjects certain low-value goods valued at ¥10,000 or less, excluding tax, and shipped from outside Japan to consumption tax as domestic supplies. USTR should encourage Japan to implement these requirements transparently, proportionately, and on a nondiscriminatory basis, while minimizing unnecessary compliance burdens on U.S. platforms and cross-border sellers.

Jordan

Taxation of Digital Products and Services

Jordan's Income and Sales Tax Department (ISTD) initiated an implementation roadmap requiring foreign digital service providers to register for and remit Value Added Tax (VAT) on electronic services supplied to Jordanian consumers. Requiring foreign digital providers without a physical presence to navigate complex tax compliance mechanisms can act as a barrier to

⁶⁹⁹ *Copyright Act* [Japan], Act No. 48 of 1970, art. 30-4.

<https://www.japaneselawtranslation.go.jp/en/laws/view/4207/en>

⁷⁰⁰ Japan National Tax Agency. (n.d.). *Platform Taxation of Consumption Tax*.

https://www.nta.go.jp/english/taxes/consumption_tax/05.htm

⁷⁰¹ 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/>

digital trade.⁷⁰² CCIA urges USTR to encourage Jordan to adopt simplified, alignment-focused digital VAT registration portals to minimize such burdens.

Kazakhstan

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Article 12(2) of the Law on Personal Data and Its Protection (No. 94-V), as amended in 2026, requires owners, operators, and third parties to store personal data in a database and/or digital object located in Kazakhstan, affecting both domestic and foreign providers.⁷⁰³ Additionally, Order No. 38/NK requires internet resources associated with domain names in the Kazakhstani internet segment to be hosted on hardware and software located in Kazakhstan; hosting those resources abroad is grounds for suspension of the domain name.⁷⁰⁴ 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.⁷⁰⁵ 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.

Amendments effective August 25, 2026 (Article 7 (3-1) also require persons processing personal data to obtain the consent of the data subject for processing data even if the subject has already made that data publicly available.⁷⁰⁶ Revised rules provide for anonymizing personal data and regulated procedures for exporting personal data. The same amendments introduced advance notification by large-scale processors to the authorized body before beginning or ceasing any personal-data processing, exempting processors classified as small or medium. Notifications must disclose, among other matters, whether processing involves cross-border transfers and where the database or digital object is located.⁷⁰⁷ The burdensomeness of such procedures is likely to significantly chill innovation and consumer access to useful digital technologies.

⁷⁰² Orbitax. (2024, February 29). Jordan Launches Registration Platform for Non-Resident Electronic Service Providers. <https://orbitax.com/news/country/article/Jordan-Launches-Registration-P-55066>.

⁷⁰³ Republic of Kazakhstan. (2013, May 21). *On Personal Data and Its Protection* (Law No. 94-V, Article 12(2), as amended in 2026). <https://old.adilet.zan.kz/rus/docs/Z1300000094>

⁷⁰⁴ Ministry of Defense and Aerospace Industry of the Republic of Kazakhstan. (2018, March 13). *On Approval of the Rules for Registration, Use and Allocation of Domain Names in the Kazakhstan Segment of the Internet* (Order No. 38/HK, as amended, paragraph 16(6)). <https://old.adilet.zan.kz/rus/docs/V1800016654>

⁷⁰⁵ Republic of Kazakhstan. (2004, July 5). *On Communications* (Law No. 567-II, as amended). <https://adilet.zan.kz/eng/docs/Z040000567>

⁷⁰⁶ Republic of Kazakhstan. (2026, June 24). *On Amendments and Additions to Certain Legislative Acts Concerning Digitalization, Personal Data Protection, Road Traffic and Regulation of Advanced Transport Technologies* (Law No. 326-VIII, introducing Article 7(3-1) of the Personal Data Law). <https://old.adilet.zan.kz/rus/docs/Z2600000326>

⁷⁰⁷ EY. (2026) Amendments to the Personal Data Law.

https://www.ey.com/en_kz/technical/tax-alerts/2026/09/kazakhstan-personal-data-law-amendments-deletion-anonymisation-data-breach-register .

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Kazakhstan adopted its Digital Code (No. 255-VIII) on January 9, 2026, with implementation beginning in July 2026.⁷⁰⁸ The Code establishes a broader framework for digital services, data, and automated decisions. Separately, the Law on Online Platforms and Online Advertising requires platforms exceeding 100,000 average daily users in Kazakhstan over a month to appoint a legal representative for interaction with the relevant authorities.⁷⁰⁹

Draft amendments published in December 2025 proposed restrictions on registration by users under 16, excluding instant-messaging services, and additional regulation of audiovisual platforms.⁷¹⁰ On August 26, 2026, President Tokayev stated that a bill restricting social-media registration by users under 16 had been submitted to Parliament in June and called for parliamentary consideration.⁷¹¹

Separately, legislation signed on December 30, 2025 expanded prohibited online content to include material deemed to promote “non-traditional sexual orientation.”⁷¹² This broadens content-removal exposure for platforms and creates additional risks of restricting lawful expression and access to information.

Since January 1, 2026, revised VAT rules for foreign companies selling goods or providing services to individuals in Kazakhstan through internet platforms apply a 16% VAT rate.⁷¹³ Article 89 of the Tax Code also permits blocking foreign suppliers’ internet resources for failure to comply with VAT-registration notices or notices addressing discrepancies identified through desk-based tax controls. This enforcement mechanism creates a risk of service interruption for affected foreign digital suppliers.

⁷⁰⁸ Republic of Kazakhstan. (2026, January 9). *Digital Code of the Republic of Kazakhstan* (No. 255-VIII, Article 106). <https://old.adilet.zan.kz/rus/docs/K2600000255>

⁷⁰⁹ Republic of Kazakhstan. (2023, July 10). *On Online Platforms and Online Advertising* (Law No. 18-VIII, Article 9(1), as amended). <https://old.adilet.zan.kz/rus/docs/Z2300000018>

⁷¹⁰ Ministry of Culture and Information of the Republic of Kazakhstan. (2025, December 4). *On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan Concerning Online Platforms and Mass Media* (draft law). <https://legalacts.egov.kz/npa/view?id=15715644>

⁷¹¹ Seilkhanov, A. (2026, August 26). *Tokayev to propose under-16 social media ban to newly-established parliament*. Qazinform. <https://qazinform.com/news/tokayev-to-propose-under-16-social-media-ban-to-newly-established-parliament-0311d1>

⁷¹² Republic of Kazakhstan. (2025, December 30). *On Amendments and Additions to Certain Legislative Acts Concerning Archival Affairs and Restrictions on the Dissemination of Unlawful Content* (Law No. 248-VIII, Article 1(12)). <https://old.adilet.zan.kz/rus/docs/Z2500000248>

⁷¹³ KPMG. (2025, November 10). *Kazakhstan: New VAT Rules for Foreign Internet Companies Effective January 1, 2026*. <https://kpmg.com/us/en/taxnewsflash/news/2025/11/kazakhstan-new-vat-rules-foreign-internet-companies-2026.html>

Challenges to the Development of AI

Kazakhstan’s Law on Artificial Intelligence (No. 230-VIII), signed on November 17, 2025, entered into force on January 18, 2026.⁷¹⁴ It classifies AI systems by risk and autonomy and requires risk management, proportionate documentation, user disclosures, and machine-readable labeling and perceptible warnings for defined synthetic outputs. High-risk systems must meet cybersecurity requirements similar to those applicable to government systems. Sectoral authorities maintain lists of trusted high-risk systems; applicants for inclusion must obtain an audit. The law also prohibits specified harmful uses, including harmful manipulation, unlawful personal-data processing, and emotion recognition without consent, subject to statutory exceptions. Users must have access to explanations of results affecting their rights and refuse AI interaction unless legally required. These requirements may increase compliance costs and complicate deployment by foreign AI providers.

Article 23 permits use of copyrighted works for AI-model training only where the author or rightsholder has not prohibited that use in a machine-readable manner, and does not even provide an exception for scientific or educational use. This framework is likely to increase rights-management costs and uncertainty undermine Kazakhstan's adoption of AI.

Kenya

Asymmetric Platform Regulation

Kenya’s Competition (Amendment) Bill, 2026 would introduce a “strategic market position” standard addressing digital markets and prohibit abuse of superior bargaining position without requiring proof of dominance or market power.⁷¹⁵ The latter standard would apply where a trading partner is deemed to lack a viable and satisfactory alternative. These provisions could expand intervention in commercial relationships even in competitive markets. USTR should encourage Kenya to implement safeguards against disproportionate restrictions on digital services, and avoid using these new powers to target U.S. firms in a discriminatory manner.

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,⁷¹⁶ The Cabinet Secretary is empowered to decide the types of personal data that must be stored and processed in Kenya based on the protection of strategic interests of

⁷¹⁴ Republic of Kazakhstan. (2025, November 17). *On Artificial Intelligence* (Law No. 230-VIII, Article 31). <https://old.adilet.zan.kz/rus/docs/Z2500000230>

⁷¹⁵ Oraro & Company Advocates. (n.d.). *The Competition (Amendment) Bill 2026*. <https://www.oraro.co.ke/the-competition-amendment-bill-2026/>

⁷¹⁶ Government of Kenya. (2019). *The Data Protection Act, 2019* (Act No. 24). <https://www.kentrade.go.ke/wp-content/uploads/2022/09/Data-Protection-Act-1.pdf>

the state or revenue. Regulation 26 of the Data Protection (General) Regulations, 2021 requires local processing or at least one serving copy in a Kenyan data center for specified processing involving civil registration and legal identity, elections, public finances, designated protected computer systems, early childhood and basic education, and primary or secondary healthcare.⁷¹⁷

The Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024 imposes localization and reporting requirements on designated critical information infrastructure.⁷¹⁸ Regulation 28 requires infrastructure holding critical information to be located in Kenya, subject to a procedure for obtaining approval to locate that information abroad. The regulations also establish cybersecurity operations centers and require monthly compliance briefs to the National Computer and Cybercrimes Coordination Committee. These obligations increase costs for affected cloud and infrastructure providers.

Kenya gazetted its Cloud Policy, 2025 on May 2, 2025.⁷¹⁹ Implementation guidelines dated June 2026 require public entities to use accredited cloud providers and migrate non-exempt systems and data within 24 months. Top-secret data must use a government-dedicated cloud in Kenya, while restricted data must use a government cloud service provider's public cloud infrastructure within Kenya. Establishing new public-sector data centers requires approval. These hosting and accreditation requirements restrict procurement options and can disadvantage cross-border cloud suppliers.

Kenya's revised 2026 telecommunications framework requires licensing for commercial co-location data centers, with a KES 15 million (about \$115,000) initial fee and annual fees of 0.4% of gross turnover or KES 800,000, whichever is higher.⁷²⁰ In September 2026, the Communications Authority proposed a separate data-center licence with a KES 100,000 initial fee and annual fees of 0.4% of gross turnover or KES 80,000, whichever is higher.⁷²¹ The proposal remains under consultation and targets implementation in FY2027/28. Such fees may discourage investment. USTR should encourage proportionate licensing requirements that take into account the benefits data centers provide.

⁷¹⁷ Government of Kenya. (2021, December 31). *The Data Protection (General) Regulations, 2021* (Legal Notice No. 263), regulation 26. <https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf>

⁷¹⁸ Government of Kenya. (2024, February 16). *The Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024* (Legal Notice No. 44), regulations 14 and 28. <https://new.kenyalaw.org/akn/ke/act/ln/2024/44/eng@2024-02-16/source>

⁷¹⁹ Government of Kenya. (2025, May 2). *The Kenya Cloud Policy, 2025* (Gazette Notice No. 5589). <https://new.kenyalaw.org/akn/ke/officialGazette/2025-05-02/83/eng@2025-05-02/source>

⁷²⁰ Communications Authority of Kenya. (2026). *Telecommunications Market Structure—2026*, category A.2. <https://www.ca.go.ke/sites/default/files/2026-06/Revised%20Telecommunications%20Market%20Structure-June%202026.pdf>

⁷²¹ Communications Authority of Kenya. (2026, September). *Proposed Licensing Framework for Data Centres: Consultation Version*, paragraph 16. <https://www.ca.go.ke/sites/default/files/2026-09/Public%20Consultation%20on%20Data%20Centres%20September%202026.pdf>

Government-Imposed Restrictions on Internet Content and Related Access Barriers

On June 25, 2024, internet connectivity fell by nearly 40% across at least 20 networks during anti-Finance Bill protests, despite the Communications Authority's prior assurance that it would not disrupt connectivity.⁷²² Digital-rights organizations reported indications of intentional disruption. Separately, civil-society organizations estimated that an internet shutdown could cost Kenya approximately US\$6.3 million per day.⁷²³ 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.⁷²⁴

The Computer Misuse and Cybercrimes (Amendment) Act, 2025 was signed on October 15, 2025 and expanded the National Computer and Cybercrimes Coordination Committee's authority to block websites and applications.⁷²⁵ On July 2, 2026, however, the High Court declared the website-blocking provision, section 6(1)(ja), and the challenged cyber-harassment provision, section 27(1)(b), unconstitutional.⁷²⁶ Separately, on March 6, 2026, the Court of Appeal declared sections 22 and 23 of the Computer Misuse and Cybercrimes Act unconstitutional because their false-publication offenses were overbroad and infringed freedom of expression.⁷²⁷ USTR should encourage implementation of the judgment and safeguards against arbitrary restrictions on access to online services.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

The Films and Stage Plays (Self-Classification) Regulations issued in November 2024 replaced the July 2024 self-classification rules and expressly cover video-on-demand and OTT services accessible in Kenya.⁷²⁸ Providers seeking self-classification must obtain an annual certificate, submit catalogues and removal procedures, and grant the Kenya Film Classification Board

⁷²² Access Now. (2024, June 25). *Authorities in Kenya must immediately restore internet access and #KeepItOn throughout protests and unrest*. <https://www.accessnow.org/press-release/kenya-protests-internet-shutdown/>

⁷²³ Wambui, M. (2024, June 29). *Internet shutdowns could cost Kenya \$6.3 million daily, stakeholders warn*. The Eastleigh Voice.

<https://eastleighvoice.co.ke/Internet%20Society%20kenya.kenya%20internet%20shutdown/54624/internet-shutdowns-could-cost-kenya-63-million-daily-stakeholders-warn>

⁷²⁴ 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>.

⁷²⁵ Government of Kenya. (2025, October 21). *The Computer Misuse and Cybercrimes (Amendment) Act, 2025* (Act No. 17), section 3. <https://new.kenyalaw.org/akn/ke/act/2025/17/eng@2025-10-21/source>

⁷²⁶ High Court of Kenya. (2026, July 2). *Law Society of Kenya & 8 others v Attorney General & 17 others* [2026] KEHC 9453 (KLR), paragraph 80.

<https://new.kenyalaw.org/akn/ke/judgment/kehc/2026/9453/eng@2026-07-02/source>

⁷²⁷ Court of Appeal of Kenya. (2026, March 6). *Bloggers Association of Kenya (BAKE) v Attorney General & 6 others* [2026] KECA 430 (KLR), paragraphs 141–143 and 153.

<https://new.kenyalaw.org/akn/ke/judgment/keca/2026/430/eng@2026-03-06/source>

⁷²⁸ Government of Kenya. (2024, November 14). *The Films and Stage Plays (Self-Classification) Regulations, 2024* (Legal Notice No. 185), regulations 4 and 20.

<https://new.kenyalaw.org/akn/ke/act/ln/2024/185/eng@2024-11-14/source>

access to their libraries for compliance monitoring. Applying these requirements alongside broadcasting rules risks duplicative and costly regulation.

The Communications Authority is considering registration and reporting requirements for nonresident OTT and streaming providers.⁷²⁹ The Authority published a study in July, proposing a light-touch Class Licensing framework for non-resident Over-The-Top (OTT) messaging providers, threatening to bring application-layer services into legacy telecom regulatory structures.⁷³⁰ USTR should encourage Kenya to avoid imposing legacy rules on OTT suppliers.

Restrictions on Cross-Border Data Flows

Kenya's Data Protection Act permits cross-border transfers subject to statutory safeguards. On September 8, 2026, the Office of the Data Protection Commissioner published its Guidance Notes for Cross-border Data Transfers.⁷³¹ The guidance recognizes multiple transfer mechanisms and includes standard contractual clauses. Its onward-transfer discussion requires specific prior written authorization for each recipient, location, data category and purpose, and prohibits onward transfers for the recipient's own analytics, profiling or product improvement. However, the accompanying standard clauses permit certain contractually authorized onward transfers and authorization of categories of sub-processors, subject to notice and an opportunity to object. Clarification of these differing provisions is needed to avoid uncertainty for routine cloud and subcontracting arrangements. USTR should encourage internationally interoperable safeguards and proportionate onward-transfer requirements.

Taxation of Digital Products and Services

Exported services are subject to a 16% VAT, except qualifying business process outsourcing exports, which were zero-rated.⁷³² Zero-rating of exported taxable services was restored in July 2023. Qualification requires use or consumption outside Kenya. The Finance Act, 2026 also

⁷²⁹ Communications Authority of Kenya. (2026, July 25). *Authority weighs light-touch rules as OTT platforms reshape Kenya's digital economy*.

<https://www.ca.go.ke/authority-weighs-light-touch-rules-ott-platforms-reshape-kenyas-digital-economy>

⁷³⁰ Communications Authority of Kenya. (2026, July 25). *Authority weighs light-touch rules as OTT platforms reshape Kenya's digital economy*.

<https://www.ca.go.ke/authority-weighs-light-touch-rules-ott-platforms-reshape-kenyas-digital-economy>.

⁷³¹ Government of Kenya. (2019). *The Data Protection Act, 2019* (Act No. 24), sections 48–49.

<https://www.kentrade.go.ke/wp-content/uploads/2022/09/Data-Protection-Act-1.pdf>; Office of the Data Protection Commissioner. (2026, September 8). *Guidance Notes for Cross-border Data Transfers*.

<https://www.odpc.go.ke/wp-content/uploads/2026/09/ODPC-%E2%80%93-Guidance-Notes-for-Cross-border-Data-Transfers.pdf>

⁷³² PwC. (2023, January 27). *Kenya: VAT in Africa*.

<https://www.pwc.co.za/en/publications/vat-in-africa/kenya-overview.html>; Government of Kenya. (2025, July 1). *Value Added Tax Act, 2013* (Act No. 35), Second Schedule, Part A, paragraph 23, as amended by the Finance Act, 2023, section 38(a)(ii). <https://new.kenyalaw.org/akn/ke/act/2013/35/eng@2025-07-01/source>

classifies interchange fees and merchant service fees from card-payment transactions as management or professional fees for withholding-tax purposes.⁷³³

Kenya replaced its 1.5% DST with a Significant Economic Presence Tax (SEPT) in December 2024.⁷³⁴ SEPT is effectively 3% of gross turnover: a 30% tax on deemed profits equal to 10% of turnover. Effective July 1, 2025, the Finance Act, 2025 expanded coverage to services supplied over the internet or electronic networks and removed the KES 5 million turnover exemption.⁷³⁵ Separately, the expanded royalty definition covers proprietary and off-the-shelf software payments, including licensing, development, training, maintenance and support fees. Covered digital-marketplace payments are subject to a withholding tax of 20% of payment to non-residents, and 5% to residents. Although Kenya's SEPT tax is inconsistent with international tax principles and could be constrained by tax treaty provisions, the absence of such a treaty with the United States makes that avenue unavailable. Given the likely result of imposing double taxation on U.S. suppliers, CCIA urges USTR to advocate for its removal.

Challenges to the Development of AI

The Draft Copyright and Related Rights Bill 2026 restricts Text and Data Analysis exceptions strictly to non-commercial research, prohibiting commercial AI model training on Kenyan-hosted content without explicit paid licensing.⁷³⁶ CCIA urges USTR to request that Kenya expand TDM exceptions to cover commercial AI model development.

Korea

In the November 2025 U.S.-Korea Joint Fact Sheet, Korea committed to “ensure that U.S. companies are not discriminated against and do not face unnecessary barriers” under laws and policies concerning digital services, including online platform regulation. CCIA urges USTR to hold Korea to this commitment and exercise continued vigilance as Korea considers numerous measures targeting U.S. firms, as detailed below.

Asymmetric Platform Regulation

Notwithstanding the November 2025 commitments, the Korean Fair Trade Commission (KFTC) Chairman has pledged to renew the push for online platform regulation, and to expand the KFTC

⁷³³ Kenya Revenue Authority. (n.d.). *Finance Act 2026: What It Means for You*.

<https://www.kra.go.ke/finance-act-2026-what-it-means-for-you>

⁷³⁴ KPMG. (2025, September 29). *Kenya: Public consultation on application of significant economic presence (SEP) tax*. <https://kpmg.com/us/en/taxnewsflash/news/2025/09/kenya-public-consultation-application-sep-tax.html>

⁷³⁵ PwC. (2026, July 17). *Kenya—Corporate—Significant developments*.

<https://taxsummaries.pwc.com/kenya/corporate/significant-developments>

⁷³⁶ Kenya Copyright Board. (2026, March). Draft Bill: The Copyright and Related Rights Bill, 2026, § 34.

<https://copyright.go.ke/sites/default/files/downloads/INVITATION%20FOR%20PUBLIC%20COMMENTS%20ON%20PROPOSED%20COPYRIGHT%20BILL.pdf>

with a new, dedicated “Key Investigation Planning Unit”⁷³⁷ to target the online platform sector—both likely to disproportionately target U.S. headquartered firms, and risking increasing trade tensions with the United States.

On December 9, 2025, Representative Lee Jeong-mun of the ruling Democratic Party introduced Bill No. 2215044, the Bill on the Fairness of Online Platform Intermediary Transactions. The bill would apply to online platform intermediary services with at least ₩10 billion (approximately US\$7 million) in annual domestic intermediary-service revenue or ₩100 billion (approximately US\$70 million) in annual transactions with domestic consumers, subject to additional criteria established by Presidential Decree. Covered platforms would face prescriptive requirements governing written contracts, commission rates, advance notice of contract modifications or service restrictions, payment deadlines, advertising and promotion arrangements, recordkeeping, and grievance handling. Platforms that receive or manage merchant proceeds would also be required to separately protect at least 50 percent of those funds through segregated accounts or payment-guarantee insurance. The proposal remains pending before the National Assembly’s Political Affairs Committee but in August 2026 the Chairman of the KFTC reiterated his priority in getting this legislation passed.⁷³⁸

The proposed Online Platform Fairness Bill raises serious concerns for U.S. providers. Although framed as a fairness and transparency measure, it would establish a platform-specific regulatory regime imposing obligations that go substantially beyond those applicable to competing brick-and-mortar retailers where Korean firms dominate. Among other provisions, the bill would prescribe payment and fund-management requirements for non-financial platforms, create statutory protections for merchant associations, and prohibit broadly defined forms of “unfair” conduct including discriminatory treatment, certain forms of self-preferencing, restrictions on multi-homing, and other practices that may be legitimate or pro-competitive. The bill would also significantly expand KFTC enforcement authority, including administrative surcharges of up to 10 percent of relevant sales, daily penalties, civil liability including treble damages for retaliation, and potential criminal penalties. These asymmetric obligations risk increasing compliance costs and legal uncertainty for cross-border business models and raise national treatment concerns under KORUS, as well as questions regarding Korea’s November 2025 commitment to ensure that U.S. digital services suppliers do not face discrimination or unnecessary barriers. The United States should urge Korea to reconsider this approach and ensure that any platform regulation is non-discriminatory, proportionate, and grounded in demonstrable evidence of consumer harm.

⁷³⁷ Rocketpunch. (2026). *Launch of the Fair Trade Commission’s Key Investigation Planning Team*. <https://www.rocketpunch.com/en/discover/64816>

⁷³⁸ Joong An Ilbo (26 August 2026). <https://n.news.naver.com/article/025/0003543740?sid=101>.

The KFTC and National Assembly are likewise accelerating the Food Delivery Platform Act.⁷³⁹ This legislation would impose government-mandated price controls and fee caps on marketplace transactions, undermining free-market competition and the ability to engage in market-based contracts. Like other efforts by Korea to regulate platforms, it relies on ex-ante thresholds engineered to capture foreign market leaders, while explicitly shielding domestic competitors. By pairing fee caps with fines up to 10 percent of revenue, explicit threats of criminal prosecution, and broadening the KFTC's powers, it would establish a negative precedent for government price-setting across foreign-led digital sectors.

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 requiring exclusive use of the store's in-app billing system. Further, policymakers supportive of the bill have made clear their intent to single out specific U.S. companies with the new law.⁷⁴⁰ 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, 2022.⁷⁴¹ 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)."⁷⁴² In October 2023, the KCC proposed fines totaling ₩68 billion (approximately US\$52 million) against Google and Apple. On August 12, 2026, the Korea Media and Communications Commission

⁷³⁹ Chosun Biz. (2026). *Lawmakers urge cap on app delivery fees.*

<https://biz.chosun.com/en/en-policy/2025/10/10/QK5LE5EIX5HFEDJTDA4BDUFPGZA/>

⁷⁴⁰ *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.

⁷⁴¹ *Enforcement Decree* [Korea]. (2022).

<https://www.kcc.go.kr/user.do?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=4&boardSeq=52916>.

⁷⁴² 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>.

(KMCC) resumed consideration of the cases; its secretariat concluded that the challenged payment practices violated the Telecommunications Business Act, but the Commission deferred final corrective measures and sanction levels. The enforcement proceedings therefore remain pending.

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.

In May 2026, Representative Lee Jeong-heon introduced Bill No. 2219036, an amendment to the Telecommunications Business Act that would require mobile operating system providers to provide technical access necessary for interoperability with device hardware and software functions and would prohibit unjustified refusal or restriction of such access.⁷⁴³ The bill was introduced on May 21 and taken up by the Science, ICT, Broadcasting and Communications Committee on September 8, 2026; it remains pending. Because the proposal leaves important implementation details to subordinate regulation, its technical, security, privacy, and commercial effects will depend in part on future rules. This proposal essentially replicates an analogous provision of Europe's DMA (Articles 6 and 7), a highly intrusive and controversial form of market intervention whose negative effects on innovation, protection of intellectual property, and degradation of privacy and security have been widely documented.⁷⁴⁴

All measures identified above create asymmetric obligations that would increase compliance costs and legal uncertainty for cross-border business models and raise national treatment concerns under KORUS, as well as questions regarding Korea's November 2025 commitment to ensure that U.S. digital services suppliers do not face discrimination or unnecessary barriers. The United States should urge Korea to reconsider this approach and ensure that any platform regulation is non-discriminatory, proportionate, and grounded in evidence of consumer harm.

Customs-related Restrictions and Import Barriers for Goods

Korea has introduced the Electronic Commerce Customs Clearance System for Shipment (ECCS), requiring foreign e-commerce operators to register to use simplified customs clearance procedures. Registered operators may also be expected to provide transaction-level data in connection with certain customs facilitation benefits, although the scope and practical implications of these requirements remain unclear. These obligations could impose additional technical, reporting and compliance burdens on U.S. online marketplaces facilitating cross-border trade. Korea should provide clear implementation guidance and ensure that

⁷⁴³ 국민참여입법센터 [Public Participation in Legislation Center]. (2026, May 21). 전기통신사업법 일부개정법률안 (의안번호 2219036, 이정현의원 등 10인) [Partial Amendment Bill to the Telecommunications Business Act (Bill No. 2219036, Rep. Lee Jeong-heon and 9 others)]. <https://opinion.lawmaking.go.kr/gcom/nsmLmSts/out/2219036/detailRP>.

⁷⁴⁴ Wagener, supra note 13.

registration and data-reporting requirements are transparent, proportionate and do not unnecessarily restrict legitimate low-value trade.

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.⁷⁴⁵ 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 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 originally accomplished this by instituting the 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. CSAP historically limited global CSP access to Korea's public-sector cloud market. In April 2026, MSIT and the National Intelligence Service announced that the existing dual CSAP/NIS review process will be consolidated into a single NIS-led verification system.⁷⁴⁶ Existing CSAP certificates will remain valid, with full implementation planned for the second half of 2027 following a one-year grace period. Whether the revised system will permit U.S. firms any additional access remains uncertain: to date, Korea's decade-long restrictions in this sector have deprived U.S. firms of access to billions of dollars of contracts, as Korea has steadily moved government workloads onto the cloud.

Current restrictions affecting more sensitive public-sector workloads, that NIS's revisions may or may not address include current 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;

⁷⁴⁵ TELECOMMUNICATIONS BUSINESS ACT [Korea] Act No. 19856. (2023).

https://elaw.klri.re.kr/eng_service/lawView.do?hseq=64463&lang=ENG.

⁷⁴⁶ Seoul Economic Daily. (2026, April 20). Korea to Unify Public Cloud Security Verification Under NIS Next Year. <https://en.sedaily.com/technology/2026/04/20/korea-to-unify-publ-cloud-security-verification-under-nis>.

- 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.

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.⁷⁴⁷ Detailed steps Korea will need to take to ensure effective market access are described in a recent CCIA briefer.⁷⁴⁸

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 technology.⁷⁴⁹ 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.

⁷⁴⁷ 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>.

⁷⁴⁸ 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>.

⁷⁴⁹ *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.

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. Separately, CCIA has raised concerns regarding supplier-eligibility restrictions in certain 2025 government GPU and high-performance computing support programs that limited opportunities for foreign CSPs.

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.⁷⁵⁰ The fund is designed to support broadcasting communications, which, under the foundational law,⁷⁵¹ 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)⁷⁵²—such as content and programming—equally to Korean digital products, and in the WTO (Telecommunications Services Reference Paper)⁷⁵³ 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. As of September 2026, the bill remains pending in the National Assembly’s Science, ICT, Broadcasting and Communications Committee and has not been enacted.

Government Imposed Content Restrictions and Related Access Barriers

Since 2023, Korea's Network Act has required content delivery network (CDN) providers to block access to content designated as illegal by the Korea Media and Communications Commission (KMCC), without a court order. No other jurisdiction imposes such an obligation on CDNs at comparable scale. Elsewhere, including under the U.S. Digital Millennium Copyright Act, removal requests go to hosting providers, which can actually remove content.

⁷⁵⁰ 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.

⁷⁵¹ *Framework Act on Broadcasting Communications Development* [Korea]. (2015). https://elaw.klri.re.kr/eng_service/lawView.do?hseq=37358&lang=ENG.

⁷⁵² 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>.

⁷⁵³ 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.

The KMCC applies a blocklist originally built for Korean ISPs. CDNs must block listed sites even where ISPs have already blocked them, re-check every listed site every 24 hours, and adapt to frequent changes in submission formats. Other Korean agencies now expect providers to build separate blocking mechanisms for their own requests rather than use the existing KMCC process. A bill to amend the Game Industry Promotion Act (Bill No. 2219989), introduced on July 16, 2026, would expressly extend orders to block illegal games to CDN providers. The bill was referred to the National Assembly's Culture, Sports and Tourism Committee on September 16, 2026 and remains pending.

These burdens fall almost entirely on U.S. providers. Overseas services make up very little of Korean CDN providers' business, so few listed sites are on their networks. U.S. CDN providers serve millions of websites worldwide, so they are effectively required to redesign global infrastructure for a single market. The added processing also slows performance and weakens defenses against DDoS attacks.

CCIA encourages the U.S. government to raise these concerns with Korea and support a more targeted approach: address content first at the hosting and ISP levels, apply CDN obligations only where necessary and technically feasible, and consolidate agency requests into a single, predictable process.

Korea has enacted further amendments to the Network Act imposing new obligations relating to “false or manipulated information.” The amendments, enacted in late 2025, promulgated in January 2026, and effective July 7, 2026, create a new regulatory regime governing both publishers and large-scale online platforms.⁷⁵⁴ Among other provisions, the law defines new categories of “false information,” “manipulated information,” and “false or manipulated information”; establishes punitive damages of up to five times proven losses in certain cases; and imposes new compliance obligations on large online service providers, including requirements to establish policies for addressing covered information, process user reports, and publish transparency reports. The implementing rules define covered large-scale providers to include certain services with at least one million average daily users. These requirements create significant compliance and liability risks for U.S. digital services suppliers and incentivize precautionary restrictions on lawful content where providers may have limited ability to independently determine the legality or accuracy of user-generated information.

Following entry into force, Korean authorities designated nine platforms as subject to the new large-platform obligations: Naver, Kakao, AXG, Nate, DCInside, Google, Meta, X, and TikTok. Covered providers must maintain systems for responding to reports of false or manipulated information and publish transparency reports. KMCC has stated that covered platforms

⁷⁵⁴ 법무법인(유한) 태평양 [Bae, Kim & Lee LLC]. (2026). 정보통신망법 시행령(허위조작정보근절법) 일부개정: 주요 내용과 시사점 [Partial Amendment to the Enforcement Decree of the Network Act (Act on Eradication of False and Manipulated Information): Key Contents and Implications]. <https://www.bkl.co.kr/law/insight/newsletter/6642>.

themselves determine whether reported content constitutes false or manipulated information under their self-regulatory policies and decide whether deletion or blocking is warranted. Separately, an administrative surcharge of up to ₩1 billion may apply to certain professional publishers that repeatedly disseminate information after it has already been finally determined by a court to be unlawful or false or manipulated, subject to additional statutory criteria. CCIA continues to urge narrow, transparent, and non-discriminatory implementation, preservation of intermediary protections, and protection of commercially sensitive information.

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.⁷⁵⁵ 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.

A further proposal introduced on October 10, 2025 by Representative Kim Jang-gyeom, Bill No. 2213496, would require certain value-added telecommunications providers to enter into contracts governing network use, including network-use conditions and compensation, and would prohibit unjustified discriminatory terms or restrictions on either contracting party’s rights or interests.⁷⁵⁶ The bill was taken up by the National Assembly’s Science, ICT, Broadcasting and Communications Committee on November 17, 2025 and remains pending.

Such proposals can be traced to years of conflict between U.S. content providers operating in the region and local telecommunication providers,⁷⁵⁷ culminating in legislation introduced in 2022

⁷⁵⁵ 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>.

⁷⁵⁶ 김현아 [Kim, H.]. (2025, October 12). 김장겸 "망 이용계약 안 맺으면 과태료"...'망 무임승차 방지법' 발의 [Kim Jang-gyeom: "Fines If No Network Use Contract Is Concluded" – "Network Free-Riding Prevention Act" Introduced]. 이데일리 [Edaily]. <https://edaily.co.kr/News/Read?mediaCodeNo=257&newsId=01489126642332264>.

⁷⁵⁷ 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-free-from-isps/>.

by Rep. Young-chan Yoon, called the “Netflix Free Ride Prevention Act.”⁷⁵⁸ 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;⁷⁵⁹ CCIA has raised concerns that such requirements could be inconsistent with Korea’s trade obligations⁷⁶⁰

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. 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 mandates interconnection fees between the three main South Korean ISPs,⁷⁶¹ based on a regulated rate, which effectively led them to abandon the global norm of settlement-free peering and incentivise collusion to keep rates high. The high fees demanded by large South Korean ISPs affect the ability of U.S. content providers to serve traffic efficiently in the market, resulting in at least one U.S. firm exiting the market.⁷⁶² CCIA research has found that Korean ISP peering demands can be an order of magnitude more expensive than Internet transit in major global markets.⁷⁶³ Further evidence of the negative effect of regulated rates in Korea is demonstrated by the negligible price declines in Korea compared to other major regional hubs: since 2023, declines in internet transit prices in Korea were one-quarter those of other major Asian hubs (4% vs 15%); and in terms of absolute levels, the key benchmark rate for 100GigE IP transit in Korea in 2026 was double that of competitive regional peers (Taiwan, Japan, Hong Kong and Singapore), at \$.82 /Mbs/month, versus rates of \$.30-.40/Mbs/month in those other markets.⁷⁶⁴

⁷⁵⁸ Young-chan, Y. (2022, September 8). *Representative Yoon Young-chan, Lead Proposer of “Netflix Free Riding Prevention Act.”* Naver. <https://blog.naver.com/yc8361/222870020115>.

⁷⁵⁹ 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/>.

⁷⁶⁰ 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/>.

⁷⁶¹ 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/>.

⁷⁶² Twitch Blog. (2023). *Update on Twitch in Korea.* <https://blog.twitch.tv/en/2023/12/05/an-update-on-twitch-in-korea/>

⁷⁶³ Computer & Communications Industry Association. (2022, September). *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>

⁷⁶⁴ Telegeography. (2026). *Transit Pricing Trends.* <https://resources.telegeography.com/ip-transit-pricing-trends-asia>.

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”⁷⁶⁵ In the November 2025 U.S.-Korea Joint Fact Sheet, the United States and Korea specifically committed to ensure that U.S. companies are not discriminated against or subjected to unnecessary barriers in laws and policies concerning digital services, expressly including network usage fees.⁷⁶⁶ CCIA appreciates the engagement of USTR and the Department of Commerce on this issue in the past and encourages continued vigilance, and support for eliminating regulated ISP-ISP rates.

Challenges to the Development of AI

South Korea’s AI Basic Act, promulgated on January 21, 2025, took effect on January 22, 2026 together with its Enforcement Decree.⁷⁶⁷ Additional amendments promulgated on January 20, 2026 took effect in stages, with certain provisions effective January 22 and the remaining provisions taking effect July 21, 2026. The framework imposes transparency obligations for high-impact and generative AI, safety obligations for AI systems that exceed 10²⁶ FLOPs of training compute and also satisfy additional technology and fundamental-rights-risk criteria, and specific obligations for high-impact AI used in designated sectors. High-impact status is therefore based on sector and risk rather than compute alone. Certain foreign providers are also subject to domestic-representative requirements. MSIT has provided a grace period of at least one year during which fact-finding investigations and penalties are generally deferred, except in exceptional cases involving serious harm. CCIA continues to raise concerns regarding compliance uncertainty and the cross-border effects of the framework on U.S. 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,

⁷⁶⁵ 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.

⁷⁶⁶ Office of the United States Trade Representative. (2025, November). Fact Sheet: The United States and Korea Agree to the Korea Strategic Trade and Investment Deal. <https://ustr.gov/about/policy-offices/press-office/fact-sheets/2025/november/fact-sheet-united-states-and-korea-agree-korea-strategic-trade-and-investment-deal>.

⁷⁶⁷ 국가법령정보센터 [Korea Law Information Center]. 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법 (법률 제20676호) [Framework Act on the Development of Artificial Intelligence and Establishment of a Foundation of Trust (Act No. 20676)]. <https://www.law.go.kr/lsInfoP.do?lsiSeq=268543>.

which “effectively privilege Korean over foreign suppliers in any data-intensive sector without materially contributing to privacy protection,” as USTR has highlighted.⁷⁶⁸

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).⁷⁶⁹ At the time, these were the largest fines 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.

Amendments to PIPA that took effect in stages beginning in 2023 expanded data-subject rights and PIPC’s enforcement authority, including the introduction of data-portability rights in 2025. PIPA authorizes penalties of up to 3% of total revenue, with revenue unrelated to the violation excluded from the penalty calculation.⁷⁷⁰ Effective September 11, 2026, specified repeated or particularly serious violations may trigger penalties of up to 10% of total revenue, including certain intentional or grossly negligent violations affecting at least 10 million data subjects. PIPA also authorizes PIPC to order the suspension of cross-border transfers where statutory transfer requirements have been violated or where the recipient or destination does not provide adequate protection and harm has occurred or there is a significant risk of harm. CCIA remains concerned that these authorities may create disproportionate exposure for foreign firms and affect legitimate cross-border data transfers.

Korea has historically restricted the export of high-precision map data, disadvantaging foreign providers that rely on overseas data processing to offer location-based services in Korea. This

⁷⁶⁸ 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>.

⁷⁶⁹ 대한민국 정책브리핑 [Korea Policy Briefing]. (2022, September 14). 개인정보 불법 수집...구글·메타 과징금 1천억 원 [Illegal Collection of Personal Information: Google and Meta Fined 100 Billion Won]. <https://www.korea.kr/news/policyNewsView.do?newsId=148905887>.

⁷⁷⁰ 국가법령정보센터 [Korea Law Information Center]. (2023, March 14). 개인정보 보호법 (법률 제19234호) [Personal Information Protection Act (Act No. 19234)]. <https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=248613>.

longstanding market access barrier has limited the ability of U.S. mapping services to offer functionality comparable to Korean competitors.⁷⁷¹ In February 2026, however, the Korean government took an important first step toward liberalizing this market by conditionally approving the export of high-precision map data for Google, marking the first such approval for a foreign supplier, with additional approvals for U.S. service suppliers expected to follow.⁷⁷²

The February 2026 approval remains subject to Korea-specific conditions that are applied extraterritorially, impacting both domestic and global users. Google must comply with security requirements relating to sensitive facilities and coordinates, specifically height coordinates and elevation, utilize a local partner to ensure data is locally processed and reviewed by the government before export, and maintain procedures for responding to Korean government security requests. Accordingly, while the decision represents significant progress after more than a decade of market access restrictions, implementation will determine whether U.S. suppliers can offer mapping and location-based services in Korea on commercially viable and non-discriminatory terms comparable to those available to Korean competitors. Google and Korean authorities continue to work through implementation and verification of the conditions attached to the approval and commercial services have yet to be made available.

USTR should continue to monitor implementation of the February 2026 decision and press Korea to ensure that approval conditions are applied proportionately, and without discrimination. Korea should also provide an expeditious and predictable pathway for other qualified U.S. suppliers seeking equivalent access, consistent with Korea's obligations under KORUS and its November 2025 commitments regarding non-discriminatory treatment of U.S. digital services suppliers.

Taxation of Digital Products and Services

On June 26, 2026, Representative Lee Kang-il and nine co-sponsors from Korea's ruling Democratic Party introduced Bill No. 2219551, which would amend the Act on International Tax Adjustment to impose a new Digital Services Tax (DST) on foreign digital service providers. The bill would impose a 2% tax on gross revenues earned from Korean users by foreign corporations providing digital services, including "online platforms" and "online advertising," above a revenue threshold to be established by Presidential Decree.⁷⁷³ The proposal also introduces related-party disclosure requirements and new rules treating certain above-market

⁷⁷¹ Information Technology and Innovation Foundation. (2025, June 27). South Korea's Export Restrictions on High-Precision Geospatial Data.

<https://itif.org/publications/2025/06/27/south-koreas-export-restrictions-on-high-precision-geospatial-data>

⁷⁷² 대한민국 정책브리핑 [Korea Policy Briefing]. (2026, February 27). 구글社 1:5000 지도 반출 허가 결정 [Decision to permit Google's export of 1:5,000 map data].

<https://www.korea.kr/news/policyNewsView.do?newsId=148960107>.

⁷⁷³ 양대근 [Yang, D.]. (2026, June 29). 與이강일 "글로벌 빅테크의 '꼼수 자금유출' 막을 것" [Ruling party's Lee Kang-il: "We will block global Big Tech's covert outflow of funds"]. 헤럴드경제 [Herald Business].

<https://biz.heraldcorp.com/article/10791723>.

payments to foreign affiliates as disguised profits. The legislation would take effect six months after promulgation. The bill was referred to the National Assembly's Finance and Economy Planning Committee on July 1, 2026 and remains pending.

The proposal is facially discriminatory because the DST would apply only to foreign corporations, while Korean suppliers providing identical digital services would not be subject to the tax. CCIA estimates that the proposal could result in more than \$500 million in annual DST liability for U.S. companies.

USTR should urge Korea to abandon Bill No. 2219551 rather than attempt to address its discriminatory effects through modifications to thresholds, scope, or rate, and should make clear that discriminatory digital taxation of U.S. suppliers is inconsistent with Korea's commitments to non-discriminatory treatment under KORUS and the broader U.S.–Korea economic relationship.

Other Barriers to Digital Trade

Discriminatory Enforcement Practices by the KFTC

Korea's longstanding use of aggressive regulatory enforcement tactics has created a challenging and unpredictable operating environment for digital service providers, and these practices often appear to disproportionately target U.S. firms.⁷⁷⁴ 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 prosecution⁷⁷⁵ for practices that are not treated as criminal offenses in other jurisdictions. The KFTC's expansion of specialized investigative bodies to disproportionately pursue U.S. firms jeopardizes the mutual commitments to fair, non-discriminatory enforcement and risks undermining the broader bilateral trade relationship

This asymmetry is reflected in enforcement outcomes: among the top ten largest fines ever imposed by the KFTC in abuse-of-dominance cases, seven targeted U.S. companies accounted for 95.5 percent of the total fine amounts in this dataset, compared to just 4.5 percent for domestic firms. This excessive and unpredictable application of regulatory powers creates significant legal uncertainty,⁷⁷⁶ deters investment, and raises the cost of doing business in Korea's digital economy. Although KORUS provides due process protections for U.S. firms (*e.g.*, Articles 16.1 and 16.5), Korea's adherence to these standards has been spotty and engendered at

⁷⁷⁴ Corey, N. & Holleyman, R. (2025, June 12). *Safeguarding U.S. Companies from Unfair South Korean Competition Policies*. NBER.

<https://www.nber.org/publication/safeguarding-u-s-companies-from-unfair-south-korean-competition-policies/>.

⁷⁷⁵ 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>.

⁷⁷⁶ 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>.

least one case of pushback from the United States.⁷⁷⁷ Recent CCIA analysis of 1,203 KFTC decisions over the past decade determined that penalties were imposed on U.S. companies at 4 to 6 times the rate imposed on Korean companies, and 80-90 times the rate imposed on Chinese companies.⁷⁷⁸ These discriminatory practices have broader implications for cross-border digital trade, calling into question the ability of U.S. firms to compete in the Korean market on a level playing field. USTR should investigate these practices as a possible breach of national treatment obligations covering both investment (Article 11.3) and cross-border services (Article 12.2).

E-Commerce Local Presence Requirements

On January 20, 2026, Korea promulgated amendments to the E-Commerce Act establishing a domestic-representative requirement under Article 20-5, effective January 21, 2027.⁷⁷⁹ The changes require foreign e-commerce operators to designate a domestic representative if they meet any one of three thresholds: KRW 1 trillion (~\$750M) annual revenue, 1 million+ average monthly Korean users, or KFTC designation for potential consumer harm. Because only one threshold must be met, a U.S. company with minimal Korea revenue could be caught on global revenue alone. Covered firms must designate a representative in Korea who is tasked with substantive obligations. CCIA is concerned that requiring a domestic representative to perform substantive consumer-protection functions (which may be centralized in other jurisdictions) may create local-presence burdens for cross-border digital suppliers and should be implemented consistently with Korea's KORUS commitments.⁷⁸⁰

Malaysia

Barriers to the Deployment and Operation of Network Infrastructure

Malaysia maintains an exemption to the Merchant Shipping Ordinance 1952 that permits non-Malaysian ships to conduct submarine cable repairs in Malaysian waters. The exemption is key in reducing the time required to conduct submarine cable 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,

⁷⁷⁷ Palmer, D. (2019, July 7). *USTR says Korea competition-related concerns are still not resolved*. POLITICO. <https://subscriber.politicopro.com/article/2019/07/ustr-says-korea-competition-related-concerns-still-not-resolved-1574166>.

⁷⁷⁸ CCIA. (2026). *The KFTC's Uneven Hand*. <https://ccianet.org/research/reports/the-kftcs-uneven-hand/#main-content> and <https://ccianet.org/articles/the-kftcs-defense-leaves-the-evidence-unanswered/>

⁷⁷⁹ 국가법령정보센터 [Korea Law Information Center]. (2026, January 20). 전자상거래 등에서의 소비자보호에 관한 법률 (법률 제21312호) [Act on Consumer Protection in Electronic Commerce, etc. (Act No. 21312)]. <https://www.law.go.kr/lsInfoP.do?lsId=009318&ancYnChk=0>.

⁷⁸⁰ CCIA. 2024. *Amendments to the Electronic Commerce Act*. <https://ccianet.org/library/comments-on-koreas-proposed-amendments-to-the-electronic-commerce-act/>

carrying around 99% of the world's internet, voice and data traffic, including the backhaul of mobile network traffic and data for digital trade.⁷⁸¹

With the exemption cancelled between 2019 and 2024, it remains vulnerable to future administrative reversal.⁷⁸² The United States and Malaysia subsequently addressed this issue in the U.S.-Malaysia Agreement on Reciprocal Trade, signed in October 2025.⁷⁸³ Article 2.19 of the Agreement provides that Malaysia shall ensure that its exemption to the Merchant Shipping Ordinance 1952 is permanent, allowing non-Malaysian vessels to conduct submarine cable repairs in Malaysian waters. However, the Agreement has not yet entered into force. USTR should continue to press Malaysia to implement this commitment by making the cabotage exemption permanent through domestic law or another durable legal mechanism, thereby providing the long-term regulatory certainty necessary to support investment in submarine cable infrastructure.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The State of Selangor has adopted a Local Economy Development (LED) policy imposing a 30% local content requirement on new data-center investments in the state, a major hub for U.S. cloud service providers.⁷⁸⁴ The requirement applies to key data-center inputs, including servers, memory, storage, networking equipment, and other advanced systems, and conditions investment approval on companies committing to achieve the local-content threshold. Selangor officials have characterized the requirement as mandatory for data centers entering the state. Such local-sourcing requirements can distort procurement decisions, increase costs, and disadvantage U.S. suppliers of advanced data-center equipment. USTR should evaluate whether this approach is consistent with Article 3.2 (Facilitation of Digital Trade) of the U.S.-Malaysia Agreement on Reciprocal Trade, press for withdrawal or revision of the requirement and urge Malaysia's federal government and other states to avoid adopting similar local-content mandates.

⁷⁸¹ Kohlstedt, K. (2017, June 30). *Inside the Cables Carrying 99% of Transoceanic Data Traffic. 99% Invisible.* <https://99percentinvisible.org/article/underwater-cable-inside-cables-carrying-99-international-data-traffic/>

⁷⁸² Wong, A. (2024, June 2). *Malaysia Finally Reinstates Cabotage Exemption for Undersea Cable Repair Ships.* *SoyaCincau.* <https://soyacincau.com/2024/06/02/malaysia-reinstates-undersea-cable-repair-vessel-cabotage-exemption/>

⁷⁸³ 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-reciprocal-trade/>

⁷⁸⁴ Dewan Negeri Selangor. (2025, November 24). *Penyata Rasmi: Mesyuarat Ketiga (Bajet), Penggal Ketiga, Dewan Negeri Selangor Kelima Belas.* <https://dewan.selangor.gov.my/wp-content/uploads/2025/11/DRAF-PENYATA-RASMI-24.11.2025-ISNIN.pdf>

In October 2025, Malaysia's National AI Office (NAIO) unveiled its Sovereign AI Strategy,⁷⁸⁵ 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.⁷⁸⁶ 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.

Since the strategy was announced, Malaysia has moved further toward implementation of its national AI agenda. Budget 2026 included RM2 billion for a Sovereign AI Cloud,⁷⁸⁷ while the government launched the Malaysia Digital Action Plan 2030 in June 2026⁷⁸⁸ and began stakeholder engagement in July 2026 on a proposed AI Governance Bill.⁷⁸⁹ In 2026, the Malaysian Communications and Multimedia Commission (MCMC) issued a tender for the National Sovereign AI Cloud (NSAIC), part of Malaysia's AI Nation 2030 agenda.⁷⁹⁰ The tender excludes suppliers subject to the U.S. CLOUD Act, which in practice disqualifies U.S. cloud service providers—because of their nationality and not their security capabilities. The technical specifications also favor a single vendor's proprietary technology instead of open, outcome-based standards. Malaysia should remove nationality-based exclusions, use technology-neutral specifications and give U.S. suppliers a fair chance to compete in public sector AI and cloud procurements. USTR should

⁷⁸⁵ 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>

⁷⁸⁶ 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>

⁷⁸⁷ 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>

⁷⁸⁸ Malaysia Ministry of Digital. (2026, June 29). *Ministry of Digital Leads Nation's AI Transformation*.

<https://www.digital.gov.my/en-GB/siaran/Kementerian-Digital-Terajui-Transformasi-AI-Negara>

⁷⁸⁹ Malaysia Ministry of Digital. (2026, July 10). *Ministry of Digital Initiates Engagement on Proposed Artificial Intelligence (AI) Governance Bill*.

<https://www.digital.gov.my/en-GB/siaran/Kementerian-Digital-Mulakan-Libat-Urus-Cadangan-Rang-Undang-Undang-Tadbir-Urus-Kecerdasan-Buatan-%28AI%29>

⁷⁹⁰ Cloud Computing News. 2026. *Malaysia develops sovereign AI cloud*.

<https://www.cloudcomputing-news.net/news/malaysia-sovereign-ai-cloud/>

evaluate whether this approach is consistent with Article 3.2 (Facilitation of Digital Trade) of the U.S.-Malaysia Agreement on Reciprocal 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.⁷⁹¹ 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.”⁷⁹² In June 2026, Communications Minister Fahmi Fadzil again raised concerns that social media platforms do not provide local media with “fair compensation” for news content and encouraged the Malaysia Media Council to engage platforms on the issue, with the government prepared to facilitate those discussions.⁷⁹³ On September 9, 2026, the Malaysia Media Council initiated a six-month technical process to develop a proposal for a Collective Management Organisation (CMO) for news publishers, intended to explore mechanisms for protecting the value of original journalism, strengthening copyright management, and supporting the sustainability of the news industry.⁷⁹⁴ USTR should continue monitoring this process and urge Malaysia to pursue voluntary, market-based arrangements rather than mandatory transfers or bargaining obligations targeted at large digital platforms.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Malaysia has significantly expanded its regulation of online platforms through the social media licensing regime under the Communications and Multimedia Act 1998⁷⁹⁵ and the Online Safety Act 2025 (ONSA),⁷⁹⁶ which entered into force on January 1, 2026. During 2026, the Malaysian

⁷⁹¹ Malaysian Communications and Multimedia Commission. (2023, September 5). *MCMC Considers Regulatory Framework to Address Online Harm and Imbalance Media AdEx*. https://www.mcmc.gov.my/skmmgovmy/media/General/PressRelease/MS_MCMC-CONSIDERS-REGULATORY-FRAMEWORK-TO-ADDRESS-ONLINE-HARM-AND-IMBALANCE-MEDIA-ADEX.pdf

⁷⁹² *Ibid.*

⁷⁹³ Zulkaflee, I. (2026, June 20). *Fahmi Vows Fair Pay for Malaysian Media Content on Social Platforms*. *The Rakyat Post*. <https://www.therakyatpost.com/news/2026/06/20/fahmi-vows-fair-pay-for-malaysian-media-content-on-social-platforms>

⁷⁹⁴ Majlis Media Malaysia. (2026, September 9). *Majlis Media Malaysia Gerakkan Usaha Memperkukuh Perlindungan Hak Cipta dan Kelestarian Kewartawanan*. <https://majlismedia.my/news/majlis-media-malaysia-gerakkan-usaha-memperkukuh-perlindungan-hak-cipta-dan-kelestarian-kewartawanan>

⁷⁹⁵ Malaysia. (1998). *Communications and Multimedia Act 1998 [Act 588]*. Malaysian Communications and Multimedia Commission. <https://www.mcmc.gov.my/en/legal/acts>

⁷⁹⁶ Malaysia. (2025). *Online Safety Act 2025 [Act 866]*. Malaysian Communications and Multimedia Commission. <https://www.mcmc.gov.my/en/legal/acts>

Communications and Multimedia Commission (MCMC) brought into force additional subsidiary regulations and codes, including the Child Protection Code⁷⁹⁷ and Risk Mitigation Code⁷⁹⁸ on June 1 and regulations governing Online Safety Plans and the compounding of offenses on July 1.⁷⁹⁹ These measures place increasingly prescriptive obligations on covered platforms to assess systemic risks, proactively detect and address harmful content, and demonstrate compliance to MCMC. While aimed at legitimate online-safety objectives, overly broad or disproportionate obligations can increase compliance costs, encourage over-removal of lawful content, and create substantial regulatory uncertainty for U.S. digital service suppliers. USTR should urge Malaysia to ensure that implementation is transparent, proportionate, risk-based, and developed through meaningful consultation with affected stakeholders.

Malaysia imposed new age-verification obligations under the Child Protection Code, which took effect on June 1, 2026.⁸⁰⁰ Licensed social media service providers must verify age against government-issued or government-recognized records and ensure that only users aged 16 or above are permitted to register new accounts and access age-appropriate features. For existing users, however, MCMC provided for progressive implementation of age verification over a transition period of up to six months. Existing users identified as under 16 are to receive one month to download or transfer their data before restrictions, suspension, or other action is taken. Following further engagement with industry in October 2026, MCMC indicated that it was reconsidering exclusive reliance on government-identification checks and intended to permit a multi-layered verification approach. Formal confirmation and the detailed requirements governing that approach remained pending at the time of writing.

USTR should continue monitoring this issue and encourage Malaysia to preserve this flexibility and permit privacy-protective, service-appropriate methods rather than mandating a single identification-based mechanism. To the extent that new requirements emerge, USTR should

Seek to ensure that implementation is technically feasible, proportionate to the stated safety objective, protective of user privacy and security, and does not impose discriminatory or unnecessarily burdensome obligations on foreign digital service suppliers.

Malaysia's Communications and Multimedia Act creates significant liability exposure through Sections 211 and 233, which regulate prohibited online content and improper use of network and

⁷⁹⁷ Malaysian Communications and Multimedia Commission. (2026, May 22). *Child Protection Code*. <https://mcmc.bernama.com/news.php?id=2572374>

⁷⁹⁸ Malaysian Communications and Multimedia Commission. (2026, May 22). *Risk Mitigation Code*. <https://mcmc.bernama.com/news.php?id=2572374>

⁷⁹⁹ Malaysia. (2026, June 26). *Online Safety (Online Safety Plan) Regulations 2026, P.U. (A) 244*. <https://mylaw.my/legislation/peraturan-peraturan-keselamatan-dalam-talian-pelan-keselamatan-dalam-talian-2026>

⁸⁰⁰ Malaysian Communications and Multimedia Commission. (2026, May 22). *Child Protection Code*. <https://mcmc.bernama.com/news.php?id=2572374>

applications services. Amendments that took effect on February 11, 2025⁸⁰¹ changed Section 233 by replacing “offensive” with the higher threshold of “grossly offensive,” while also extending the provision to communications transmitted with the intent to commit an offence involving fraud or dishonesty and substantially increasing applicable penalties. In February 2026, Malaysia’s Federal Court upheld the constitutionality of the terms “offensive” and “annoy” in the pre-amendment version of Section 233;⁸⁰² the Court also found that the prosecution at issue should not have been brought. USTR should encourage Malaysia to ensure that intermediary and content-liability rules contain sufficiently clear standards and proportionate penalties so that digital services are not incentivized to over-remove lawful user content.

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).⁸⁰³ 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 licensing framework, however, cloud service providers remain exposed to obligations developed principally for telecommunications services, including requirements concerning government data-access and disclosure requests, interception authorities, and technical standards imposed by MCMC. These requirements can create substantial compliance and security risks when applied to global cloud and data-hosting services that do not perform the same functions as traditional telecommunications carriers. USTR should monitor implementation of that commitment while continuing to press Malaysia to exempt cloud and data-hosting providers from inappropriate telecommunications-style regulation.

In 2024, MCMC established a licensing framework for Internet messaging and social media service providers with at least eight million users in Malaysia; the licensing requirement took effect on January 1, 2025.⁸⁰⁴ Since January 1, 2026, qualifying Internet messaging and social media service providers have been automatically deemed registered as Applications Service Provider Class [ASP(C)] licensees under Section 46A of the Communications and Multimedia Act. This “deeming” mechanism eliminates the need for covered providers to affirmatively apply

⁸⁰¹ Malaysia. (2025). *Communications and Multimedia (Amendment) Act 2025 [Act A1743]*. Malaysian Communications and Multimedia Commission. <https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/A1743-BI-COMMUNICATIONS-AND-MULTIMEDIA-AMENDMENT-ACT-2025-1.pdf>

⁸⁰² Federal Court of Malaysia. (2026, February 6). *The Government of Malaysia v. Heidy Quah Gaik Li* [Civil Appeal No. 01(f)-44-11-2025(B), [2026] 3 MLRA 350]. https://www.elaw.my/JE/01/JE_2026_9.html

⁸⁰³ Malaysian Communications and Multimedia Commission. (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>

⁸⁰⁴ Malaysian Communications and Multimedia Commission. (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

for a license but subjects them by operation of law to the regulatory framework applicable to licensed providers. The Online Safety Act 2025 separately imposes online-safety duties on covered licensed services, although the Act expressly excludes a “private messaging feature” from its application.⁸⁰⁵ Accordingly, Internet messaging services may be deemed licensed under the CMA even where particular private-messaging features fall outside ONSA’s substantive scope.

Separately, in August 2025, Malaysia announced that it would eliminate the requirement that U.S. social media platforms and cloud service providers contribute 6% of Malaysian revenue to the Universal Service Provision Fund (USPF),⁸⁰⁶ a commitment subsequently incorporated into the U.S.-Malaysia Agreement on Reciprocal Trade. However, the Agreement has not yet entered into force, so USTR should continue to monitor implementation of Malaysia’s commitment to eliminate the USPF contribution while pressing Malaysia to ensure that its remaining licensing, data-access, content-moderation, and online-safety requirements are transparent, proportionate, technology-neutral, and non-discriminatory.

In September 2026, MCMC opened a consultation on proposed amendments to the Communications and Multimedia (Licensing) Regulations 2000, including a higher class licence registration fee for Applications Service Providers than for other licence categories, a new regulatory fee applicable only to class licensees operating from outside Malaysia, and changes to licensing timelines and obligations for deemed licensees.⁸⁰⁷ The proposal does not appear to establish a clear methodology, objective parameters, or a ceiling for the fee. Without those safeguards, an ostensibly administrative charge could evolve into an open-ended or revenue-linked levy that disproportionately burdens large foreign digital service suppliers and recreates, through the licensing framework, discriminatory effects similar to a digital services tax. USTR should monitor the consultation closely and encourage Malaysia to ensure that any fee is fixed, cost-based, transparent, and applied on a non-discriminatory basis.

Challenges to the Development of AI

Malaysia is developing a statutory framework for artificial intelligence. In July 2026, the Ministry of Digital, through the National AI Office, opened a public consultation on a proposed AI Governance Bill that would establish central institutional oversight, principle-based governance requirements, and a risk-based regulatory framework for AI developers and

⁸⁰⁵ Malaysia. (2025). *Online Safety Act 2025 [Act 866]*, § 2.

<https://mylaw.my/legislation/online-safety-act-2025/section-2>

⁸⁰⁶ Parliament of Malaysia, Dewan Rakyat. (2025, August 4). *Official Report of the Dewan Rakyat, Second Meeting, Fourth Term, Fifteenth Parliament*. <https://www.parlimen.gov.my/files/hindex/pdf/DR-04082025.pdf>

⁸⁰⁷ Ministry of Communications & Malaysian Communications and Multimedia Commission. (2026, September 21). Public Consultation on Proposed Enhancements to the Communications and Multimedia (Licensing) Regulations 2000. Unified Public Consultation Portal, Malaysia Productivity Corporation. <https://upc.mpc.gov.my/view-consultation/295>.

deployers.⁸⁰⁸ At the same time, as noted above, Malaysia continues to pursue a broader “AI sovereignty” agenda, including the development of sovereign AI cloud and compute capabilities and promotion of domestic AI models. While efforts to strengthen domestic AI capacity are legitimate, policies that require the use of local models, infrastructure, data, or technology could restrict market access for U.S. AI and cloud providers and fragment the cross-border AI ecosystem. USTR should urge Malaysia to ensure that the AI Governance Bill and related sovereign-AI initiatives remain risk-based, technology-neutral, internationally interoperable, and non-discriminatory, and do not impose unnecessary data localization, local technology preferences, or other requirements that disadvantage U.S. providers. The Malaysian Government has stated that the Bill would be tabled in Parliament in the first quarter of 2027.

Threats to the Security of Devices and Services

The 2025 Communications and Multimedia (Amendment) Act amendments,⁸⁰⁹ 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 (e.g., for data stored in the United States and subject to the Electronic Communications Privacy Act (ECPA)). 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 request that Malaysia use the U.S.-Malaysia Mutual Legal Assistance Treaty, or negotiate a bilateral Cloud Act agreement as the preferred legal mechanisms for requesting data from U.S.-based service providers. The United States should 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.

Other Digital Trade Barriers

Malaysia requires a certificate of approval from the Standards and Industrial Research Institute of Malaysia (SIRIM) to import communications equipment. However, SIRIM does not test or

⁸⁰⁸ Malaysia Productivity Corporation. (2026, July 10). *Public Consultation Feedback: Proposed Artificial Intelligence (AI) Governance Bill*. <https://upc.mpc.gov.my/view-consultation/264>.

⁸⁰⁹ Malaysia. (2025). *Communications and Multimedia (Amendment) Act 2025 [Act A1743]*. Malaysian Communications and Multimedia Commission. <https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/A1743-BI-COMMUNICATIONS-AND-MULTIMEDIA-AMENDMENT-ACT-2025-1.pdf>

certify refurbished products, effectively barring their import. This limits the ability of cross-border marketplaces to support customers seeking refurbished or graded electronics, particularly once a product is no longer in production and replacement components are unavailable as new. USTR should advocate for regulatory flexibility to address this issue.

Malta

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Malta Gaming Authority (MGA) requires remote computer game operators hosting data abroad to maintain a live replica of regulatory data in Malta, including player details, financial transactions and gameplay transactions.⁸¹⁰ The MGA's published guidance describes local replication as a means of ensuring real-time regulatory access, subject to assessment of the operator's setup. It permits hosting in Malta, other EEA states, and third-country jurisdictions accepted following case-by-case assessment.⁸¹¹ Companies are obligated to disclose detailed documentation regarding server locations, data replication processes, and data transmission processes.

Malta's Cloud Services Policy (GMICT P 0124),⁸¹² effective from September 2024, gives primary preference to cloud services supplied by the government through its designated agent. A system owner selecting another service must justify that choice in writing, and contracting authorities may mandate use of the government service in tenders. Given the unlikelihood that a government-supplied cloud service will offer the most capable functionality, such preferences are likely to undermine Malta's digitization of its government services.

Mexico

Customs-Related Restrictions and Import Barriers for Goods

U.S. exporters continue to report customs-related challenges at the U.S.-Mexico border that can increase clearance times and costs. These include heightened inspections, overlapping information requests, insufficient advance notice of procedural changes, and coordination problems between Mexico's Customs Agency and Tax Administration Service. Mexico has taken some positive steps in 2026, including an upgrade to its single-window system and the

⁸¹⁰ Paris, K. (2026, June 20). *iGaming Replication Server in Malta: Meeting the MGA Requirement*. Sirap. <https://www.sirap.com/igaming-replication-server-malta-mga/>

⁸¹¹ Malta Gaming Authority. (2015, December). *Technical Infrastructure hosting Gaming and Control Systems – Remote Gaming*. <https://www.mga.org.mt/app/uploads/Technical-Infrastructure-hosting-Gaming-and-Control-Systems-Remote-Gaming.pdf>

⁸¹² GMICT. 2024. *Cloud Services Policy*. https://mita.gov.mt/wp-content/uploads/2025/10/GMICT_P_0124_Cloud.pdf

operationalization of its customs broker agency program at all Mexican ports.⁸¹³ The United States should continue engaging Mexico to fully implement its commitments under the USMCA Customs Administration and Trade Facilitation Chapter, including provisions related to expedited release, transparency in customs procedures, use of information technology, and a functional single window.

Mexico enacted a broad Customs Law reform in late 2025, with implementing rules taking effect on January 1, 2026.⁸¹⁴ The new framework imposes stricter liability on customs brokers, requires substantially more information for individual import transactions, increases potential penalties, and expands the Customs Agency's authority to detain and seize shipments. U.S. stakeholders have also raised concerns that Mexico has not fully implemented the periodic payment option for express delivery shipments required by the USMCA and that updated rules eliminate simplified procedures for shipments valued above US\$2,500, requiring those shipments to use a specialized customs broker. These requirements can increase compliance costs and delays for U.S. exporters, particularly small and medium-sized businesses. USTR should continue pressing Mexico for transparent implementation and full compliance with its USMCA customs and express-delivery commitments.

Mexico continues to provide insufficient prior notification of procedural changes in customs requirements. Regulatory amendments to trade rules are frequently introduced without opportunities for public comment, undermining transparency and predictability for U.S. exporters. Recent amendments to the General Rules on Foreign Trade (Reglas Generales de Comercio Exterior) and the General Rules and Criteria on Foreign Trade (Criterios de Carácter General en Materia de Comercio Exterior) were published with immediate application, without allowing for a comment period, disrupting trade operations for U.S. exporters. Each year, a new version of the General Rules on Foreign Trade is issued in the last days of December to enter into force on January 1 of the following year, leaving businesses with virtually no time to adapt to new requirements. The newly established Council responsible for examining and processing courier licensing applications has increased delays for new approvals. The process remains slow and unpredictable, creating additional disruptions to operations. Furthermore, certain goods are still not permitted to be imported through all ports of entry. Restricting goods to designated ports has made it difficult for U.S. exporters to arrange efficient transportation and increases logistics costs.

⁸¹³ Office of the United States Trade Representative. (2026, July 17). *United States and Mexico to Convene in Mexico City for Third Bilateral Negotiating Round Related to the Joint Review of the USMCA*. <https://www.ustr.gov/about/policy-offices/press-office/press-releases/2026/july/united-states-and-mexico-convene-mexico-city-third-bilateral-negotiating-round-related-joint-review>

⁸¹⁴ Diario Oficial de la Federación. (2025, November 19). *Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Aduanera*. https://www.dof.gob.mx/nota_detalle.php?codigo=5773357&fecha=19/11/2025

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.⁸¹⁵ 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 requires 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. 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. CCIA urges USTR to continue to press Mexico to remove these requirements, as they serve as a *de facto* requirement for U.S. companies 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

On October 7, 2026 Mexico’s Chamber of Deputies approved amendments to the Federal Copyright Law that would introduce a secondary liability regime for ISPs by conditioning existing liability protections on ISPs maintaining a public repeat-infringer termination policy. It would impose secondary liability where an ISP fails to comply with that requirement and either knowingly contributes to infringement or has the ability to control infringing conduct and derives a direct financial benefit from it, with administrative fines of up to US\$258,000 for certain violations. While the proponents assert that the bill is not intended to create automatic or strict liability or a generalized monitoring obligation, the “ability to control” and “financial benefit” standards could create uncertainty for ISPs and affect the predictability of the safe-harbor framework if interpreted broadly, and civil society groups have separately raised concerns about incentives for over-removal of lawful content.⁸¹⁶

⁸¹⁵ Baker McKenzie. (n.d.). *Cloud Compliance Center: Mexico*.

<https://resourcehub.bakermckenzie.com/en/resources/cloud-compliance-center/na/mexico>

⁸¹⁶ EU SE. 2026. *Copyright Reform Raises Concerns about Freedom of Expression Online*

<https://eusee.hivos.org/alert/copyright-reform-raises-concerns-about-potential-effects-on-freedom-of-expression-online/>

A separate and potentially far-reaching intermediary liability risk is pending before Mexico's Supreme Court in *Ulrich Richter Morales and Claudia Ramírez Tavera v. Google Inc. and Google México*.⁸¹⁷ A lower court imposed damages of more than 5 billion pesos (*i.e.*, almost \$300 million) against Google based on allegedly defamatory third-party content published through its service Blogger. If upheld, the judgment could establish a precedent under which internet intermediaries may be held broadly liable for content created by third parties, incentivizing increased monitoring and over-removal of lawful expression and imposing substantial compliance burdens on U.S. digital services. Such an outcome could also be inconsistent with Mexico's obligations under USMCA Article 19.17 on Interactive Computer Services.⁸¹⁸ USTR and the Department of State should continue to underscore the trade and free-expression implications of such a precedent.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

Mexico is considering modifications to NOM-184-SCFI-2018, a mandatory standard historically applicable to telecommunications service providers, that would expand its application to digital platforms. This could subject digital service providers to requirements originally designed for public telecommunications services— even though Mexico's 2026 National Quality Infrastructure Program describes the NOM's scope as limited to telecommunications providers and contracts. Industry stakeholders question whether a technical standard can impose telecommunications-specific obligations on digital platforms absent express authority in the underlying law, raising due process concerns under Mexican law as well as consistency with USMCA Article 18.14 (disciplines on applying public telecommunications requirements to value-added service suppliers). The process has also raised transparency concerns, as stakeholders learned of the proposed expansion months after the working group was established and were given limited time to comment, prompting industry requests for additional consultation.

Challenges to the Development of AI

In May 2026, Mexico enacted amendments to the Federal Labor Law and Federal Copyright Law extending protections for performers' image, voice, and characters to uses involving artificial intelligence and creating exclusive rights against certain AI-based impersonation,

⁸¹⁷ Suprema Corte de Justicia de la Nación. (2023). *Amparo Directo 8/2023*. <https://www.scjn.gob.mx/>; Computer & Communications Industry Association. (2026, January 28). *Letter to State and USTR on Mexico Intermediary Liability*. <https://ccianet.org/wp-content/uploads/2026/02/Letter-to-State-and-USTR-on-Mexico-Intermediary-Liability.pdf>

⁸¹⁸ Office of the United States Trade Representative. (2020). *United States-Mexico-Canada Agreement, Chapter 19: Digital Trade, Article 19.17 (Interactive Computer Services)*. <https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf>

including “clones” of performances and identifiable simulations of performers’ voices.⁸¹⁹ The amendments raise significant uncertainty for U.S. AI developers, streaming services, and other digital service suppliers because key concepts remain undefined and the law could potentially be interpreted to reach AI training conducted outside Mexico, outputs that merely resemble a performer, functional uses such as translation or subtitling, and uses involving characters whose underlying rights are held by separate rightsholders. The framework also creates uncertainty regarding remuneration obligations and the circumstances under which previously granted consent may be revoked.

Mexico should use implementing regulations to clarify that liability requires identifiable and intentional impersonation or cloning of a specific performer; exclude stylistic similarity and functional uses such as translation and subtitling; clarify that training conducted outside Mexico does not trigger liability absent a clear nexus to infringing outputs directed at the Mexican market; clearly allocate rights and remuneration where performers and underlying character rightsholders differ; and establish defined, prospective standards governing revocation of consent. These safeguards are necessary to prevent unnecessary barriers to cross-border AI and digital services and potential inconsistencies with Mexico’s USMCA digital trade commitments.

⁸¹⁹ Diario Oficial de la Federación. (2026, May 14). *Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal del Trabajo y de la Ley Federal del Derecho de Autor, en materia de derechos de las personas trabajadoras artistas intérpretes o ejecutantes*. <https://sidof.segob.gob.mx/notas/5787418>; Computer & Communications Industry Association. (2026, June). *Key Areas to be Clarified in Implementing Mexico’s New AI Dubbing Law*. <https://ccianet.org/wp-content/uploads/securepdfs/2026/06/Key-Areas-to-be-Clarified-in-Implementing-Mexicos-New-AI-Dubbing-Law.pdf>.

Restrictions on Cross Border Data Flows

Mexico's existing regulatory framework for payment processing continues to limit the ability of U.S. electronic payment service providers to offer their complete suite of value-added services on a cross-border basis, including fraud prevention services, and to process domestic transactions using their own proprietary networks and technical standards. Mexico's former competition authority, COFECE, identified barriers to competition in the card payment processing market in 2023 and issued recommendations to the Central Bank of Mexico and the National Banking and Securities Commission, but those recommendations have not been implemented.⁸²⁰ In late 2025, Mexican regulators proposed new rules governing card payment networks and clearinghouses, but the proposals did not resolve the barriers identified by COFECE.⁸²¹ The National Banking and Securities Commission withdrew its card-network proposal in February 2026 for further analysis, while the clearinghouse proposal remained under consideration.⁸²² USTR should continue pressing Mexico to implement its USMCA commitments and ensure that U.S. electronic payment service suppliers can compete on a level playing field.

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.⁸²³ The measure was approved by Congress in October 2020 and published in the Diario Oficial on December 8, 2020.⁸²⁴ 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.

⁸²⁰ Comisión Federal de Competencia Económica. (2023, September 14). *Cofece identificó barreras a la competencia en el mercado de procesamiento de pagos con tarjeta*. <https://www.cofece.mx/cofece-identifico-barreras-a-la-competencia-en-el-mercado-de-procesamiento-de-pagos-con-tarjeta/>

⁸²¹ Banco de México, Comisión Nacional Bancaria y de Valores, & Secretaría de Hacienda y Crédito Público. (2025, October 27). *Se somete a consulta pública el proyecto de las nuevas Disposiciones de carácter general aplicables a las redes de medios de disposición*. <https://www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7B976B09C2-7D30-6F00-F99F-23F67278FA68%7D.pdf>

⁸²² Comisión Nacional Bancaria y de Valores. (2026, August 27). *Consulta pública del proyecto de Disposiciones de Carácter General Aplicables a Redes de Medios de Disposición*. <https://www.gob.mx/cnbv/prensa/consulta-publica-del-proyecto-de-disposiciones-de-caracter-general-aplicables-a-redes-de-medios-de-disposicion>

⁸²³ Cámara de Diputados. (2020, September 8). *Iniciativa del Ejecutivo Federal que reforma, adiciona y deroga diversas disposiciones de la Ley del Impuesto sobre la Renta, de la Ley del Impuesto al Valor Agregado y del Código Fiscal de la Federación*. <https://gaceta.diputados.gob.mx/PDF/64/2020/sep/20200908-D.pdf>

⁸²⁴ Código Fiscal de la Federación [Mexico]. (2020, December 8). https://www.diputados.gob.mx/LeyesBiblio/ref/cff/CFF_ref57_08dic20.pdf

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.⁸²⁵ 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 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.⁸²⁶ 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 November 2025, Mexico enacted Article 30-B of the Federal Fiscal Code, requiring covered digital service providers to provide the Tax Administration Service (SAT) with permanent online and real-time access to information necessary to verify compliance with Mexican tax obligations.⁸²⁷ The requirement took effect in 2026, and implementing rules require covered fiscal information to be made available electronically for access by the tax authority.⁸²⁸ Failure to comply may result in the temporary blocking of the digital service under Mexico's Value-Added Tax Law. Although Mexican authorities have stated that the requirement is limited to fiscal information, the continuous-access obligation creates significant operational, cybersecurity, and compliance concerns for digital service suppliers, while the availability of service blocking as an enforcement mechanism raises additional proportionality and market-access concerns. USTR should press Mexico to remove or substantially narrow this requirement and ensure that blocking access to the Mexican market is not used as a disproportionate tax-enforcement remedy.

⁸²⁵ U.S. Chamber of Commerce. (2023, August 17). *Comments Regarding North American Competitiveness Committee Recommendations*. https://downloads.regulations.gov/USTR-2023-0005-0013/attachment_1.pdf

⁸²⁶ Servicio de Administración Tributaria. (2024, October 3). *SAT simplifica trámites y brinda facilidades a los contribuyentes*.

<https://www.gob.mx/sat/prensa/sat-simplifica-tramites-y-brinda-facilidades-a-los-contribuyentes-055-2024>

⁸²⁷ Diario Oficial de la Federación. (2025, November 7). *Decreto por el que se reforman, adicionan y derogan diversas disposiciones del Código Fiscal de la Federación*. <https://sidof.segob.gob.mx/notas/docFuente/5772358>

⁸²⁸ Servicio de Administración Tributaria. (2025, December 28). *Resolución Miscelánea Fiscal para 2026*, Rule 2.9.21, "Acceso en línea a la información fiscal de plataformas digitales para comprobar el cumplimiento de obligaciones fiscales." https://dof.gob.mx/2025/SHCP/SHCP_281225_01.pdf

Mexico's 2026 Economic Package raised the income tax (ISR) and value-added tax (IVA) rates that digital marketplaces must withhold from the proceeds of sellers operating on their marketplaces, with the higher rates taking effect in January 2026. Digital marketplaces are required to act as withholding agents, deducting these amounts from each sale and remitting them to the Tax Administration Service (SAT) on the seller's behalf. Because the withholding applies to gross transaction value rather than to a seller's actual margin, the elevated rates fall disproportionately on small and medium-sized enterprises, whose thin margins mean the withheld amount can approach or exceed their real profit on a sale. This is driving sellers to abandon the formal digital marketplaces and shift toward informal channels where no withholding applies, so the marketplaces are losing sellers from their catalogs and seeing transaction volume erode as a direct result of the measure. The impact falls squarely on the U.S. digital marketplaces that must administer the elevated withholding while watching their seller base contract, undermining the very formalization objectives that Mexico's own policy agenda promotes. Mexico should recalibrate the withholding rates so that they approximate sellers' actual tax liability rather than a share of gross revenue, and should avoid rate levels that push sellers out of the formal economy and off the marketplaces that serve Mexican consumers.

Mexico's Income Tax Law imposes a withholding tax on legal entities that sell goods or provide services through digital platforms, with the applicable rate set according to the type of good or service and remitted by the platform on the seller's behalf. Despite requests from online marketplaces to reduce the applicable withholding rate, and industry evidence pointing to a decline in sellers and transactions following implementation of the current regime, Mexico's proposed 2027 Revenue Law maintains the 2.5% income tax withholding rate applicable to legal entities selling goods or providing services through digital platforms. Industry stakeholders have raised concerns that maintaining the current rate could continue to affect participation by sellers, particularly SMEs, and transaction volumes in Mexico's digital marketplace ecosystem.

Other Barriers to Digital Trade

Mexican energy policy continues to restrict the ability of private companies, including U.S. technology companies seeking reliable and clean electricity for data centers and other operations, to secure competitive energy supply. Constitutional and statutory reforms adopted in 2024 and 2025 strengthened the preferential position of the state-owned Federal Electricity Commission (CFE). The March 2025 energy reform package guarantees CFE's prevalence in the electricity sector, including by providing that CFE maintain at least 54 percent of the average electricity dispatched to the grid and requiring CFE ownership of at least 54 percent in "mixed investment" electricity generation projects.⁸²⁹ Private companies

⁸²⁹ Diario Oficial de la Federación. (2025, March 18). *Decreto por el que se expiden la Ley de la Empresa Pública del Estado, Comisión Federal de Electricidad; la Ley de la Empresa Pública del Estado, Petróleos Mexicanos; la Ley del Sector Eléctrico; la Ley del Sector Hidrocarburos; la Ley de Planeación y Transición Energética; la Ley de Biocombustibles; la Ley de Geotermia y la Ley de la Comisión Nacional de Energía; y se reforman diversas disposiciones legales.* https://www.dof.gob.mx/nota_detalle.php?codigo=5752329&fecha=18/03/2025

also continue to face delays, unexplained or unjustified denials, and other obstacles involving permits, grid access, and energy infrastructure.⁸³⁰ In 2025, Mexico replaced its independent energy regulator with the National Energy Commission (CNE), which operates under the supervision of the Secretariat of Energy, further centralizing regulatory authority.⁸³¹ These measures can restrict U.S. companies' ability to obtain sufficient, competitively priced, and clean electricity and undermine investment in energy-intensive digital infrastructure. The United States requested consultations with Mexico under the USMCA in 2022 regarding measures favoring CFE and PEMEX; the dispute has not proceeded to a panel, and USTR continues to identify Mexico's preferential energy policies as a significant investment barrier.⁸³²

Mexico completed a major restructuring of its competition and telecommunications regulatory institutions in 2025 following the December 2024 constitutional reform eliminating several autonomous regulatory bodies. The Federal Economic Competition Commission (COFECE) and Federal Telecommunications Institute (IFT) have been dissolved. Competition enforcement is now principally vested in the Comisión Nacional Antimonopolio (CNA), a decentralized public body associated with the Secretariat of Economy, while telecommunications regulation is carried out by the Comisión Reguladora de Telecomunicaciones (CRT), an administrative body within the executive branch's Agencia de Transformación Digital y Telecomunicaciones (ATDT).⁸³³

The division of the former IFT's responsibilities between the CNA and CRT creates a new institutional framework for telecommunications oversight. The CNA exercises competition-related authorities, including determining the existence of preponderant economic agents in the telecommunications and broadcasting sectors and imposing certain competition remedies, while the CRT exercises sector-specific regulatory functions and implements and supervises applicable telecommunications requirements. The two bodies are required to coordinate on matters where their authorities intersect.

The restructuring raises concerns regarding regulatory independence, predictability, and potential political influence because functions previously exercised by constitutionally autonomous

⁸³⁰ Bloomberg Línea. (2025, April 11). *México atenderá trámites del sector energético a partir del 21 de abril tras pausa por extinción de reguladores*. <https://www.bloomberglinea.com/latinoamerica/mexico/mexico-atendera-tramites-del-sector-energetico-a-partir-del-21-de-abril-tras-pausa-por-extincion-de-reguladores/>

⁸³¹ Secretaría de Energía. (2025, May 21). *Entra en funciones la nueva Comisión Nacional de Energía, ente regulador que contará con un Comité Técnico para la toma de decisiones*. <https://www.gob.mx/sener/es/articulos/entra-en-funciones-la-nueva-comision-nacional-de-energia-ente-regulador-qu-e-contara-con-un-comite-tecnico-para-la-toma-de-decisiones>

⁸³² Office of the United States Trade Representative. (2022, July 20). *United States Requests Consultations Under the USMCA Over Mexico's Energy Policies*. <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/july/united-states-requests-consultations-under-usmca-over-mexicos-energy-policies>

⁸³³ Diario Oficial de la Federación. (2025, July 16). *Decreto por el que se expide la Ley en Materia de Telecomunicaciones y Radiodifusión y se abroga la Ley Federal de Telecomunicaciones y Radiodifusión*. https://dof.gob.mx/nota_detalle.php?codigo=5763167&fecha=16/07/2025

regulators are now performed by entities situated within or more closely connected to the executive branch. USTR should monitor implementation of the new framework to ensure that competition and telecommunications decisions remain impartial, transparent, and nondiscriminatory and that U.S. companies are not disadvantaged relative to Mexican state-owned or domestic enterprises.

In October 2025, the United States and Mexico expanded the scope of their Mutual Recognition Agreement for Conformity Assessment of Telecommunications Equipment to cover Mexico's Specific Absorption Rate requirements and two additional regulations.⁸³⁴ Mexico also made further changes in 2026 to simplify testing requirements for U.S. telecommunications equipment exports.⁸³⁵ CCIA welcomes both these steps as a positive development.

In 2026, Mexico's Federal Consumer Protection Agency (PROFECO) and the Secretariat of Economy initiated a process to extend NOM-184-SCFI-2018 to over-the-top (OTT) streaming platforms. NOM-184 is a consumer-protection technical standard whose scope is limited to telecommunications services provided over a public telecommunications network. It imposes carrier-oriented obligations such as registration of adhesion contracts and tariffs before the regulator, dedicated telephone customer service, itemized consumption-based billing, terminal-equipment warranties, and minimum service-interruption compensation. Streaming platforms fall outside that scope because they do not operate a public telecommunications network or provide a telecommunications service; they deliver content over the open internet, so neither the underlying law nor the norm that implements it should reach them and nor are the prescribed obligations relevant to their service. PROFECO nonetheless seeks to bring OTTs in by treating streaming as a form of restricted television and audio, a telecommunications category defined in the Federal Telecommunications and Broadcasting Law (LMTR), and applying NOM-184's obligations on that basis. This stretches a definition written for licensed pay-TV and audio services to reach internet content providers that are regulated differently, giving the extension a weak legal foundation, and because that definition covers both audio and video, it would pull music and audio services into scope even though the stated target is video-on-demand. The result is a non-tariff barrier that disproportionately burdens U.S. providers by subjecting them to a regime designed for network carriers. Mexico should confirm that NOM-184 does not apply to OTT streaming services, and if PROTECT persists, USTR should evaluate this proposal in light of USMCA's Article 18.14 (Conditions for the Supply of Value-added Services) that was designed to prevent the extension of legacy rules on internet-enabled services.

⁸³⁴ Secretaría de Economía. (2025, October 28). *Acuerdo por el que se modifica el diverso de reconocimiento mutuo entre el Gobierno de los Estados Unidos Mexicanos y el Gobierno de los Estados Unidos de América para la evaluación de la conformidad de equipos de telecomunicaciones*. <https://sidof.segob.gob.mx/notas/5771085>

⁸³⁵ Office of the United States Trade Representative. (2026, July 17). *United States and Mexico to Convene in Mexico City for Third Bilateral Negotiating Round Related to the Joint Review of the USMCA*. <https://www.ustr.gov/about/policy-offices/press-office/press-releases/2026/july/united-states-and-mexico-convene-mexico-city-third-bilateral-negotiating-round-related-joint-review>

Mexico's Ministry of Culture, in collaboration with Collective Management Organizations, has been developing a mechanism to implement a compensatory remuneration scheme for private copying applicable to electronic devices, potentially including smartphones, tablets, laptops, and computers. Under this scheme, manufacturers and importers would be responsible for payment upon the introduction or first commercialization of covered devices in the Mexican market, with the proposed remuneration amounting to up to 2% of the device's value; this could impose significant additional costs on manufacturers and importers of general-purpose electronic devices irrespective of whether the devices are actually used to make private copies of copyrighted works. Details of the proposal have yet to be released, leaving affected companies unable to assess its scope, methodology, covered products, calculation mechanism, and potential economic impact; stakeholders have raised concerns regarding the transparency of the process and the opportunity for meaningful input before the measure is finalized, and adoption without publication of the full proposal and an adequate consultation period could raise concerns regarding Mexico's commitments under Chapter 28 (Good Regulatory Practices) of the USMCA. More broadly, introduction of a private-copying levy on general-purpose electronic devices could create an additional market-access barrier for electronic devices imported into Mexico and increase the cost of placing these products on the Mexican market. USTR should oppose this initiative as unwarranted rent-seeking, further ensconcing well-documented inefficiencies and perverse incentives of collection societies.⁸³⁶

Morocco

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Morocco's cloud qualification framework restricts U.S. suppliers' access to public-sector and critical-infrastructure contracts. Decree No. 2-24-921 of October 22, 2024 establishes qualification requirements for cloud providers serving covered entities with sensitive information systems or data.⁸³⁷ Implementing requirements were issued through Order No. 3-17-25 of August 1, 2025, establishing organizational, technical, legal, and governance criteria for qualification.⁸³⁸

For Level 1 qualification, applicable to hosting, managing, or operating sensitive information systems, providers must be incorporated under Moroccan law and locate their hosting infrastructure and systems used to operate and administer the services in Morocco. Level 2

⁸³⁶ Wolters Kluwer. 2013. *Private copying levy: the aftershocks of Padawan*.

<https://legalblogs.wolterskluwer.com/copyright-blog/private-copying-levy-the-aftershocks-of-padawan/>.

⁸³⁷ Decree No. 2-24-921 concerning the use of cloud service providers by entities and critical infrastructure with sensitive information systems or data [Morocco]. (2024, October 22). Articles 2–5.

https://www.dgssi.gov.ma/sites/default/files/2024-11/decret%202-24-921_ar_0.pdf

⁸³⁸ Direction Générale de la Sécurité des Systèmes d'Information (DGSSI). (2025). *Publication au Bulletin officiel de l'arrêté du Chef du gouvernement n° 3-17-25 du 7 safar 1447 (1er août 2025) fixant le référentiel des exigences de qualification des prestataires de services Cloud*.

<https://www.dgssi.gov.ma/fr/actualites/publication-au-bulletin-officiel-de-larrete-du-chef-du-gouvernement-ndeg-3-17-25-du-7/>

qualification, required for processing, managing, or storing sensitive data, adds Moroccan majority-ownership requirements and restrictions on control by other shareholders. It also requires domestic data processing and storage, administration and supervision of services exclusively from within Morocco, and Moroccan personnel responsible for service operation and management. These conditions restrict cross-border delivery and disadvantage U.S. suppliers, including locally established subsidiaries. The decree permits exceptional waivers of specified ownership and control conditions with prior approval from the Head of Government. It also temporarily permits use of unqualified providers where an equivalent qualified service is unavailable, subject to risk assessment. These exceptions do not provide a general right of access for foreign suppliers.

These restrictions raise concerns regarding Morocco's government procurement commitments under the U.S.-Morocco Free Trade Agreement.⁸³⁹ For covered procurements, Article 9.2 requires national treatment and prohibits discrimination against locally established suppliers based on foreign affiliation or ownership. Article 9.7 also prohibits technical specifications and conformity-assessment procedures that create unnecessary obstacles to bilateral trade. Application of these obligations depends on the agreement's entity and service coverage, thresholds, exclusions, and applicable exceptions, including essential-security provisions. CCIA urges USTR to engage with Morocco to ensure that cloud qualification and procurement requirements comply with its trade commitments. Morocco should remove discriminatory ownership and nationality conditions and adopt proportionate, risk-based security requirements that allow qualified U.S. suppliers to compete, including through recognition of relevant international security standards.

Nepal

Government-Imposed Content Restrictions and Related Access Barriers

Nepal's 2023 National Cyber Security Policy⁸⁴⁰ calls for developing a government-owned intranet and a National Internet Gateway to limit access to foreign websites. While the gateway's architecture or filtering requirements have not been specified, Nepalese and international digital-rights organizations warn that a centralized gateway could facilitate surveillance and censorship, undermine network resilience, and restrict cross-border

⁸³⁹ *United States–Morocco Free Trade Agreement*. (2004). Office of the United States Trade Representative. <https://ustr.gov/trade-agreements/free-trade-agreements/morocco-fta/final-text>

⁸⁴⁰ Republica. (2023, August 9). *Govt approves National Cyber Security Policy 2023*. <https://myrepublica.nagariknetwork.com/news/govt-approves-national-cyber-security-policy-2023/>

connectivity.⁸⁴¹ Implementation along these lines could create operational and market-access barriers for U.S. digital services.⁸⁴²

On February 9, 2026, Nepal's National Assembly approved the withdrawal of the Social Media Bill, 2081 (2025), which had proposed mandatory platform registration, broad content restrictions, and criminal penalties for online expression.⁸⁴³ Its withdrawal removes that legislative proposal but leaves in place separate registration and moderation requirements imposed under the 2023 Social Media Directive.

On September 4, 2025, Nepal ordered the blocking of 26 social media platforms for failing to register under its existing regulatory framework.⁸⁴⁴ The government lifted the ban on September 9 following mass protests. The episode demonstrates the market-access risks associated with enforcing platform-registration requirements through nationwide blocking. CCIA urges USTR to monitor any renewed restrictions.

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.⁸⁴⁵ Additionally, licensed Broadcast OTT providers with Nepal-based customers or generating fees in Nepal must maintain local cache servers and register customers on a Nepal-based server. They must retain customer information and transaction records, preserve broadcast material for at least 60 days, and adopt age-based categorization of Broadcast OTT content.

In June 2026, Nepal revised its broadcasting regulations to specify additional requirements for foreign OTT services.⁸⁴⁶ Reported fees include NPR 1 million per foreign OTT program-provider platform and NPR 2.5 million per platform for distributors of foreign OTT signals with downlink permission. An OTT broadcasting-service license carries a NPR 10 million fee. These category-specific charges add financial barriers for foreign streaming services.

⁸⁴¹ Internet Society. 2024. *Nepal's Proposed National Internet Gateway*.

<https://www.internetsociety.org/resources/2024/internet-impact-brief-nepals-proposed-national-internet-gateway/>

⁸⁴² 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/>

⁸⁴³ National Assembly, Federal Parliament of Nepal. (n.d.). सामाजिक सञ्जाल विधेयक, २०८१ (मिति २०८२/१०/२६ मा फिर्ता) [Social Media Bill, 2081 (withdrawn February 9, 2026)]. <https://na.parliament.gov.np/np/bills/JCC7TZJz>

⁸⁴⁴ The New York Times News Service. (2025, September 8). *Nepal bans 26 social media platforms, including Facebook and YouTube*. Aletihad.

<https://en.aletihad.ae/news/mena-world/4604072/nepal-bans-26-social-media-llatforms--including-facebook-and>

⁸⁴⁵ 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>

⁸⁴⁶ Republica. (2026, June 16). *Government brings OTT platforms under legal regulation*.

<https://myrepublica.nagariknetwork.com/news/government-brings-ott-platforms-under-legal-regulation-37-97.html>

Other Barriers to Digital Trade

In July 2026, Nepal approved the National Advertisement Policy, 2083, which calls for regulation of advertising through social media, digital platforms, influencers, and artificial intelligence.⁸⁴⁷ It also proposes incentives for advertising domestic goods and services and requiring companies selling foreign goods and services to allocate a portion of their business expenditure to consumer-awareness programs. USTR should monitor implementing measures, including the scope and amount of any mandatory expenditure, and whether it disproportionately affects foreign firms.

Nepal's Electronic Commerce Directive, 2082, issued in 2026, adds operational requirements, including encryption of sensitive personal information, use of Nepal Rastra Bank-approved digital payment gateways, and retention of transaction and complaint records for at least five years.⁸⁴⁸ Platforms must immediately suspend transactions following unauthorized access, information leakage, or system malfunction and resume only after recovery. These obligations add compliance costs and service-continuity risks.

Taxation of Digital Products and Services

Nepal introduced a 2% DST through its Finance Act for FY 2022/23, effective July 17, 2022.⁸⁴⁹ The tax applies to revenue from covered digital services supplied by non-residents to users in Nepal and sales of data collected from Nepal-based users. Targeted advertising directed at users in Nepal is covered even when sold to an overseas advertiser. Qualifying sales to Nepal-based business users for business purposes are excluded. Annual covered transactions up to NPR 3 million are exempt; once that threshold is exceeded, the tax applies to the full covered transaction value. In 2025, Nepal expanded the definition of “digital services” in the Finance Bill for FY 2025/2026 to explicitly include targeted online advertisements and paid personal advertisements in the scope of its DST.⁸⁵⁰ CCIA considers the tax's exclusive application to non-residents and its transaction-value basis inconsistent with established international tax principles, imposing additional tax and compliance burdens on U.S. and other foreign providers. Although income on revenue subject to the DST is exempt from Nepal's income tax, potential double taxation remains a concern.

⁸⁴⁷ Rastriya Samachar Samiti. (2026, July 2). *National Advertisement Policy passed; Regulations from digital ad to deepfake in priority*. The Rising Nepal. <https://risingnepaldaily.com/news/82849>

⁸⁴⁸ Ministry of Industry, Commerce and Supplies, Nepal. (2026). *विद्युतीय व्यापार (ई-कमर्स) निर्देशिका, २०८२ [Electronic Commerce Directive, 2082]*, Sections 8(1), 9(1), and 14. https://giwmscdnone.gov.np/media/pdf_upload/ecommerce-directives_8errkt4.pdf

⁸⁴⁹ Inland Revenue Department, Nepal. (2022, July 7). *Notice Regarding Digital Service Tax (DST) and Value Added Tax for Non-Resident Person*. https://giwmscdntwo.gov.np/media/pdf_upload/bid7_o03jdri.pdf

⁸⁵⁰ Baker Tilly Nepal. (2025). *Nepal Tax Fact 2025/26 (2082/83): Major Taxation Provisions*. https://bakertilly.com.np/storage/download/1750310698_Tax_Fact_2025-2026.pdf.

Netherlands

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Netherlands' government-wide cloud policy (*Herziening rijksbreed cloudbeleid*), adopted by the Council of Ministers in July 2026, functions as a *de facto* discriminatory barrier against U.S. cloud providers. While framed as risk management rather than an outright ban, the policy systematically steers the Dutch public sector's highest-value workloads toward EU-headquartered suppliers through a jurisdiction-based test rather than a data-location test. Critical and essential entities — energy, water, banking and payments, telecoms and digital infrastructure, major transport, healthcare and systemic parts of central government — are advised against using, for their primary processes, any supplier that falls “in part” under a non-EU/EEA jurisdiction. This wording is drafted to capture U.S.-parented providers even where all data is stored and processed within the EU, casting doubt over whether U.S. firms can serve these workloads at all — regardless of the substantial local investment, EU data residency and sovereign offerings they provide. The policy is reinforced by a default exclusion of public cloud for government email and document management (overridable only on a demanding three-part test with ministerial sign-off), a cybersecurity screen that can exclude suppliers from countries deemed to run “an active cyber programme against Dutch interests”, and a layer of per-deployment risk assessments, exit-plan obligations and central notification requirements that materially raise the cost and lengthen the sales cycle of every significant U.S. cloud deployment. Taken together, these measures discriminate on the basis of corporate nationality rather than any objective security or performance standard, disadvantage U.S. providers relative to EU-based competitors in procurement, and are consistent with a broader European trend toward using jurisdiction — not data location — as the deciding criterion for market access. USTR should evaluate this policy in light of the WTO GPA obligations the Netherlands has not to discriminate in the procurement of cloud services on the basis of nationality.

New Zealand

Forced Revenue Transfers for Digital News

On December 4, 2022, New Zealand 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.⁸⁵¹ 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.

⁸⁵¹ 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>

On August 17, 2023, the government introduced the “Fair Digital News Bargaining Bill,” which would establish a mandatory bargaining framework for covered digital platforms making New Zealand news content available, including through links.⁸⁵² Where voluntary agreements cannot be reached, the framework would provide for mediation and binding final-offer arbitration. The government’s 2022 regulatory impact assessment focused on Google and Meta and estimated that the proposed bargaining framework could generate NZ\$40-60 million in gross annual payments to news businesses, or NZ\$30–50 million above estimated annual payments under the status quo.⁸⁵³ The Economic Development, Science and Innovation Committee reported the bill back on May 28, 2024, recommending that it not pass in its current form. The bill remains awaiting its second reading and has not been enacted.

The political and regulatory outlook for the legislation remains closely tied to the upcoming election (November 7), where polls between the Labour and National parties continue to show a tight race. A Labour-led government would present a high regulatory risk of implementing a mandatory framework closely aligned with Australia’s News Media Bargaining Code. In a high-stakes campaign environment, the Labour Party may announce an election commitment to a News Bargaining Initiative (NBI) framed as legislated compensation for media companies. Furthermore, any future governing coalition involving the Green Party would likely elevate the priority and urgency of enacting NBI legislation in the next term. USTR should monitor this issue closely and be prepared to oppose it.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

On August 24, 2026, the government introduced the Online Safety (Minimum Age and Child Safety Risk Assessment) Bill, which remains awaiting its first reading.⁸⁵⁴ The bill would require covered platforms to take reasonable steps to prevent New Zealand users under 16 from holding accounts. Coverage would extend to content-sharing services with specified features—including personalized recommendations, endless feeds, engagement feedback, or disappearing content—and AI companion services. Exclusions include services primarily providing messaging, online gaming, music or podcasts, professional networking, education, health, or general-purpose AI assistance.

Covered operators would also have to prepare child-safety risk assessments at least annually addressing risks to users under 18, with senior-management confirmation. For the most serious corporate breaches, maximum civil penalties would be the greater of NZ\$40 million or 10% of annual global turnover. Courts could also issue service or access restriction orders involving

⁸⁵² New Zealand Parliament. (2023). *Fair Digital News Bargaining Bill* (No. 278-1). <https://bills.parliament.nz/v/6/fc7faac0-2ec0-4e47-7ab5-08db9ebb2302>

⁸⁵³ 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>

⁸⁵⁴ New Zealand Parliament. (2026, August 25). *Online Safety (Minimum Age and Child Safety Risk Assessment) Bill* (No. 339-1). <https://bills.parliament.nz/v/6/ba928141-d337-493a-01d5-08df0193ecfa>

payment providers, advertising networks, internet service providers, and app stores. These proposed obligations could increase compliance costs and market-access risks for U.S. suppliers through age-assurance requirements, recurring risk assessments, and restrictions on access to noncompliant services.

Nigeria

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

NITDA's 2019 Guidelines for Nigerian Content Development in ICT require data and information management companies to host sovereign data in Nigeria unless NITDA expressly approves offshore hosting.⁸⁵⁵ They also require government ministries, departments, and agencies to host sovereign data locally. These provisions restrict offshore cloud services, but do not establish a blanket localization requirement for all data.

NITDA's National Cloud Computing Guideline, 2026, scheduled to take effect on January 1, 2027, introduces additional localization and procurement restrictions.⁸⁵⁶ Sovereign data classified at Level 2 or above must be hosted in Nigeria by default, subject to specified exceptions and waivers. Financial data handled by regulated financial institutions must primarily be hosted, processed, and stored domestically. Federal public institutions must prioritize indigenous cloud providers; foreign providers may be engaged only where NITDA confirms that local capacity is unavailable or grants provisional indigenous status based on qualifying investment in local data-center infrastructure. These conditions would restrict U.S. suppliers' ability to serve Nigeria through global cloud infrastructure.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

NITDA's 2022 Code of Practice for Interactive Computer Service Platforms and Internet Intermediaries requires platforms with more than one million registered users in Nigeria to incorporate locally, maintain a Nigerian contact address, and appoint a liaison officer.⁸⁵⁷

NITDA may extend these obligations to smaller platforms on specified public-interest grounds. The Code also requires removal of unlawful content within 48 hours of notice from an authorized government agency, annual compliance reporting, and cooperation

⁸⁵⁵ National Information Technology Development Agency. (2019, August). *Guidelines for Nigerian Content Development in Information and Communication Technology (ICT)* (as amended), §13.1(2). <https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf>

⁸⁵⁶ National Information Technology Development Agency. (2026, August 4). *National Cloud Computing Guideline 2026*, §§5, 9.3, and 17.2(V). https://nitda.gov.ng/wp-content/uploads/2026/08/NATIONAL-GUIDELINE-FOR-CLOUD-COMPUTING-IN-NIGERIA-2026_Final.pdf

⁸⁵⁷ National Information Technology Development Agency. (2022, September 26). *Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries*, definition of "Large Service Platforms" and Part III(1)–(3). <https://nitda.gov.ng/wp-content/uploads/2022/10/APPROVED-NITDA-CODE-OF-PRACTICE-FOR-INTERACTIVE-COMPUTER-SERVICE-PLATFORMS-INTERNET-INTERMEDIARIES-2022-002.pdf>

with court-ordered information requests. These obligations increase compliance costs and constrain cross-border service delivery.

Separately, NCC issued its Internet Code of Practice 2026 on February 13, 2026.⁸⁵⁸ Chapter Six establishes additional obligations for covered online platforms, digital service providers, and application service providers, including submission of community rules within six months of issuance, twice-yearly reporting, and designated channels for regulatory engagement. Section 5.4 requires internet access service providers to notify NCC before deploying AI or other emerging technologies for network management and customer engagement, and to maintain the ability to withdraw those tools when directed. These provisions introduce additional regulatory obligations, subject to the July 2026 harmonization directive described below.

On July 7, 2026, the communications ministry directed NCC, NITDA, and NDPC to defer implementation or enforcement of recently issued measures affecting internet platforms, online intermediaries, and other digital-economy matters undergoing inter-agency policy harmonization.⁸⁵⁹ Existing provisions within the agencies' statutory mandates remain enforceable where consistent with the ministerial directive. The measure addresses overlapping regulation rather than repealing the existing platform framework.

Under the Advertising Regulatory Council of Nigeria Act 2022, ARCON requires pre-exposure vetting of advertisements directed at Nigerian audiences, including online advertising.⁸⁶⁰ This creates substantial compliance burdens for platforms serving advertising at scale. In 2022, ARCON brought a ₦30 billion claim against Meta over unapproved advertisements; it withdrew that lawsuit in July 2024.⁸⁶¹ Separately, on June 18, 2026, the Federal High Court in Lagos set aside ARCON's ₦60 billion sanction against Facebook Nigeria Operations Limited, finding that the regulator exceeded its powers and denied the company a fair hearing.⁸⁶² The judgment addressed that sanction and did not abolish advertising-vetting requirements.

⁸⁵⁸ Nigerian Communications Commission. (2026, February 13). *Internet Code of Practice 2026*. <https://ncc.gov.ng/media/5104/view>

⁸⁵⁹ Federal Ministry of Communications, Innovation and Digital Economy. (2026, July 7). *Federal Ministry Directs Harmonised Approach to the Regulation of Internet Platforms and Online Intermediaries*. <https://fmcide.gov.ng/federal-ministry-directs-harmonised-approach-to-the-regulation-of-internet-platforms-and-online-intermediaries/>

⁸⁶⁰ Federal Republic of Nigeria. (2022, July 5). *Advertising Regulatory Council of Nigeria Act, 2022* (Act No. 23), §§54 and 63. <https://placng.org/i/wp-content/uploads/2022/10/Advertising-Regulatory-Council-of-Nigeria-Act-2022.pdf>

⁸⁶¹ Akingbolu, R. (2024, July 22). *N30bn Lawsuit: ARCON Explains Reason for Withdrawal Suit against Meta*. THISDAY.

<https://www.thisdaylive.com/2024/07/22/n30bn-lawsuit-arcon-explains-reason-for-withdrawal-suit-against-meta/>

⁸⁶² Onyekwere, J. (2026, July 7). *Court upturns ₦60b fine against Facebook Nigeria*. The Guardian. <https://guardian.ng/news/court-upturns-n60b-fine-against-facebook-nigeria/>

Restrictions on Cross Border Data Flows

The Nigeria Data Protection Act 2023 conditions international transfers on adequate protection or specified statutory exceptions, including informed consent and certain contractual necessities.⁸⁶³ Its General Application and Implementation Directive (GAID), effective September 19, 2025, provides additional transfer requirements. Schedule 5 identifies NDPC adequacy decisions, Commission-approved transfer instruments—including standard contractual clauses and binding corporate rules—and other lawful bases as transfer routes. Approval requirements for these instruments add administrative burdens for companies relying on international data flows.

The 2019 Guidelines additionally require telecommunications and networking service companies to host subscriber and consumer data within Nigeria. Separately, Central Bank guidelines require domestic card transactions to be routed through local switching infrastructure.

Forced Revenue Transfers for Digital News

On July 6, 2026, the Federal Competition and Consumer Protection Commission announced an investigation following complaints by Nigerian media organizations concerning Meta, Alphabet, X, and generative AI platforms.⁸⁶⁴ The inquiry covers alleged anticompetitive conduct, unauthorized extraction and use of journalistic content for AI development and training, and publishers' opportunities to negotiate compensation. FCCPC stated that the investigation does not presume wrongdoing. The inquiry creates potential regulatory exposure for U.S. platforms, but its announcement does not establish a mandatory news-payment regime or a finding of infringement.

Taxation of Digital Products and Services

The Nigeria Tax Act 2025, effective January 1, 2026, retains taxation of non-resident businesses with significant economic presence in Nigeria, expressly covering activities including online advertising, digital content, app stores, and cloud computing.⁸⁶⁵ Section 17 provides for profit attribution using the non-resident business's profit margin where attributable profits cannot be determined or fall below that benchmark. Tax payable is subject to a floor equal to applicable withholding tax or, where income is not subject to withholding, 4% of Nigerian-source income. This can create tax exposure disconnected from the profitability of Nigerian operations, and, given the absence of a U.S.-Nigeria tax treaty, double taxation.

⁸⁶³ Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*, §§41–43.

<https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf>

⁸⁶⁴ Federal Competition and Consumer Protection Commission. (2026, July 6). *President Tinubu Directs FCCPC to Investigate Big Techs*. <https://fccpc.gov.ng/president-tinubu-directs-fccpc-to-investigate-big-techs/>

⁸⁶⁵ Federal Republic of Nigeria. (2025, June 26). *Nigeria Tax Act, 2025* (Act No. 7), commencement provision and §17. <https://nass.gov.ng/documents/download/11249>

Other Barriers to Digital Trade

Following the Federal High Court ruling setting aside ARCON's initial ₦60 billion penalty against Meta, ARCON filed an appeal and issued a fresh ₦60 billion enforcement notice demanding that foreign platforms pre-vet all advertisement creative content with ARCON prior to publication.⁸⁶⁶ Mandatory ad pre-vetting creates severe administrative friction and discriminates against cross-border digital advertising platforms. CCIA urges USTR to press Nigeria to eliminate mandatory advertisement pre-vetting requirements.

Norway

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Norway is developing a closed national cloud service for sensitive, unclassified government information, requiring companies serving the public sector to store over 60% of data using this national service. In its 2026 budget proposal, the government proposed NOK 30 million for a preparatory project, explicitly seeking to reduce dependence on foreign providers. The Government is also applying pressure to extend this requirement to sectors such as energy, telecoms and financial services. National-control requirements that could restrict participation by U.S. cloud suppliers, depending on their design.⁸⁶⁷ USTR should seek clarification of supplier eligibility and encourage proportionate, nondiscriminatory security requirements.

Discriminatory Local Content Quotas and Audiovisual Service Mandates

Based on a 2025 law, investment obligations on streaming services are scheduled to take effect on January 1, 2027.⁸⁶⁸ Covered audiovisual on-demand providers established in Norway or another EEA state and targeting Norwegian audiences will have to invest 4% of annual Norwegian gross revenue, excluding VAT, in qualifying Norwegian audiovisual works. Exemptions include providers below €2 million in annual turnover or 1% audience share. The

⁸⁶⁶ Lawyard. (2026, July 8). Federal High Court quashes ₦60 billion ARCON fine against Facebook Nigeria, declares regulator acted beyond powers. <https://www.lawyard.org/news/federal-high-court-nullifies-%E2%82%A660-billion-arcon-fine-on-facebook-nigeria-rules-regulator-exceeded-legal-powers>.

⁸⁶⁷ Norwegian Ministry of Digitalisation and Public Governance. (2025, February 28). *Ekspertutvalget for nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur – Ekomsikkerhetsutvalget*. <https://www.regjeringen.no/no/dokumenter/nasjonal-kontroll-med-kritisk-digital-kommunikasjons-infrastruktur/id3089835/?ch=2>; Norwegian Ministry of Justice and Public Security. (2025, October 15). *Regjeringen styrker arbeidet med sikkerhet og beredskap*. <https://www.regjeringen.no/no/aktuelt/regjeringen-styrker-arbeidet-med-sikkerhet-og-beredskap/id3122316/>; Norwegian Ministry of Digitalisation and Public Governance. (2025, February 28). *Ekspertutvalget for nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur – Ekomsikkerhetsutvalget*. <https://www.regjeringen.no/no/dokumenter/nasjonal-kontroll-med-kritisk-digital-kommunikasjons-infrastruktur/id3089835/?ch=2>

⁸⁶⁸ Norwegian Ministry of Culture and Equality. (2026, February 2). *Ny investeringsplikt for strømmetjenester på høring*. <https://www.regjeringen.no/no/aktuelt/ny-investeringsplikt-for-strommetjenester-pa-horing/id3147773/>

implementing proposal adds registration and annual reporting requirements. This obligation would constrain content-investment decisions and increase compliance costs for covered U.S. streaming businesses operating through EEA establishments.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

In August 2026, Norway reaffirmed plans to introduce legislation restricting social-media access for youth until January 1 of the year a user turns 16.⁸⁶⁹ The government intends to enforce this ban through the Digital Services Act, including provider responsibility for age verification. However, the European Commission and EFTA Surveillance Authority indicated that compatibility with EEA law depends on the national legislation itself imposing no obligations on providers. USTR should monitor the final proposal for disproportionate verification burdens and fragmentation of cross-border services.

Pakistan

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Sectoral regulators impose restrictive data localization requirements relating to the use of cloud computing. In 2024, the Securities and Exchange Commission of Pakistan prohibited licensed digital lenders from storing data on cloud infrastructure located outside the country.⁸⁷⁰ 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.⁸⁷¹ 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.

In June 2026, MoITT published a draft National Data Governance Policy covering federal public bodies and their contractors, processors, and partners.⁸⁷² The draft would require restricted, confidential, and personal government data to be hosted, stored, and processed in Pakistan, with specific Pakistan Digital Authority approval for cross-border processing or remote access. Other internal government data could be processed offshore only with prior approval. These proposed requirements would restrict foreign cloud providers' ability to serve public-sector customers using global infrastructure.

⁸⁶⁹ Norwegian Ministry of Children and Families & Ministry of Digitalisation and Public Governance. (2026, August 13). *Positiv tilbakemelding frå EU til ny lov om sosiale medium*.

<https://www.regjeringen.no/no/aktuelt/positiv-tilbakemelding-fra-eu-til-ny-lov-om-sosiale-medium/id3170219/>
⁸⁷⁰ Securities and Exchange Commission of Pakistan. (2024). *Circular No. 12 of 2024: Requirements for NBFCs engaged in digital lending*.

<https://www.secp.gov.pk/document/circular-no-12-of-2024-requirements-for-nbfc-engaged-in-digital-lending/>
⁸⁷¹ State Bank of Pakistan. (2024). *FE Circular No. 02 of 2024: Issuance of Regulatory Framework for Exchange Companies*. <https://www.sbp.org.pk/epd/2024/FEC2.htm>

⁸⁷² Ministry of Information Technology and Telecommunication. (2026, June). *Data Governance Policy 2026 (draft)*. <https://moitt.gov.pk/SiteImage/Policies/Data%20Governance%20Policy%20June%202026.pdf>

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.⁸⁷³ In March 2026, the government appointed SMPRA's first chairman, advancing implementation of the new regulatory framework.⁸⁷⁴ The amended law grants SMPRA broad legislative and enforcement powers, including the authority to require social media platforms to register 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 is known to be fake or false, or for which sufficient grounds support that belief beyond a reasonable doubt, 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. Separately, industry concerns regarding the earlier Removal and Blocking of Unlawful Online Content Rules included requirements to monitor and block livestreaming content, meet short takedown deadlines, and disclose data to authorities in decrypted and readable formats.⁸⁷⁵ 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.

The government has repeatedly deployed internet shutdowns in response to protests and elections, imposing large economic losses and harming human rights.⁸⁷⁶ Industry has reported that shutdowns have introduced significant uncertainty and encouraged investment flight.⁸⁷⁷ Access Now documented 20 internet shutdowns in Pakistan during 2025, demonstrating the continued use of connectivity restrictions. Separately, in August 2024, the Pakistan Software Houses Association warned that disruptions associated with implementation of an internet firewall could cost the economy up to US\$300 million.⁸⁷⁸

⁸⁷³ National Assembly of Pakistan. (2025, January 29). *Prevention of Electronic Crimes (Amendment) Act, 2025 (Act No. II of 2025)*. https://www.na.gov.pk/uploads/documents/679b243193585_457.pdf

⁸⁷⁴ The News International. (2026, March 20). *Ayaz Shaukat appointed first SMPRA chairman*. <https://www.thenews.pk/print/1405601>

⁸⁷⁵ Asia Internet Coalition. (2021, June 28). *Industry comments on the Amendment—Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules*. <https://aicasia.org/download/405/>

⁸⁷⁶ Access Now. (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/>

⁸⁷⁷ 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/>

⁸⁷⁸ Shahid, A. (2024, August 15). *Pakistan's internet firewall could cost economy \$300 million, association says*. Reuters.

In November 2025, PTA announced licenses for VPN providers under its reinstated Class Value Added Services licensing regime. In January 2026, Proton reported that its services had been restricted in Pakistan since December 22, 2025.⁸⁷⁹ Restrictions on VPN access can disrupt secure business connectivity and impede cross-border delivery of digital services.

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.⁸⁸⁰ In January 2025, MoITT informally shared an updated draft, but it has yet to be made publicly available. The bill remains unenacted. The January 2025 draft 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. These proposed powers could enable restrictions on cross-border transfers on broadly framed public-interest or national-security grounds. If enacted, the transfer restrictions could impede firms’ use of global cloud infrastructure, depending on the final legislation and implementing measures. The draft also grants regulators sweeping powers with few procedural safeguards or 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.

<https://www.reuters.com/technology/pakistans-internet-firewall-could-cost-economy-300-million-association-says-2024-08-15/>

⁸⁷⁹ Castro, C. (2026, January 7). *Pakistan begins blocking unregistered VPN apps—and this popular service is among the casualties*. TechRadar.

<https://www.techradar.com/vpn/vpn-privacy-security/pakistan-begins-blocking-unregistered-vpn-apps-and-this-popular-service-is-among-the-casualties>; Khan, N. (2024, November 20). *Pakistan VPN ban could hike IT sector operational costs by \$150 million annually—association*. Arab News.

<https://www.arabnews.pk/pakistan/pakistan-vpn-ban-could-hike-it-sector-operational-costs-by-150-million-annually-association-2580050>

⁸⁸⁰ Ministry of Information Technology and Telecommunication. (2023). *Draft Personal Data Protection Bill, 2023*. <https://moitt.gov.pk/Detail/YjVmNzU0MWMtYzBkMC00Yjg5LTk1ODktOTJiODYzZTY5ZWVk>

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.⁸⁸¹ On July 30, 2025, the Federal Board of Revenue issued S.R.O. 1366(I)/2025 exempting digitally ordered goods and services supplied from outside Pakistan, with retroactive effect from July 1, 2025.⁸⁸² The relief was implemented through an exemption notification rather than repeal of the underlying Act. 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. However, an applicable income-tax treaty’s permanent-establishment definition prevails over the domestic definition. The implications for eligible U.S. suppliers must therefore be assessed under the U.S.–Pakistan income-tax treaty.⁸⁸³

Panama

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

AIG Resolution No. 07 of April 30, 2025, approving the government’s ICT standards, requires databases containing sensitive state-security or institutional information to remain in Panama.⁸⁸⁴ Section 30.8 defines sensitivity by reference to confidential national-security information whose disclosure, alteration, or loss could compromise national security. Other government cloud services and databases may be hosted abroad with justification and AIG evaluation and authorization before procurement. The standards also prohibit public-cloud hosting for mission-critical or state-security services. Section 30.9 separately bars sensitive institutional data, including specified sensitive personal data, from public clouds or external private hosting. These localization and hosting restrictions limit U.S. suppliers’ ability to serve covered

⁸⁸¹ Government of Pakistan. (2025). *Finance Bill, 2025*.

<https://fbr.gov.pk/Budget2025-26/FinanceBill/Finance-Bill-2025.pdf>; Computer & Communications Industry Association. (2025). *Pakistan’s ‘Digital Presence Proceeds’ Tax*.

<https://ccianet.org/wp-content/uploads/2025/07/Pakistans-%E2%80%98Digital-Presence-Proceeds-Tax.pdf>

⁸⁸² Federal Board of Revenue. (2025, July 30). *Notification (Digital Presence Proceeds Tax)*, S.R.O. No.

1366(I)/2025. [https://download1.fbr.gov.pk/SROs/20257302072529390SRO1366\(I\)2025.pdf](https://download1.fbr.gov.pk/SROs/20257302072529390SRO1366(I)2025.pdf)

⁸⁸³ United States and Pakistan. (1957, July 1). *Convention for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with Respect to Taxes on Income*.

<https://www.irs.gov/pub/irs-trty/us-pakistan-income-tax-treaty.pdf>

⁸⁸⁴ Autoridad Nacional para la Innovación Gubernamental. (2025, April 30). *Resolución No. 07: Normas generales para la gestión de las tecnologías de la información y comunicación (TIC) en el Estado, versión 2.1*, § 30.8.

<https://aig.gob.pa/descargas/2019/06/1-resolucion-no-07-2025-normas-generales-para-la-gestion-de-las-tics-version-21.pdf>

government workloads using overseas infrastructure or public-cloud offerings. Overseas hosting of otherwise eligible government data and services remains subject to prior AIG authorization.

For all other cloud services, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and databases not linked to State-security platforms or sensitive institutional data, public-sector entities may store data outside Panamanian territory only after obtaining prior evaluation and authorization from the AIG on a case-by-case basis, submitting a description of the data, the provider, the country of storage, the retention period, and the provider's security measures. This prior-approval requirement introduces delay and administrative friction that a notification-based mechanism would avoid, and is more restrictive than the practice in peer jurisdictions. Second, because the categories of "State security" and "sensitive institutional data" are broadly defined, an expansive interpretation could pull a significant share of public-sector workloads back into mandatory localization, since internationally competitive providers operate no in-country region in Panama. Building on the progress achieved through Resolution 42, Panama should replace the prior-authorization requirement with a notification mechanism featuring clear timelines, define the "sensitive" and "State-security" data categories narrowly and precisely, and adopt a technology-neutral, risk-based framework that recognizes cloud multi-region resilience and internationally recognized security certifications (e.g., ISO 27001, SOC) as compliant.

Other Barriers to Digital Trade

Effective June 24, 2026, AIG Resolution No. 18 requires government digital platforms involving citizen access or interaction to obtain AIG approval before launch.⁸⁸⁵ Applications must include independent cybersecurity-test validation, evidence addressing critical and high vulnerabilities, and functional and load-test results. AIG has up to 15 days to respond, and operation without approval is prohibited. This creates an additional compliance requirements for suppliers supporting government platforms

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.⁸⁸⁶ In September 2026, the Department of Information and Communications Technology

⁸⁸⁵ Autoridad Nacional para la Innovación Gubernamental. (2026, June 15). *Resolución No. 18*, Articles 1, 5–6. Gaceta Oficial No. 30553 D, June 24, 2026.

<https://aig.gob.pa/descargas/2019/06/resolucion-18-2026-autorizacion-de-los-sistemas-de-las-entidades-por-la-aig-gaceta.pdf>

⁸⁸⁶ 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>

and the Office of Censorship drafted legislation to implement this policy.⁸⁸⁷ Proposed measures include requiring social media providers to register as companies in Papua New Guinea, classifying platforms according to their suitability, and imposing age restrictions on platforms considered inappropriate for children. Local incorporation and platform-classification requirements could increase compliance costs and restrict market access for foreign providers.

Separately, the draft Cybersecurity Bill 2026, released for consultation in August, would require social media platforms to prevent children under 16 ordinarily resident in Papua New Guinea from creating or maintaining accounts and implement age-verification systems.⁸⁸⁸ The draft expressly requires an alternative to government-issued identification and would establish a Child Online Safety Commissioner. These proposed requirements could increase verification and compliance costs for foreign platforms serving the market.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The draft Data Governance and Data Protection Bill 2026, released for consultation in August, would generally require government agencies to store and process restricted data and citizens' personal data domestically, subject to specified transfer and hosting exceptions.⁸⁸⁹ Certain government, digital public infrastructure, and strategically designated data would require domestic hosting or a ministerially approved sovereign hosting arrangement. Private data controllers processing personal data offshore would also have to notify the regulator and ensure compliant protections. These proposed requirements could limit foreign cloud providers' ability to serve government customers and increase cross-border processing costs.

Peru

Customs-Related Restrictions and Import Barriers for Goods

Under Article 5.7 of the U.S.-Peru Trade Promotion Agreement Peru agreed to institute expedited customs procedures for express shipments. However, the Peruvian government has limited the number of shipments to individuals without a tax number (RUC) to three per year. Since millions of Peruvian adults lack an RUC, this requirement limits the ability for individuals to import goods for personal use, which constitutes a trade barrier and a limitation to the use of express delivery shipments in Peru.

⁸⁸⁷ Department of Information and Communications Technology, Papua New Guinea. (2026, September 1). *DICT, Censorship Office Work on New Legal Framework for Social Media to Protect Children Online*. <https://www.ict.gov.pg/dict-censorship-office-work-on-new-legal-framework-for-social-media-to-protect-children-online/>

⁸⁸⁸ Department of Information and Communications Technology, Papua New Guinea. (2026). *Cybersecurity Bill 2026 (Fourth Draft for External Consultation)*, sections 49–51. https://www.ict.gov.pg/Draft%20Bill/Cybersecurity%20Bill%202026_V4_Consultation.pdf

⁸⁸⁹ Department of Information and Communications Technology, Papua New Guinea. (2026). *Data Governance and Data Protection Bill 2026 (Fifth Draft)*, sections 81–83. https://www.ict.gov.pg/Draft%20Bill/DGDP%20Act%202026%20Fifth%20Draft_PublicConsultation.pdf

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Numerous legislative proposals on children's online safety have advanced over the past two years proposing protective telecommunications profiles, a registry identifying devices used by minors, and access controls for public internet services. On February 9, 2026, the Health and Population Committee approved a separate consolidated proposal.⁸⁹⁰ During the second half of the year, new proposals restricting minors' access to social media were tabled and discussed including Bill 498-2026-2031-CD, which would prohibit children under 16 from holding social media accounts and require platforms to implement age-verification mechanisms to ensure compliance.⁸⁹¹ These proposals warrant scrutiny for potentially burdensome access-control and compliance obligations affecting digital services.

On February 7, 2026, Peru published Legislative Decree No. 1724, amending its Copyright Law to introduce conditional liability protections for internet access, caching, hosting, and search services, together with notice-and-takedown procedures.⁸⁹² This addresses Peru's longstanding implementation gap under Article 16.11(29) of the U.S.-Peru Trade Promotion Agreement. USTR's 2026 Special 301 Report continued to identify implementation concerns and criticized inadequate opportunities for stakeholder input.⁸⁹³ CCIA urges USTR to seek transparent implementation that provides effective intermediary protections consistent with the agreement.

Challenges to the Development of Artificial Intelligence

Supreme Decree No. 115-2025-PCM, published on September 9, 2025, implements Peru's AI Law, Law No. 31814.⁸⁹⁴ Its first implementation deadline for specified private-sector transparency and governance obligations fell on September 10, 2026. The first deadline scoped in AI for health, education, justice, security, economy and finance, with separate schedules for smaller businesses and innovative enterprises. Requirements include provision of records of high-risk systems' data sources and algorithmic logic, and human oversight of significant

⁸⁹⁰ Congreso de la República del Perú. (2026, February 9). *Aprueban dictámenes para proteger la salud mental infantil y uso seguro de internet*. <https://comunicaciones.congreso.gob.pe/noticias/aprueba-dictamenes-para-proteger-la-salud-mental-infantil-y-uso-seguro-de-internet/>

⁸⁹¹ Anselmo, R. (2026, October 6). Proyecto de ley plantea prohibir el uso de redes sociales a menores de 16 años en Perú [Bill proposes prohibiting social media use by children under 16 in Peru]. La República. <https://larepublica.pe/sociedad/2026/10/06/proyecto-de-ley-plantea-prohibir-el-uso-de-redes-sociales-a-menores-de-16-anos-en-peru-220098>.

⁸⁹² Presidencia de la República del Perú. (2026, February 7). *Decreto Legislativo N.º 1724, que modifica el Decreto Legislativo N.º 822, Ley sobre el Derecho de Autor, a fin de incorporar disposiciones en materia de eximentes de responsabilidad de proveedores de acceso a Internet y de proveedores de servicios en el entorno digital*. <https://busquedas.elperuano.pe/dispositivo/NL/2484948-7>

⁸⁹³ Office of the United States Trade Representative. (2026). *2026 Special 301 Report*. <https://ustr.gov/sites/default/files/files/Press/Releases/2026/2026%20Special%20301%20Report.pdf>

⁸⁹⁴ Presidencia del Consejo de Ministros. (2025, September 9). *Decreto Supremo N.º 115-2025-PCM, que aprueba el Reglamento de la Ley N.º 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país*. <https://busquedas.elperuano.pe/dispositivo/NL/2436426-1>

decisions in specified sectors. Private-sector impact assessments remain voluntary. Separately, Article 28.8 requires public entities to publish source code for publicly funded AI systems under a free or open license, subject to existing public-software and transparency rules. CCIA urges implementation that protects confidential business information and clarifies the scope of source-code obligations affecting government suppliers.

Restrictions on Cross-Border Data Flows

Peru's revised Personal Data Protection Law regulation, Supreme Decree No. 016-2024-JUS, took effect in March 2025.⁸⁹⁵ Articles 18–21 provide for transfers to countries with adequate protection or, otherwise, appropriate safeguards such as contractual clauses, subject to statutory exceptions. USTR's 2026 NTE Report states that, as of December 31, 2025, Peru had not initiated an assessment of U.S. adequacy despite repeated requests. The resulting reliance on additional safeguards increases compliance burdens for U.S. suppliers.⁸⁹⁶

Peru finalized the regulation implementing its Digital Trust Framework,⁸⁹⁷ through Supreme Decree No. 126-2025-PCM, effective February 3, 2026. The regulation, designed to promote cybersecurity, issued digital trust seals to public services, and subjects private sector intermediaries managing critical internet resources to incident-reporting requirements.

Article 20.2 requires covered public- and private-sector data platforms to integrate with the National Digital Security Center and provides for supervision of their data management. This raises concerns with respect to government intrusion, insufficient safeguards, and ambiguous provisions that could support future localization or cross-border transfer restrictions. CCIA urges Peru to clarify the scope of these obligations, protect confidential information, and ensure implementation does not require unnecessary localization or restrict access to foreign digital services.

To implement safeguards, Peru should 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.

⁸⁹⁵ Ministerio de Justicia y Derechos Humanos. (2024, November 30). *Decreto Supremo N.º 016-2024-JUS, que aprueba el Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales.*

<https://img.lpderecho.pe/wp-content/uploads/2024/11/Decreto-Supremo-016-2024-IUS-LPDerecho.pdf>

⁸⁹⁶ Office of the United States Trade Representative. (2026). *2026 National Trade Estimate Report on Foreign Trade Barriers.*

<https://ustr.gov/sites/default/files/files/Press/Releases/2026/National%20Trade%20Estimate%20Report%202026.pdf>

⁸⁹⁷ 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>

Philippines

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

The Philippines has expanded the procurement of commercial cloud services through the eMarketplace of the modernized Philippine Government Electronic Procurement System, operated by the Procurement Service of the Department of Budget and Management. PS-DBM formally onboarded several U.S. service suppliers into the eMarketplace in 2026.⁸⁹⁸ U.S. cloud providers seeking to serve government customers continue to face procurement and qualification requirements that warrant monitoring to ensure foreign suppliers receive nondiscriminatory access and that government agencies retain flexibility to select among secure and competitive cloud offerings.

On July 13, 2026, President Ferdinand Marcos Jr. issued Executive Order No. 119, establishing a new risk-based framework for the classification, residency, and cross-border transfer of government data.⁸⁹⁹ The final Order is substantially narrower than earlier proposals and expressly excludes private-sector and commercial data owned by private entities, while applying to government data processed or stored by private entities on behalf of covered government agencies. Under the Order's residency framework, Top Secret and Secret data must be stored within Philippine territory or other territories over which the Philippines exercises sovereignty or jurisdiction. Confidential data generally must be stored within those jurisdictions but may be stored or processed abroad with prior approval of the Joint Oversight Committee for Data Classification (JOC-DC) and subject to appropriate safeguards. Restricted data may be stored on secure cloud platforms subject to encryption, risk-mitigation, and other cybersecurity requirements, while all other government data, including Open Access data, may be stored on secure cloud platforms irrespective of physical location or ownership, subject to applicable safeguards. Covered agencies have a three-year phased compliance period, with compliance for Top Secret and Secret data required within the second year and compliance for all remaining government data within the third year. USTR should encourage the Philippines to preserve the Order's risk-based approach during implementation, prevent overclassification, and ensure that implementing rules do not expand localization requirements to commercial data or discriminate against foreign cloud providers.

⁸⁹⁸ Procurement Service–Department of Budget and Management. (2026, July 24). *PS-DBM expands green technology products with the inclusion of Google Cloud Computing Services in the eMarketplace*. <https://ps-philgeps.gov.ph/home/index.php/about-ps/news/8714-ps-dbm-expands-green-technology-products-with-the-inclusion-of-google-cloud-computing-services-in-the-emarketplace> ; and Procurement Service–Department of Budget and Management. (2026, September 2). *PS-DBM, Amazon Web Services hold alignment meeting on the onboarding of CCS into the eMarketplace*. <https://ps-philgeps.gov.ph/home/index.php/about-ps/news/8783-ps-dbm-amazon-web-services-hold-alignment-meeting-on-the-onboarding-of-ccs-into-the-emarketplace>

⁸⁹⁹ Republic of the Philippines. (2026, July 13). *Executive Order No. 119: Updating the Government Data Classification, Establishing a Data Residency Framework, and for Other Purposes*. https://lawphil.net/executive/execord/eo2026/eo_119_2026.html

Republic Act No. 12234, the Konektadong Pinoy Act, which took effect in August 2025, removed the longstanding requirement that data transmission services obtain a legislative franchise and replaced it with a streamlined registration framework.⁹⁰⁰ The reform represents a significant opening of the Philippine telecommunications market and has the potential to lower barriers to entry for U.S. technology and connectivity providers. Implementing rules were promulgated in November 2025.⁹⁰¹ Both the Act and its IRR nevertheless authorize DICT to formulate policies to safeguard local data when necessary for national security and the public interest, while expressly providing that primacy should be given to cross-border data flows as a key enabler of the global economy. USTR should encourage DICT to implement this authority narrowly, transparently, and on a risk-based basis, consistent with the law's cross-border data-flow principle, and avoid discriminatory localization or national-security requirements that could undermine the market-opening objectives of the Act.

Barriers to the Deployment and Operation of Network Infrastructure

The Philippines allocates and manages 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). These laws and directives provide the country's legal framework for spectrum enfranchisement, operation, and permitting in line with International Telecommunication Union requirements, and general provisions on the allocation and assignment of radio spectrum. While RA 7925 requires the conduct of open tenders in allocating spectrum, no public bidding has ever been carried out to allocate spectrum (e.g., spectrum auctions). Evaluation of applications typically involves submission by an applicant of a letter of request to the National Telecommunications Commission for its spectrum needs. This model is inherently non-transparent, constituting an administrative approach by which applicants are chosen based on the government's prioritization of certain criteria (like financial or technical capacity).

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Republic Act No. 11967, the Internet Transactions Act of 2023, was enacted on December 5, 2023, and its implementing rules were issued on May 24, 2024.⁹⁰² The framework imposes a range of obligations on e-marketplaces and other digital platforms, including requirements to collect identifying and contact information from online merchants, maintain and regularly update merchant information, establish consumer-redress mechanisms, and respond to government compliance and takedown orders. The law also provides for subsidiary platform liability under

⁹⁰⁰ Republic of the Philippines. (2025, August 24). *Republic Act No. 12234: Konektadong Pinoy Act*. <https://ldr.senate.gov.ph/legislative-issuance/republic-act-no-12234>

⁹⁰¹ Republic of the Philippines. (2025, November 5). *Implementing Rules and Regulations of the Konektadong Pinoy Act (Republic Act No. 12234)*. https://lawphil.net/statutes/repacts/ra2025/irr_12234_2025.html

⁹⁰² Department of Trade and Industry. (2024, May 24). *Implementing Rules and Regulations of Republic Act No. 11967 or the Internet Transactions Act of 2023*. <https://ecommerce.dti.gov.ph/wp-content/uploads/2024/06/Joint-Administrative-Order-No.-24-03.pdf>

specified circumstances. While intended to strengthen consumer protection in e-commerce, these requirements can create significant compliance burdens for digital platforms and raise concerns regarding proportionality, privacy, and intermediary liability. USTR should encourage Philippine authorities to implement the Act in a manner that is risk-based, protects consumer privacy, and avoids imposing disproportionate obligations on online intermediaries.

In September 2025, the Department of Trade and Industry (DTI) issued Department Administrative Order No. 25-12, which made E-Commerce Philippine Trustmark registration mandatory for online merchants, e-retailers, e-marketplaces, and digital platforms.⁹⁰³ DTI subsequently shifted implementation to a voluntary transition period and, in December 2025, extended voluntary registration through December 31, 2026.⁹⁰⁴ DTI's current Trustmark guidance states that application is voluntary. As of September 2026, the status of mandatory registration after December 31, 2026 remains unresolved. USTR should request clarity from the Government of Philippines on the mandatory requirements of the Administrative Order.

In June 2026, the House of Representatives approved House Bill No. 9465, the proposed Digital Media Anti-False Information Act, and transmitted the measure to the Senate.⁹⁰⁵ The House-passed bill would impose extensive obligations on digital platforms operating in the Philippines, including requirements relating to local legal presence, transparency reporting, sponsored content, notice-and-action mechanisms, user redress, advertising repositories, and recommender systems. Very large online platforms would be subject to additional systemic-risk and compliance requirements and could face administrative penalties of up to 6 percent of Philippine annual gross revenue for grave or repeated violations. The bill currently awaits action in the Senate.

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."⁹⁰⁶

In January 2024, the Bureau of Internal Revenue (BIR) issued Revenue Memorandum Circular No. 5-2024 and No. 38-2024 addressing the income-tax treatment of cross-border services, generating significant uncertainty regarding whether services performed by nonresident suppliers

⁹⁰³ Department of Trade and Industry. (2025, September 11). *DTI sets Sept. 30 deadline for mandatory Trustmark registration*. <https://www.dti.gov.ph/dti-latest-news/dti-sets-sept-30-deadline-mandatory-trustmark-registration>

⁹⁰⁴ Philippine News Agency. (2025, December 22). *DTI extends voluntary Trustmark registration until end-2026*. <https://www.pna.gov.ph/articles/1265667>

⁹⁰⁵ House of Representatives of the Philippines. (2026). *House Bill No. 9465: Digital Media Anti-False Information Act*. https://www.congress.gov.ph/legis/results?congress=20&oth_nos=HB09465&qrytype=N&signif=NL

⁹⁰⁶ United States Department of the Treasury. (1983). *Income Tax Convention with the Republic of the Philippines*. <https://www.irs.gov/pub/irs-trty/philip.pdf>

outside the Philippines could nevertheless be treated as Philippine-source income.⁹⁰⁷ In March 2026, BIR clarified through Revenue Memorandum Circular No. 24-2026⁹⁰⁸ that cross-border services are not automatically subject to Philippine income tax merely because they fall within an identified category of cross-border services. It reiterated the general rule that services are taxed where performed, while allowing consideration of where the economic benefit is received or the service is completed in circumstances consistent with the Philippine Supreme Court's *Aces Philippines* decision.⁹⁰⁹

The various RMCs continue to create significant confusion, tax uncertainty, and compliance costs for non-resident service providers and their local customers in the Philippines, because of conflicting broad language used that continue to suggest a generalized “benefits received” or “place of utilization/consumption” test as determinant of source of income in the Philippines. Doing so is inconsistent with both domestic tax law in the Philippines and established international tax principles, where the source of income is determined only based on activities the service provider actually performed to earn the income and where the actual performance of the service occurs, not where the benefits are received or where the place of utilization/consumption is. By its overarching interpretation of the *Aces Philippines* case in the various RMCs, the BIR is unduly asserting domestic source taxation on cross-border service arrangements, even though their facts and circumstances are different from the *Aces Philippines* case, and where the actual services and relevant economic activities are performed outside the Philippines. USTR should continue to discourage BIR’s over-assertion of domestic source taxing rights which create significant tax risks and uncertainty for US companies, and encourage predictable application of these rules consistent with the U.S.-Philippines tax treaty and established international taxation principles.

Other Barriers to Digital Trade

Republic Act No. 12009, the New Government Procurement Act, establishes explicit preferences for Philippine goods, services, and suppliers in government procurement.⁹¹⁰ The Act requires procuring entities to give priority and preference to Philippine products and services and provides that a domestic bidder shall receive the award where its bid does not exceed the lowest foreign bid by more than 25 percent. The implementing rules, which took effect in February 2025, also generally limit eligibility for the procurement of goods

⁹⁰⁷ Bureau of Internal Revenue. (2026, March 30). *Revenue Memorandum Circular No. 24-2026: Clarifying the Application of Revenue Memorandum Circular Nos. 5-2024 and 38-2024 on the Tax Treatment of Cross-Border Services*. <https://bir-cdn.bir.gov.ph/BIR/pdf/RMC%20No.%2024-2026.pdf>

⁹⁰⁸ Bureau of Internal Revenue. (2026, March 30). *Revenue Memorandum Circular No. 24-2026: Clarifying the Application of Revenue Memorandum Circular Nos. 5-2024 and 38-2024 on the Tax Treatment of Cross-Border Services*. <https://bir-cdn.bir.gov.ph/BIR/pdf/RMC%20No.%2024-2026.pdf>

⁹⁰⁹ Supreme Court of the Philippines. (2022, August 30). *Aces Philippines Cellular Satellite Corporation v. Commissioner of Internal Revenue*, G.R. No. 226680. <https://elibrary.judiciary.gov.ph/thebookshelf/showdocs/1/68589>

⁹¹⁰ Republic of the Philippines. (2024, July 20). *Republic Act No. 12009: New Government Procurement Act*. https://lawphil.net/statutes/repacts/ra2024/ra_12009_2024.html

to Filipino individuals and Philippine entities with at least 60 percent Filipino ownership. Foreign suppliers may participate under specified, limited circumstances.⁹¹¹ These requirements can significantly limit the ability of foreign suppliers, including U.S. technology and digital services providers, to compete directly for Philippine government contracts.

Poland

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Poland's amendment to the National Cybersecurity System Act entered into force on April 3, 2026.⁹¹² However, the President referred the amendment to the Constitutional Tribunal for subsequent review, citing concerns about disproportionate obligations on businesses. The law, which remains in effect pending review, authorizes the Minister of Digital Affairs to designate high-risk vendors and restrict specified ICT products, services, or processes. Covered entities must stop introducing designated products and services and withdraw existing ones within four to seven years. The risk assessment includes potential control by states outside the EU or NATO, alongside technical and security factors; non-EU status alone does not trigger designation. As of August 6, 2026, the Ministry reported that no designation proceedings or decisions had occurred.⁹¹³ The breadth of the minister's discretion and potential replacement obligations nevertheless create uncertainty and costs for suppliers and customers.

In June 2026, Poland announced plans for a technological-sovereignty test covering public technology purchases exceeding PLN 5 million and infrastructure investments exceeding PLN 15 million.⁹¹⁴ The review would assess supplier dependence and the state's control over systems and data. Implementation should use objective security and interoperability criteria; preferences based on supplier nationality or domestic ownership could restrict U.S. providers' access to public contracts.

⁹¹¹ Republic of the Philippines. (2025, February 10). *Implementing Rules and Regulations of Republic Act No. 12009 or the New Government Procurement Act*. https://lawphil.net/statutes/repacts/ra2025/irr_12009_2025.html

⁹¹² Ministerstwo Cyfryzacji. (2026, April 2). *Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa zaczyna obowiązywać*. <https://www.gov.pl/web/cyfryzacja/novelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-zaczyna-obowiazac>

⁹¹³ Ministerstwo Cyfryzacji. (2026, August 6). *Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) – procedura dot. listy dostawców wysokiego ryzyka*. <https://www.gov.pl/web/cyfryzacja/novelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc---procedura-dot-listy-dostawcow-wysokiego-ryzyka>; Rzeczpospolita Polska. (2026, January 23). *Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*. Dziennik Ustaw, 2026, poz. 252. <https://dziennikustaw.gov.pl/D2026000025201.pdf>

⁹¹⁴ Polska Agencja Prasowa. (2026, June 2). *Premier zapowiada „test suwerenności”. Rząd bierze pod lupę wielkie państwowe zakupy IT*. Bankier.pl. <https://www.bankier.pl/wiadomosc/Premier-zapowiada-test-suwerennosci-Rzad-bierze-pod-lupe-wielkie-panstwowe-zakupy-IT-9144904.html>

Taxation of Digital Products and Services

On July 31, 2026, Poland's Ministry of Digital Affairs published draft legislation (UD385) proposing a 3% tax on Polish revenues from targeted online advertising, multi-sided digital interfaces, and paid transfers of user data.⁹¹⁵ The proposal would apply to entities or consolidated groups exceeding both €1 billion in worldwide revenue and PLN 25 million in taxable Polish revenue in the preceding year, regardless of residence or headquarters. It entered a 60-day consultation, with proposed commencement on January 1, 2027.⁹¹⁶ The accompanying impact assessment projects PLN 1.716 billion (about \$450 million) in the first revenue-generating year and PLN 3.080 billion in the fourth.

The proposal excludes direct online sales through a supplier's own website and exempts entities predominantly engaged in publishing editorial material. It would reduce an entity's Polish corporate income tax liability, qualifying research and development costs, and specified capital expenditure incurred in Poland, which in theory could fully offset the tax. These features raise concerns that suppliers serving Poland across borders would face a greater effective burden than competitors with substantial Polish operations or investment. Taxpayers without an EU seat or fixed establishment would also have to appoint a tax representative, adding compliance costs for affected U.S. providers. CCIA urges USTR to engage with Poland to encourage it to abandon this discriminatory measure.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

On September 4, 2026, Parliament completed passage of legislation establishing Poland's national Digital Services Act enforcement framework and designating the President of the Office of Electronic Communications (UKE) as Digital Services Coordinator.⁹¹⁷ The legislation now awaits presidential signature. Separately, the Ministry of Digital Affairs has drafted a bill that would establish procedures for orders blocking illegal content and restoring access to content unjustifiably removed by service providers.⁹¹⁸ These proposed powers could affect providers' content-moderation decisions; their implementation should be monitored to ensure that they preserve effective judicial review.

⁹¹⁵ Ministerstwo Cyfryzacji. (2026, July 31). *Projekt ustawy o podatku rekompensującym od niektórych usług (UD385)*.

<https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-podatku-rekompensujacym-od-niektorych-uslug-ud385>

⁹¹⁶ Ministerstwo Cyfryzacji. (2026, July 31). *Projekt ustawy o podatku rekompensującym od niektórych usług (UD385)* [Draft legislation and public consultation materials].

<https://www.gov.pl/web/cyfryzacja/projekt-ustawy-o-podatku-rekompensujacym-od-niektorych-uslug-ud385>

⁹¹⁷ Urząd Komunikacji Elektronicznej. (2026, September 4). *Sejm uchwalił ustawę wdrażającą przepisy Aktu o usługach cyfrowych. Prezes UKE Koordynatorem ds. usług cyfrowych*.

<https://www.uke.gov.pl/uslugi-cyfrowe/aktualnosci/sejm-uchwalil-ustawe-wdrazajaca-przepisy-aktu-o-uslugach-cyfrowych-prezes-uke-koordynatorem-ds-uslug-cyfrowych.26.html>

⁹¹⁸ Polskie Radio (28 January 2026)

<https://www.polskieradio.pl/395/7789/artykul/3639997.poland-drafts-new-bill-to-block-illegal-online-content-after-presidential-veto> .

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, subject to extensive government control, has accelerated, as has its removal from the global financial and business system. For example, Yandex sold its news feed and homepage to state-controlled VK, expanding state-linked ownership of major online information services.⁹¹⁹

Asymmetric Platform Regulations

Federal Law No. 194-FZ, signed July 7, 2025 and effective September 1, 2025, prohibits restrictions on installing applications through Russia's designated unified app store, RuStore, and on those applications' functionality and payment methods on covered devices.⁹²⁰ These requirements privilege a domestic distribution channel and constrain foreign providers' control over their platforms.

Federal Law No. 289-FZ of July 31, 2025 and Government Resolution No. 54 of January 28, 2026 establish a regulatory framework for intermediary digital platforms effective October 1, 2026.⁹²¹ Foreign-operated platforms meeting the functional criteria are covered based on an average of at least 100,000 daily users in Russia over the preceding calendar year.

Russian-operated platforms must additionally meet either a 10,000-transacting-seller threshold or ₺50 billion in annual transaction value. These different thresholds subject foreign platforms to a discriminatory burden. Noncompliant foreign operators may face payment, advertising and access restrictions.

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 communications and services, imposing significant obligations on services to comply with government demands. Over the past several years, Russia's telecommunications regulator,

⁹¹⁹ Trevelyan, M., & Rodionov, M. (2024, May 17). *Yandex parent company says first phase of Russia divestment deal is complete*. Reuters.

<https://www.reuters.com/business/yandex-nv-says-first-phase-russia-divestment-deal-is-complete-2024-05-17/>

⁹²⁰ Russian Federation. (2025, July 7). *Federal Law No. 194-FZ on amendments to the Law of the Russian Federation "On Protection of Consumer Rights."* https://www.consultant.ru/document/cons_doc_LAW_509282/

⁹²¹ Government of the Russian Federation. (2026, January 28). *Resolution No. 54 on approving additional criteria for classifying digital platforms as intermediary digital platforms.* https://www.consultant.ru/document/cons_doc_LAW_525381/

Roskomnadzor, has veered away from its primary mandate, instead becoming a quasi-intelligence agency, orchestrating the Kremlin's censorship and surveillance activities.⁹²²

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 Information⁹²³ and the Federal Law on Amending the Code of Administrative Violations,⁹²⁴ 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.⁹²⁵

Government Resolution No. 1667, effective March 1, 2026, updated the rules for centralized management of public communications networks, including binding instructions to operators to address designated threats.⁹²⁶ Federal Law No. 33-FZ of February 20, 2026 additionally requires operators to suspend communications services at the FSB's request in circumstances established by presidential acts and exempts operators from contractual liability for those suspensions.⁹²⁷ On September 5, 2025, the Digital Development Ministry published a greenlist of services intended to remain accessible during mobile-internet restrictions.⁹²⁸ It included domestic services such as MAX and Russian marketplaces while excluding WhatsApp and YouTube, giving selected domestic providers an availability advantage during shutdowns.

⁹²² 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>

⁹²³ Russian Federation. (2019). *Federal Law No. 31-FZ on amendments to Article 15-3 of the Federal Law on Information, Information Technologies and Information Protection*. <http://publication.pravo.gov.ru/Document/View/0001201903180031>

⁹²⁴ Russian Federation. (2019). *Federal Law No. 27-FZ on amendments to the Code of the Russian Federation on Administrative Offenses*. <http://publication.pravo.gov.ru/Document/View/0001201903180021>

⁹²⁵ 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-disconnect-the-country-from-the-world-wide-web/>

⁹²⁶ Government of the Russian Federation. (2025, October 27). *Resolution No. 1667 on approving the rules for centralized management of the public communications network*. https://www.consultant.ru/document/cons_doc_LAW_518235/

⁹²⁷ Russian Federation. (2026, February 20). *Federal Law No. 33-FZ on amendments to Articles 46 and 68 of the Federal Law "On Communications"*. https://www.consultant.ru/document/cons_doc_LAW_527050/

⁹²⁸ Reuters. (2025, September 5). *Russia lists local apps that will survive its internet blackouts*. <https://www.reuters.com/technology/russia-lists-local-apps-that-will-survive-its-internet-blackouts-2025-09-05/>

In December 2019, Russia adopted a law requiring the pre-installation of Russian software on certain consumer electronic products sold in Russia.⁹²⁹ The law took effect in early 2021.⁹³⁰ The requirements cover designated categories of smartphones, computers, tablets and smart TVs. From September 1, 2025, the state-backed MAX messenger became mandatory for pre-installation on smartphones and tablets sold in Russia.⁹³¹

In 2021, Federal laws N482-FZ and N511-FZ came into effect.⁹³² 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 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.⁹³³

Russia restricts tools used to circumvent online censorship. In February 2026, Roskomnadzor reported blocking 469 VPN services.⁹³⁴ Since September 2025, individuals have faced fines of ₺3,000–5,000 for intentionally searching for and accessing material known to be extremist, including through VPNs.⁹³⁵ The offense covers both material on the federal extremist-materials list and material falling within the statutory definition in Law No. 114-FZ.

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

⁹²⁹ 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-laptop>

⁹³⁰ Reuters. (2021, April 1). *Russian law requires smart devices to come pre-installed with domestic software*.
<https://www.reuters.com/article/technology/russian-law-requires-smart-devices-to-come-pre-installed-with-domestic-software-idUSKBN2BO4P2/>

⁹³¹ Osborn, A. (2025, August 21). *Russia orders state-backed MAX messenger app, a WhatsApp rival, pre-installed on phones and tablets*. Reuters.
<https://www.reuters.com/technology/russia-orders-state-backed-max-messenger-app-whatsapp-rival-pre-installed-phones-2025-08-21>

⁹³² Rakhmetov, B. (2021, February 22). *The Putin Regime Will Never Tire of Imposing Internet Control: Developments 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>

⁹³³ 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/Radio 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>

⁹³⁴ Human Rights Watch. (2026, March 12). *Russia: Digital Iron Curtain Falls on Internet Freedom Protection Day*.
<https://www.hrw.org/news/2026/03/12/russia-digital-iron-curtain-falls-on-internet-freedom-protection-day>

⁹³⁵ Russian Federation. (2025, July 31). *Federal Law No. 281-FZ on amendments to the Code of Administrative Offenses and the Federal Law "On Amendments to the Code of Administrative Offenses."*
https://www.consultant.ru/document/cons_doc_LAW_511068/

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.”⁹³⁶ 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.⁹³⁷

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. 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.⁹³⁸

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.⁹³⁹ Russia blocked Facebook, X and Instagram in 2022,⁹⁴⁰ began throttling YouTube and blocked Signal in 2024,⁹⁴¹ and restricted WhatsApp and Telegram voice calls in August 2025.⁹⁴² In February 2026, the Kremlin confirmed the blocking of

⁹³⁶ Izadi, E., & Ellison, S. (2022, March 5). *Russia’s independent media, long under siege, teeters under new Putin crackdown*. The Washington Post.

<https://www.washingtonpost.com/media/2022/03/04/putin-media-law-russia-news/>

⁹³⁷ TASS. (2023, August 7). *Google fined 3 million rubles for failing to remove prohibited content and fakes about SVO*. <https://tass.ru/ekonomika/18528253>

⁹³⁸ 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/cdxvwnkl5kgo>

⁹³⁹ 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>

⁹⁴⁰ Freedom House. (2022). *Russia: Freedom on the Net 2022*. <https://freedomhouse.org/country/russia/freedom-net/2022>

⁹⁴¹ Freedom House. (2025). *Russia: Freedom on the Net 2025*. <https://freedomhouse.org/country/russia/freedom-net/2025>

⁹⁴² Litvinova, D. (2025, August 13). *Russia restricts calls via WhatsApp and Telegram, the latest step to control the internet*. Associated Press. <https://apnews.com/article/russia-internet-messenger-whatsapp-telegram-crackdown-2a89703deb1094af1b0206161efe2050>

WhatsApp,⁹⁴³ while Roskomnadzor announced further restrictions on Telegram.⁹⁴⁴ Also in February 2026, internet-censorship researchers reported that YouTube's domain had disappeared from Russia's national domain-name system, preventing users relying on that system from resolving the site.⁹⁴⁵

Law No. 406-FZ of July 31, 2023 introduced prescribed authentication methods for resources owned by Russian legal entities or citizens where access requires user authentication.⁹⁴⁶ Permitted methods include a mobile telephone number, state identification systems, or qualifying Russian-owned authentication systems. From July 7, 2026, companies face fines of ₺500,000–700,000 for failing to meet the prescribed authentication requirements. Hosting providers must notify Roskomnadzor, be included in its hosting-provider register, and identify or authenticate customers before providing services. Federal Law No. 210-FZ of June 26, 2026 additionally prohibits providing hosting to covered VPN and other circumvention services that fail to comply with statutory requirements to prevent access to blocked resources.⁹⁴⁷

Federal Law No. 42-FZ, signed March 11, 2024 and effective March 22, 2024, amended the 2022 foreign-agent law and advertising legislation to prohibit advertising on foreign agents' information resources and advertising those resources.⁹⁴⁸ In August 2024, Google began shutting down payments to Russian-based websites and content owners monetizing advertisements placed by Google.⁹⁴⁹ Federal Law No. 72-FZ, signed April 7, 2025 and effective September 1, 2025, prohibits advertising on blocked information resources and resources associated with organizations designated undesirable or prohibited for extremist or terrorist activity.⁹⁵⁰ The prohibition restricts monetization of affected foreign platforms, including platforms that Russian users continue to access through circumvention tools.

⁹⁴³ Shamlii, A. (2026, February 12). *Russia blocks WhatsApp as it pushes state-backed alternative on citizens*. CBS News. <https://www.cbsnews.com/news/russia-blocks-whatsapp-as-it-pushes-state-backed-alternative-on-citizens/>

⁹⁴⁴ Osborn, A., & Dey, M. (2026, February 12). *Russia fully blocks WhatsApp, talks up state-backed alternative*. Reuters.

<https://www.reuters.com/technology/russia-blocks-metas-whatsapp-messaging-service-ft-reports-2026-02-12/>

⁹⁴⁵ Human Rights Watch. (2026, March 12). *Russia: Digital Iron Curtain Falls on Internet Freedom Protection Day*.

<https://www.hrw.org/news/2026/03/12/russia-digital-iron-curtain-falls-on-internet-freedom-protection-day>

⁹⁴⁶ 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>

⁹⁴⁷ Russian Federation. (2026, June 26). *Federal Law No. 210-FZ on amendments to the Federal Law "On Communications" and certain legislative acts of the Russian Federation*, Article 5.

https://www.consultant.ru/document/cons_doc_LAW_537891/5bdc78bf7e3015a0ea0c0ea5bef708a6c79e2f0a/

⁹⁴⁸ Russian Federation. (2024). *Federal Law No. 42-FZ on amendments 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*. <http://publication.pravo.gov.ru/document/0001202403110004>

⁹⁴⁹ 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/>

⁹⁵⁰ Russian Federation. (2025, April 7). *Federal Law No. 72-FZ on amendments to Article 12 of the Federal Law "On Countering Extremist Activity" and the Federal Law "On Advertising"*.

https://www.consultant.ru/document/cons_doc_LAW_502592/

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.⁹⁵¹ In July 2022, Russian-backed separatists blocked Google due to the purported spread of "disinformation" in a breakaway region of eastern Ukraine.⁹⁵² Regional internet outages have occurred throughout Ukraine since Russia began its war campaign in the country,⁹⁵³ with some areas experiencing blackouts for multiple days—in some cases due to reported Russian cyberattacks.⁹⁵⁴ 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.

Challenges to the Development of Artificial Intelligence

Federal Law No. 243-FZ of July 26, 2026 establishes support for 'sovereign' and 'national' foundation AI models.⁹⁵⁵ Provisions effective March 1, 2027 will permit the government to reserve specified uses for these models and establish qualification requirements, including Russian-controlled developers and response processing and data storage in Russian-owned data centers in Russia. Qualifying existing systems have until September 1, 2032 to implement these requirements. From March 1, 2027, Article 10(2) will also provide a copyright and related-rights exception for temporary copying into computer memory exclusively to train qualifying 'sovereign' or 'national' models, subject to lawful-access conditions. This gives qualifying Russian-controlled developers a legal advantage unavailable to other developers.

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

⁹⁵¹ Burgess, M. (2022, June 15). *Russia Is Taking Over Ukraine's Internet*. WIRED. <https://www.wired.com/story/ukraine-russia-internet-takeover/>

⁹⁵² Reuters. (2022, July 22). *Russian-backed separatists in Ukraine block Google search engine*. <https://www.reuters.com/world/europe/russian-backed-separatists-ukraine-block-google-search-engine-2022-07-22/>

⁹⁵³ 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-cna18973>

⁹⁵⁴ FitzGerald, D. (2022, May 1). *Occupied regions of southern Ukraine lose internet services*. The Wall Street Journal. <https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-04-30/card/occupied-regions-of-southern-ukraine-lose-internet-service-YrGVuhNABlkQzxc099dM>

⁹⁵⁵ Russian Federation. (2026, July 26). *Federal Law No. 243-FZ on supporting the development of artificial intelligence technologies in the Russian Federation*, Article 6. <https://gb-dnr.ru/normative-base/detail/2942>

its activities.⁹⁵⁶ 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.

Since January 1, 2022, covered foreign internet companies have been required under Law No. 236-FZ to establish a Russian legal entity, branch or representative office. 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.

Federal Law No. 259-FZ of July 14, 2022 introduced corporate fines for specified landing-law violations, including failure to establish the required local presence, of up to 10% of the relevant annual revenue, subject to a ₺6 million minimum.⁹⁵⁷ Repeat violations carry fines of up to 20%, subject to a ₺10 million minimum. These local-presence requirements expose company representatives to pressure to remove content and disclose users' personal data.

Federal Law No. 23-FZ, effective July 1, 2025, prohibits using foreign databases for specified operations when collecting Russian citizens' personal data, subject to statutory exceptions.⁹⁵⁸ The Digital Development Ministry clarified that subsequent cross-border transfers remain possible following compliant domestic collection and subject to the separate transfer requirements. From January 1, 2026, internet-based information service suppliers must retain specified user information and records of registration, authentication and other actions in Russia for three years, increased from one year.

Since March 1, 2023, personal-data operators have been required to assess foreign recipients' safeguards and notify Roskomnadzor before commencing cross-border transfers.⁹⁵⁹ Federal Law No. 265-FZ, effective July 26, 2026, removed the preferential treatment previously available to

⁹⁵⁶ 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>

⁹⁵⁷ Russian Federation. (2022, July 14). *Code of Administrative Offenses, Article 13.49(2), introduced by Federal Law No. 259-FZ*.

https://www.consultant.ru/document/cons_doc_LAW_34661/01319a1b75191753b6d53b65b1bdac98e52f9921/

⁹⁵⁸ Russian Federation. (2025, February 28). *Federal Law No. 23-FZ on amendments to the Federal Law "On Personal Data" and certain legislative acts of the Russian Federation*.

https://www.consultant.ru/document/cons_doc_LAW_499984/

⁹⁵⁹ 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-rule-s-on-cross-border-data-transfers>

destination countries party to Convention 108.⁹⁶⁰ Transfers to countries on Roskomnadzor’s adequacy list may begin after notification; transfers to other countries generally must await expiry of the regulator’s review period. Roskomnadzor retains authority to prohibit or restrict transfers on statutory grounds.

Bill No. 502113-8 became Federal Law No. 421-FZ on November 30, 2024, effective December 11, 2024.⁹⁶¹ It introduced Criminal Code Article 272.1 concerning unlawful handling of unlawfully obtained computer information containing personal data. Where the offense involves cross-border transfer, penalties can include imprisonment for up to eight years and a fine of up to ₺2 million.

Taxation of Digital Products and Services

Since April 1, 2025, Russia has imposed a 3% levy on covered quarterly revenue from distributing online advertising directed at users in Russia.⁹⁶² Russian advertisers contracting with foreign providers must calculate and withhold the levy from their payments. Proceeds support registered Russian software and designated information resources, imposing additional costs on digital advertising while financing domestic providers.

Rwanda

Taxation of Digital Products and Services

Law No. 014/2025 of May 27, 2025, published on May 29, 2025, introduced a 1.5% digital services tax on Rwanda-sourced gross revenues of companies supplying digital services with a substantial national presence.⁹⁶³ The law delegates the definition of substantial national presence, taxable services, registration, declaration, and payment requirements to a Ministerial Order.

⁹⁶⁰ Russian Federation. (2026, July 26). *Federal Law No. 265-FZ on amendments to Article 12 of the Federal Law “On Personal Data” and certain legislative acts of the Russian Federation*, Articles 1 and 7. https://www.consultant.ru/document/cons_doc_LAW_540340/

⁹⁶¹ Digital Policy Alert. (2024, December 11). *Russia: Implemented Law amending Criminal Code establishing liability for illegal use and transfer, collection and storage of computer information containing personal data* (Federal Law No. 421-FZ). <https://digitalpolicyalert.org/event/25027-implemented-law-amending-criminal-code-establishing-liability-for-illegal-use-and-transfer-collection-and-storage-of-computer-information-containing-personal-data-federal-law-no-421-fz>

⁹⁶² Russian Federation. (2024, December 26). *Federal Law No. 479-FZ on amendments to the Federal Law “On Advertising” and certain legislative acts of the Russian Federation*, Articles 1(4) and 4. https://www.consultant.ru/document/cons_doc_LAW_494360/

⁹⁶³ Republic of Rwanda. (2025, May 27). *Law No. 014/2025 amending Law No. 027/2022 of 20/10/2022 establishing taxes on income*. https://www.rra.gov.rw/fileadmin/user_upload/Law_amending_the_2022_Income_Tax_May_2025.pdf

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.⁹⁶⁴ The draft regulations contained broad platform-designation criteria, which lacked safeguards against arbitrary designation and a requirement for clear evidence of 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.⁹⁶⁵ 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

Saudi Arabia’s 2019 Regulations on the Use of Information and Communication Technologies in Government Entities require government entities, state-owned enterprises and operators of Critical National Infrastructure (CNI) to host their data inside the Kingdom. This covers many sectors, from financial services and aviation to oil and gas. Sector regulators can also add their own localization rules on top of this. In 2024, the National Cybersecurity Authority (NCA) issued updated Essential Cybersecurity Controls (ECC-2:2024) and Cloud Cybersecurity Controls (CCC-2:2024). The updates removed explicit requirements for cloud providers to deliver storage, processing, disaster recovery, monitoring and support from within the Kingdom. However, this did not loosen localization requirements. Instead, the NCA moved responsibility for data localization to the National Data Management Office (NDMO). Entities must now consult the NDMO before making any decision on where data is hosted. Without clear NDMO rules, U.S. cloud providers and their customers have no dependable way to know which workloads can be served from outside Saudi Arabia.

⁹⁶⁴ Communications and Information Technology Commission. (2022). *Competition Regulations for Digital Content Platforms*.
<https://istitlaa.ncc.gov.sa/en/transportation/citc/crdcp/Documents/Competition%20Regulations%20for%20Digital%20Content%20Platforms.pdf>

⁹⁶⁵ CCIA. (2022, November 30). *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/>

Since 2024, SDAIA has issued numerous rules and consultations affecting data governance and digital services. Rules governing the National Register of Controllers within the Kingdom require registration by public entities, controllers whose main activity involves personal-data processing, controllers processing sensitive data, and individuals processing personal data beyond personal or family use. The rules expressly contemplate separate registration rules for controllers outside the Kingdom. Second, the Data Sovereignty Public Policy consultation outlines four key principles guiding Saudi Arabia's data sovereignty approach.⁹⁶⁶ Third, SDAIA finalized the General Rules for Secondary Use of Data in December 2025.⁹⁶⁷ They govern specified government-related data sharing for public-interest and research purposes, exclude profit-oriented purposes, and require usage licenses for private entities accessing government data. Separately, the June 2026 Data Monetization Policy permits commercialization through government-data products and services, subject to licensing, registration, purpose restrictions, and limits on onward sharing.⁹⁶⁸ Industry seeks clarity on the interaction between these frameworks and predictable access terms for commercial research and innovation. Finally, SDAIA's 2025 consultation proposed controls covering data-protection consultancy, training, and technical solutions.⁹⁶⁹ In February 2026, SDAIA issued separate rules governing accreditation certificates for controllers and processors and licensing of certification, audit, and inspection activities.⁹⁷⁰ July 2026 consultations proposed implementing standards for these activities.⁹⁷¹ Industry seeks clear boundaries between regulated certification and audit services and ordinary advisory or technical services, alongside proportionate licensing requirements.

Restrictions on Cross Border Data Flows

Saudi Arabia's Personal Data Protection Law (PDPL) allows companies to transfer personal data out of the Kingdom if they use one of three approved safeguards: standard contractual clauses (SCCs), binding common rules for transfers within a corporate group, or a certificate of accreditation. SDAIA set these safeguards out in its September 2024

⁹⁶⁶ Saudi Data and Artificial Intelligence Authority. (2024). *Data Sovereignty Draft Public Policy*.

<https://istitlaa.ncc.gov.sa/en/Transportation/NDMO/DataSovereigntyPolicy/Pages/default.aspx>

⁹⁶⁷ Saudi Press Agency. (2025, December 31). *SDAIA Issues General Rules for the Secondary Use of Data Document*. <https://www.spa.gov.sa/N2478848>

⁹⁶⁸ Baqadir, S. (2026, September 1). *Saudi Arabia's New Data Monetization Policy: What Private Entities Need to Know*. Al Tamimi & Company. https://www.tamimi.com/law_update_articles/saudi-arabias-new-data-monetization-policy-what-private-entities-need-to-know

⁹⁶⁹ Al Tamimi & Company. (2025, April 28). *SDAIA's New Draft Controls Shaping the Future of Data Protection*. <https://www.tamimi.com/news/sdaias-new-draft-controls-shaping-the-future-of-data-protection/>

⁹⁷⁰ Saudi Press Agency. (2026, February 17). *SDAIA Issues Rules Governing Personal Data Protection Licensing, Accreditation*. <https://spa.gov.sa/en/N2517131>

⁹⁷¹ DGA Group. (2026, July). *Saudi Arabia's New Digital Economy: The Kingdom Makes Strides in Data Monetization, Cybersecurity, and AI Policy*. <https://dgagroup.com/wp-content/uploads/2026/07/Saudi-Arabias-New-Digital-Economy-The-Kingdom-Makes-Strides-in-Data-Monetization-Cybersecurity-and-AI-Policy-3.pdf>

Regulation on Personal Data Transfer Outside the Kingdom. While this is an improvement on the original law, which required prior SDAIA approval for most transfers, there is an outstanding concern relating to the terms of the SCCs. Companies cannot change them, and any change makes them invalid. They also require the company receiving the data outside Saudi Arabia to comply with and enforce binding decisions made under Saudi law. As a result, a U.S. parent company that receives data from its Saudi subsidiary becomes directly subject to Saudi regulatory decisions. Companies must also carry out a risk assessment before each regular or large-scale transfer of sensitive data. Together, these requirements raise compliance costs for routine data flows within a company.

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.⁹⁷² In 2026, X geoblocked more than 60 dissident accounts in Saudi Arabia following government demands;⁹⁷³ similarly, Meta restricted access within Saudi Arabia to dissidents' Facebook and Instagram accounts following government orders.⁹⁷⁴

CST's Regulations for Providing Digital Content Platform Services⁹⁷⁵ already impose licensing, registration, or notification requirements on covered domestic and foreign providers. Social-media and video-sharing platforms with at least 100,000 Saudi users must notify CST and appoint a platform liaison officer. These obligations are separate from the proposed Media Law.

On November 5, 2023, the General Authority of Media Regulation opened a consultation on a draft Media Law.⁹⁷⁶ 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.⁹⁷⁷ 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

⁹⁷² Freedom House. (2024). *Saudi Arabia: Freedom on the Net 2024 Country Report*.

<https://freedomhouse.org/country/saudi-arabia/freedom-net/2024>

⁹⁷³ Abdul, G. (2026, August 4). *Elon Musk's X latest to block Saudi dissident accounts inside kingdom*. The Guardian. <https://www.theguardian.com/technology/2026/aug/04/x-twitter-blocks-dissident-accounts-saudi-arabia>

⁹⁷⁴ Kirchgaessner, S., & Abdul, G. (2026, May 22). *Meta and Snapchat blocking Saudi dissidents' accounts*. The Guardian. <https://www.theguardian.com/media/2026/may/22/instagram-x-social-media-platforms-blocking-saudi-dissidents-accounts>

⁹⁷⁵ Communications, Space and Technology Commission. (2023, October 8). *Regulations for Providing Digital Content Platform Services* (Decision No. 505/1445).

<https://www.cst.gov.sa/en/regulations-and-licenses/regulations/Document-1549>

⁹⁷⁶ Digital Policy Alert. (2023, November 5). *Saudi Arabia: Opened consultation on Saudi Arabia Media Law including licensing requirements*. <https://digitalpolicyalert.org/event/21143-introduced-saudi-arabian-media-law>

⁹⁷⁷ Zaghdoudi, A. (2024, February 29). *In Saudi Arabia, no safe harbor for free speech*. Access Now. <https://www.accessnow.org/saudiarabiasafeharbor/>

exempting platforms from intermediary liability, which is of concern, given the Kingdom's focus on digital content moderation.

Saudi Arabia's new Copyright Law took effect on August 12, 2026.⁹⁷⁸ Article 49 establishes a conditional safe harbor for internet content providers covering users' copyright infringements. The Implementing Regulations, published July 31, 2026, dictate removal or disabling of access within 48 working hours after knowledge of infringement or receipt of a complete rights-holder notice, whichever occurs first.⁹⁷⁹ Additional conditions include qualifying technical or user-requested activity without content modification, absence of knowledge or obvious indications of infringement, a reporting mechanism, no direct financial benefit from infringement, a written policy for restricting or terminating infringing users' accounts, and compliance with SAIP requirements. Users may submit counter-notices, which providers must communicate to the original notifier within two business days. This protection is specific to copyright and does not resolve broader intermediary-liability concerns.

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.⁹⁸⁰ Enforcement is already active under existing media legislation. In May 2026, GMedia reported summoning 49 people over 68 alleged social-media violations involving public-order, national-security, and public-interest provisions.⁹⁸¹

SDAIA's updated Deepfakes Guidelines, dated May 2025, address consent, privacy, disclosure of synthetic content, and safeguards against harmful uses.⁹⁸² They encourage measures including watermarking and source verification. USTR should seek clarity on how these expectations interact with binding Saudi laws and platforms' responsibilities for user-generated content.

Saudi Arabia's 2022 Telecommunications and Information Technology Law already provides for internet filtering and prohibits bypassing filtering or facilitating circumvention.⁹⁸³ Violations can

⁹⁷⁸ Chakra, B. A., Batarfi, S., Alghamdi, M., & Al-Harbi, R. A. (2026, August 27). *Saudi Arabia copyright law implementing regulations: key clarifications and remaining questions*. Gowling WLG.

<https://gowlingwlg.com/en/insights-resources/articles/2026/saudi-arabia-copyright-law-implementing-regulations>

⁹⁷⁹ Saudi Authority for Intellectual Property. (2026, July 31). اللائحة التنفيذية لنظام حقوق المؤلف [Implementing Regulations of the Copyright Law], Articles 83–85. Umm Al-Qura. <https://www.uqn.gov.sa/decisions-and-regulations/4001498>

⁹⁸⁰ Hassan, S. (2025, September 25). *Saudi Arabia issues major update to social media rules for businesses*. Caterer Middle East.

<https://www.caterermiddleeast.com/saudi-arabia/saudi-arabia-issues-major-update-to-social-media-rules-for-businesses>

⁹⁸¹ Al Omran, A. (2026, May 15). *Saudi Arabia curbs complaints about jobs for foreigners*. Financial Times.

<https://www.ft.com/content/0fe4a1e7-cba8-4740-9891-523f34ad6392>

⁹⁸² Saudi Data and Artificial Intelligence Authority. (2025, May). *Deepfakes Guidelines: Mitigating Risks While Fostering Innovation* (SDAIA-P119). <https://sdaia.gov.sa/en/SDAIA/about/Files/File0001.pdf>

⁹⁸³ O'Connell, N. (2023, May). *An overview of Saudi Arabia's new Telecommunications & Information Technology Law – Part II*. Al Tamimi & Company.

<https://turtl.tamimi.com/story/an-overview-of-saudi-arabias-new-telecommunications-and-information-technology-law-part-ii/page/1>

result in fines of up to SAR 25 million and other sanctions. A consultation opened on July 8, 2024 proposed amendments affecting CST's powers, including removal of its express power to block digital content platforms and provisions for third-party verification of providers' compliance.⁹⁸⁴ USTR should seek clarity on the amendments' status and on the scope of existing obligations applicable to digital platforms.

In March 2025, the Saudi Central Bank prohibited local banks from using instant-messaging applications such as WhatsApp for customer communications, citing security concerns.⁹⁸⁵ Banks were urged to use alternatives such as in-app live chat or chatbots. The restriction limits global messaging providers' access to bank customer-service business.

Challenges to the Development of AI

Saudi Arabia's AI framework continues to evolve. SDAIA's April 2026 draft Responsible AI Policy proposes risk classification, registration, ethics labeling, and audit mechanisms. Its subsequent draft AI-First Policy addresses government adoption.⁹⁸⁶ In July 2026, SDAIA announced a non-binding National AI Risk Management Framework, while NCA consulted on AI Cybersecurity Guidelines covering generative and agentic AI, including third-party risks.⁹⁸⁷ Industry seeks coordinated, proportionate requirements, clear allocation of responsibilities, and interoperability with international frameworks. Separately, CST published its draft Global AI Hub Law for consultation on April 14, 2025.⁹⁸⁸ The draft establishes private, extended, and virtual hubs for hosting foreign government and commercial data under differentiated jurisdictional arrangements. It includes foreign-law and court-jurisdiction provisions and permits Saudi intervention or termination in specified circumstances. USTR should encourage Saudi Arabia to provide clearer operational safeguards, predictable approval terms, and guidance on resolving conflicting legal obligations and protecting service continuity. In addition, USTR should encourage Saudi Arabia to provide 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.

⁹⁸⁴ Giardini, T., Issa, J., & Deeg, N. (2024, December 18). *DPA Digital Digest: Saudi Arabia [2024 Edition]*. Digital Policy Alert. <https://digitalpolicyalert.org/digest/dpa-digital-digest-saudi-arabia>

⁹⁸⁵ Al Amir, K. (2025, March 3). *Saudi banks banned from using WhatsApp for customer service*. Gulf News. <https://gulfnews.com/world/gulf/saudi/saudi-banks-banned-from-using-whatsapp-for-customer-service-1.500051010>

⁹⁸⁶ Ramadan, D., & Stansfield, C. (2026, April 29). *Saudi Arabia moves to operationalise responsible AI governance*. Access Partnership. <https://accesspartnership.com/opinion/saudi-arabia-moves-to-operationalise-responsible-ai-governance/>

⁹⁸⁷ DGA Group. (2026, July). *Saudi Arabia's New Digital Economy: The Kingdom Makes Strides in Data Monetization, Cybersecurity, and AI Policy*. <https://dgagroup.com/wp-content/uploads/2026/07/Saudi-Arabias-New-Digital-Economy-The-Kingdom-Makes-Strides-in-Data-Monetization-Cybersecurity-and-AI-Policy-3.pdf>

⁹⁸⁸ 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>

The Copyright Law effective August 12, 2026 also introduces an TDM exception permitting copying for development of AI products and algorithms without author authorization or compensation.⁹⁸⁹ Article 26(4) requires lawful publication, lawful acquisition of ownership of the original copy, and copying limited to the intended purpose. Article 30 of the Implementing Regulations, published July 31, 2026, adds recordkeeping requirements and restrictions on commercial use.⁹⁹⁰ Use in a purely commercial context is permitted only if it is non-substantial relative to the work or does not affect its normal exploitation. Developers must retain records identifying the type, source, purpose, and date of use and provide them to competent authorities considering related disputes upon request. Industry seeks clarification of these commercial-use restrictions, required recordkeeping detail, and limits on incorporating protected works into final products.

Restrictions on Cross-Border Data Flows

Saudi Arabia's Personal Data Protection Law, issued in September 2021 and amended in March 2023, entered into force on September 14, 2023; the general compliance grace period ended on September 14, 2024.⁹⁹¹ Administrative fines can reach SAR 5 million, with higher penalties for repeat violations. Cross-border transfers are governed by Article 29 and the Regulation on Personal Data Transfer Outside the Kingdom, including adequacy-based transfers, appropriate safeguards such as standard contractual clauses and binding common rules, and specified exceptions. Applicable national-security, protection, and risk-assessment requirements remain relevant to international cloud operations. Industry seeks clear, workable transfer mechanisms and publication of SDAIA's adequacy determinations.

In February 2025, SDAIA published its Risk Assessment Guideline for Transferring Personal Data Outside the Kingdom.⁹⁹² The non-binding guideline explains how to assess processing risks, overseas recipients, safeguards, onward transfers, and potential effects on the Kingdom's vital interests. It supports implementation of the Transfer Regulation's binding risk-assessment requirements, including for safeguard-based transfers and continuous or large-scale transfers of sensitive personal data.

⁹⁸⁹ Saudi Arabia. (2026). نظام حقوق المؤلف [Copyright Law] (Royal Decree No. M/169), Articles 26(4) and 61. Nezams. <https://nezams.com/نظام-حقوق-المؤلف/>

⁹⁹⁰ Saudi Authority for Intellectual Property. (2026, July 31). اللائحة التنفيذية لنظام حقوق المؤلف [Implementing Regulations of the Copyright Law], Article 30. Umm Al-Qura. <https://www.uqn.gov.sa/decisions-and-regulations/4001498>

⁹⁹¹ DLA Piper. (2026, February 11). Data protection laws in Saudi Arabia. <https://www.dlapiperdataprotection.com/?c=SA>

⁹⁹² Saudi Data and Artificial Intelligence Authority. (2025, February). Risk Assessment Guideline for Transferring Personal Data Outside the Kingdom. <https://dgp.sdaia.gov.sa/wps/wcm/connect/16aec46f-ea3d-47f6-8e0d-e49ffa2349d5/Risk%2BAssessment%2BGuide%2Bfor%2BTransferring%2BPersonal%2BData%2BOutside%2Bthe%2BKingdom.pdf?MOD=AJPERES>

SDAIA consulted on amendments to the PDPL Implementing Regulation from April 27 to May 27, 2025.⁹⁹³ The proposal would expressly require registration for controllers using Article 4 transfer safeguards and introduce a ten-business-day deadline for responding to regulatory requests. Industry seeks proportionate registration obligations, workable response periods, and clarity on proposed terminology changes concerning data breaches.

Other Barriers to Digital Trade

Since January 1, 2024, Saudi Arabia's regional-headquarters procurement rules generally restrict government entities from contracting with covered multinational companies and related parties that lack a regional headquarters in the Kingdom, subject to specified exceptions.⁹⁹⁴ 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. Qualifying RHQs receive a 30-year zero-percent corporate income-tax rate on eligible income and specified withholding-tax relief, subject to licensing and economic-substance requirements, alongside a 10-year Saudization exemption. Mandatory activities must begin within six months of licensing; at least three optional activities and employment of 15 full-time staff, including three senior executives, are required within one year. RHQs may earn revenue from licensed headquarters activities, while commercial operations outside that scope require appropriate separate licensing. 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.

Singapore

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

On May 7, 2024, Parliament passed amendments to the Cybersecurity Act 2018.⁹⁹⁵ Provisions commencing on October 31, 2025, expanded oversight of overseas and third-party-owned critical information infrastructure and broadened incident-reporting obligations.⁹⁹⁶ The amendments also establish a separate framework for designated major foundational digital infrastructure providers, including cloud computing and data centre providers.

⁹⁹³ DataGuidance. (2025, April 28). *Saudi Arabia: SDAIA opens public consultation on amendments to PDPL Implementing Regulation*. <https://www.dataguidance.com/news/saudi-arabia-sdaia-opens-public-consultation-1>

⁹⁹⁴ Zakat, Tax and Customs Authority. (n.d.). *Guideline for Regional Headquarters in KSA: Guideline to Clarify the Tax and Zakat Provisions Applicable to the Activities of Regional Headquarters*. <https://zatca.gov.sa/en/HelpCenter/guidelines/Documents/Guideline%20for%20Regional%20Headquarters%20in%20KSA%20%282%29.pdf>

⁹⁹⁵ Parliament of Singapore. (2024, April 3). *Cybersecurity (Amendment) Bill* (Bill No. 15/2024). [https://www.parliament.gov.sg/docs/default-source/bills-introduced/cybersecurity-\(amendment\)-bill-15-2024.pdf](https://www.parliament.gov.sg/docs/default-source/bills-introduced/cybersecurity-(amendment)-bill-15-2024.pdf)

⁹⁹⁶ Allen & Gledhill. (2025, October 24). *Amendments to Cybersecurity Act 2018 to update provisions related to critical information infrastructure and systems of temporary cybersecurity concern in force on 31 October 2025*. <https://www.allenandgledhill.com/sg/publication/articles/31411/amendments-to-cybersecurity-act-2018-to-update-provisions-related-to-critical-information-infrastructure-and-systems-of-temporary-cybersecurity-concern-in-force-on-31-october-2025>

On September 8, 2026, Singapore introduced the Digital Infrastructure Bill, proposing IMDA licensing for major co-location and cloud data centres with critical IT loads of at least 10 MW and cloud providers whose IaaS and PaaS services generate at least S\$100 million in average annual revenue from Singapore users over the preceding three years.⁹⁹⁷ Licensees would face security, business-continuity, disaster-recovery, and incident-reporting requirements. A separate licensing regime would impose energy-efficiency requirements on data centres with critical IT loads of at least 3 MW. The details of these proposed requirements will be detailed in Codes of Practice that are not yet issued, and warrant monitoring for their compliance costs, feasibility, and interaction with the Cybersecurity Act. CCIA encourages USTR to ensure that there are clear distinctions made between the requirements for a cloud provider versus a co-location data center provider to ensure there are no overlapping requirements.

Government-Imposed Content Restrictions and Related Access Barriers

The Protection from Online Falsehoods and Manipulation Act (POFMA) took effect on October 2, 2019.⁹⁹⁸ It empowers ministers, subject to statutory conditions, to require correction notices or restrictions on access to false statements of fact communicated in Singapore.⁹⁹⁹ Directions are subject to statutory challenge and court appeal. CCIA remains concerned that ministerial control over initial directions can constrain platforms' independent content moderation despite the availability of statutory appeals. Early enforcement included correction directions concerning politically contested statements; correction directions do not themselves require removal of the underlying content. Google stopped accepting political advertisements covered by POFMA's advertising code in December 2019 and continues to prohibit those advertisements in Singapore.¹⁰⁰⁰

The Online Safety (Miscellaneous Amendments) Act, passed on November 9, 2022, took effect on February 1, 2023, amending the Broadcasting Act to regulate specified online communication services accessible in Singapore.¹⁰⁰¹ It empowers IMDA to direct services to disable Singapore

⁹⁹⁷ Ministry of Digital Development and Information. (2026, September 8). *New Digital Infrastructure Bill to Strengthen the Foundations for Singapore's Digital Economy*. <https://www.mddi.gov.sg/newsroom/new-digital-infrastructure-bill-to-strengthen-the-foundations-for-singapore-s-digital-economy/>

⁹⁹⁸ Singapore. (2019). *Protection from Online Falsehoods and Manipulation Act 2019 (No. 18 of 2019)*. <https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625>

⁹⁹⁹ 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/>

¹⁰⁰⁰ Google. (n.d.). *Political content*. Google Ads Advertising Policies Help. <https://support.google.com/adspolicy/answer/6014595>

¹⁰⁰¹ Ministry of Communications and Information. (2023, January 31). *Online Safety (Miscellaneous Amendments) Act Takes Effect on 1 February 2023*. <https://www.mddi.gov.sg/newsroom/online-safety-act-takes-effect-on-1-february-2023/>

users' access to egregious content and, for non-compliance, direct internet service providers to block access to the service.

Separately, the Code of Practice for Online Safety took effect on July 18, 2023, imposing system-level safety, reporting, and accountability requirements on designated social media services.¹⁰⁰² The initial designated services were Facebook, HardwareZone, Instagram, TikTok, Twitter (now X), and YouTube. CCIA remains concerned that broadly defined harmful-content categories could encourage excessive restrictions on lawful expression and urges proportionate implementation.

Singapore extended online safety regulation to designated app stores through a Code effective March 31, 2025, with age-assurance measures required by March 31, 2026.¹⁰⁰³ These measures must at least establish whether users are under 18 to restrict access to age-inappropriate apps. In August 2026, MDDI also outlined a proposed tiered framework restricting under-13 access to designated social media services and requiring age-appropriate content, interactions, and features for users aged 13–18.¹⁰⁰⁴ Services unable to meet those safeguards could also face restrictions on serving that older group. In late August 2026, the government announced plans to introduce legislation in early 2027. Measures under consideration include daily usage limits, restrictions on autoplay and infinite scroll, and safeguards against unsolicited contact from strangers.

A separate bill, the Online Criminal Harms Bill (“OCH Bill”), passed on July 5, 2023.¹⁰⁰⁵ 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

¹⁰⁰² Infocomm Media Development Authority. (2023, July 17). *IMDA's Online Safety Code comes into effect*. <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imdas-online-safety-code-comes-into-effect>

¹⁰⁰³ Bird & Bird. (2026, April 1). *App Stores in Singapore Required to Implement Age Assurance Measures*. <https://www.twobirds.com/en/insights/2026/singapore/app-stores-in-singapore-required-to-implement-age-assurance-measures>

¹⁰⁰⁴ Ministry of Digital Development and Information. (2026, August 5). *MDDI's Response to PQ on Establishing Frameworks for Under-18 Social Media Access and Design Feature Safeguards*. <https://www.mddi.gov.sg/newsroom/mddi-s-response-to-pq-on-establishing-frameworks-for-under-18-social-media-access-and-design-feature-safeguards/>

¹⁰⁰⁵ Koh, C. L. (2023, August 21). *Singapore passes Online Criminal Harms Act*. Osborne Clarke. <https://www.osborneclarke.com/insights/singapore-passes-online-criminal-harms-act>; Singapore. (2023). *Online Criminal Harms Bill (Bill No. 17/2023)*. <https://www.parliament.gov.sg/docs/default-source/default-document-library/online-criminal-harms-bill-17-2023.pdf>

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.” Implementation Directives have imposed specific technical requirements on U.S. providers. Directives issued to Apple and Google on November 24, 2025, required anti-spoofing measures on iMessage and Google Messages. A second directive to Meta, issued on January 27, 2026, expanded facial-recognition and prioritized-report-review requirements to address impersonation scams, with phased deadlines extending through June 30, 2026.¹⁰⁰⁶

On August 17, 2026, the Singapore Police Force issued new OCHA Codes of Practice for Online Messaging and Conferencing Services and Social Media Services, and enhanced the E-Commerce Services Code.¹⁰⁰⁷ Requirements include government-record checks of advertisers’ identities, screening and removal of suspected scam advertisements, safeguards against unsolicited messaging and government impersonation, and stronger protections for e-commerce logins from unfamiliar devices. The messaging code covers seven services, including WhatsApp, Apple iMessage and FaceTime, and Google Messages and Meet; the social media code covers Facebook, Instagram, and TikTok. Compliance is generally required by January 31, 2027, with government-impersonation safeguards for messaging services due September 30, 2026. Requirements are calibrated by service risk, with full or partial waivers possible.

On September 9, 2026, Parliament passed the Scams (Countermeasures) and Other Matters Bill.¹⁰⁰⁸ Its OCHA amendments provide for administrative penalties of up to S\$10 million for non-compliance with Codes of Practice or Implementation Directives, and authorize directions issued through computer programs, including AI systems. The new penalty framework provides for written representations and appeals to the Minister for Home Affairs. These changes warrant scrutiny for proportionality and effective review of automated enforcement. The Bill also provides for criminal fines of up to S\$10 million for failure to comply with rectification notices or compliance orders, plus up to S\$300,000 per day for continuing offences after conviction. Separately, computer-issued OCHA directions remain subject to reconsideration by a designated

¹⁰⁰⁶ Ministry of Home Affairs. (2025, November 25). *Issuance of Implementation Directives to Apple and Google Under the Online Criminal Harms Act*.

<https://www.mha.gov.sg/media-room/newsroom/issuance-of-implementation-directives-to-apple-and-google-under-the-online-criminal-harms-act/>; Ministry of Home Affairs. (2026, January 29). *Issuance of Implementation Directive to Meta Under the Online Criminal Harms Act*.

<https://www.mha.gov.sg/mediaroom/press-releases/issuance-of-implementation-directive-to-meta-under-the-online-criminal-harms-act-ocha>

¹⁰⁰⁷ Singapore Police Force. (2026, August 18). *Issuance of Codes of Practice Under the Online Criminal Harms Act*.

https://www.police.gov.sg/Media-Hub/News/2026/08/20260818_issuance_of_codes_of_practice_under_the_online_criminal_harms_act

¹⁰⁰⁸ Ministry of Home Affairs. (2026, September 9). *The Scams (Countermeasures) and Other Matters Bill was passed in Parliament today to strengthen our operational capabilities against scams* [Facebook post].

<https://www.facebook.com/mhasingapore/posts/1502742218553598/>

officer and appeal to an independent Reviewing Tribunal comprising a District Judge or Magistrate.

Parliament passed the Online Safety (Relief and Accountability) Act 2025 on November 5, 2025.¹⁰⁰⁹ The Online Safety Commission began operations on June 29, 2026, alongside specified statutory tort provisions. Its initial remit covers online harassment, doxxing, online stalking, intimate image abuse, and image-based child abuse; eight further categories will be implemented progressively. The Commissioner can direct platforms to disable access to harmful content or restrict accounts and require disclosure of identifying information in appropriate cases. The civil framework requires platforms to take reasonable measures after receiving notice of specified harms and permits damages or injunctions for breaches. These overlapping administrative and civil obligations expand platforms' compliance and liability exposure.

South Africa

Asymmetric Platform Regulation

On February 6, 2026, the Competition Commission finalized its Online Intermediation Platforms Guidance Note.¹⁰¹⁰ The non-binding guidance focuses particularly on “leading or largest” platforms and identifies practices including self-preferencing and interoperability restrictions for scrutiny under the Competition Act. The Commission states that it will take the Guidance Note into account when assessing platform cases.¹⁰¹¹ CCIA has cautioned that focusing enforcement on certain digital companies, or relying on global scale rather than competitive effects in the South African market, could create asymmetric outcomes and legal uncertainty.¹⁰¹²

¹⁰⁰⁹ Singapore. (2025). *Online Safety (Relief and Accountability) Bill (Bill No. 18/2025)*. [https://www.parliament.gov.sg/docs/default-source/bills-introduced/online-safety-\(relief-and-accountability\)-bill-18-2025.pdf](https://www.parliament.gov.sg/docs/default-source/bills-introduced/online-safety-(relief-and-accountability)-bill-18-2025.pdf)

¹⁰¹⁰ Department of Trade, Industry and Competition. (2026, February 6). *Publication of the Online Intermediation Platforms Guidance Note*. https://www.gov.za/sites/default/files/gcis_document/202602/54086gon7095.pdf

¹⁰¹¹ Competition Commission South Africa. (2026, February 6). *Online Intermediation Platforms Guidance Note*. <https://www.compcom.co.za/wp-content/uploads/2026/02/Online-Intermediation-Platforms-Guidance-Note.pdf>

¹⁰¹² Computer & Communications Industry Association. (2025, December 1). *CCIA Comments on SACC Draft Guidance Note for Online Intermediation Platforms*. <https://ccianet.org/wp-content/uploads/2025/12/CCIA-Comments-on-SACC-Draft-Guidance-Note-for-Online-Intermediation-Platforms.pdf>

Barriers to the Deployment and Operation of Network Infrastructure

South Africa requires holders of individual electronic communications service and network service licences (e.g., fixed, mobile and satellite communication services) to maintain at least 30% ownership by historically disadvantaged groups.¹⁰¹³ In December 2025, the Minister of

Communications and Digital Technologies issued a policy direction seeking recognition of Equity Equivalent Investment Programmes (EEIPs) within the licensing framework.¹⁰¹⁴ In May 2026, South Africa requires holders of individual electronic communications service and network service licences (e.g., fixed, mobile and satellite communication services) to maintain at least 30% ownership by historically disadvantaged groups.¹⁰¹⁵ In December 2025, the Minister of Communications and Digital Technologies issued a policy direction seeking recognition of Equity Equivalent Investment Programmes (EEIPs) within the licensing framework.¹⁰¹⁶ In May 2026, ICASA stated that full recognition of EEIPs as an alternative to the statutory ownership requirement would require amendment of the Electronic Communications Act.¹⁰¹⁷ The government has announced that it will pursue legislative amendments; until then, applicants for individual licences remain subject to the 30% ownership requirement.¹⁰¹⁸

¹⁰¹³ Independent Communications Authority of South Africa. (2026, May 13). *ICASA communicates its response to the Policy Direction on Broad Based Black Economic Empowerment*.
<https://www.icasa.org.za/news/2026/icasa-communicates-its-response-to-the-policy-direction-on-broad-based-black-economic-empowerment>

¹⁰¹⁴ Independent Communications Authority of South Africa. (2025, December 13). *ICASA notes the policy direction on broad-based black economic empowerment in the ICT sector*.
<https://www.icasa.org.za/news/2025/icasa-notes-the-policy-direction-on-broad-based-black-economic-empowerment-in-the-ict-sector>

¹⁰¹⁵ Independent Communications Authority of South Africa. (2026, May 13). *ICASA communicates its response to the Policy Direction on Broad Based Black Economic Empowerment*.
<https://www.icasa.org.za/news/2026/icasa-communicates-its-response-to-the-policy-direction-on-broad-based-black-economic-empowerment>

¹⁰¹⁶ Independent Communications Authority of South Africa. (2025, December 13). *ICASA notes the policy direction on broad-based black economic empowerment in the ICT sector*.
<https://www.icasa.org.za/news/2025/icasa-notes-the-policy-direction-on-broad-based-black-economic-empowerment-in-the-ict-sector>

¹⁰¹⁷ Independent Communications Authority of South Africa. (2026, May 13). *ICASA communicates its response to the Policy Direction on Broad Based Black Economic Empowerment*.
<https://www.icasa.org.za/news/2026/icasa-communicates-its-response-to-the-policy-direction-on-broad-based-black-economic-empowerment>

¹⁰¹⁸ Department of Communications and Digital Technologies. (2026, May 19). *Minister Solly Malatsi: Communications and Digital Technologies Dept Budget Vote 2026/27*.
<https://www.gov.za/news/speeches/minister-solly-malatsi-communications-and-digital-technologies-dept-budget-vote-0>

ICASA is also developing a new satellite licensing framework. In May 2026, ICASA published draft amendments to the Radio Frequency Spectrum Regulations and Radio Frequency Spectrum Fees Regulations that would establish a registration regime for satellite space-segment operators, revised spectrum-fee formulas, blanket licensing for satellite terminal networks, and rules for Earth Stations in Motion.¹⁰¹⁹ Public hearings were held on August 19–20, 2026, and the amendments remained pending as of September 2026.¹⁰²⁰ Separately, in June 2026, ICASA clarified that a single entity providing services through a satellite constellation in South Africa requires an Individual Electronic Communications Service (I-ECS) licence, an Individual Electronic Communications Network Service (I-ECNS) licence, and the relevant radio-frequency-spectrum licence(s).¹⁰²¹ ICASA further confirmed that new I-ECNS licences can only be issued following a ministerial policy direction and an invitation to apply; in the absence of such a process, prospective entrants may seek to acquire an existing individual licence through a transfer approved by ICASA.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

In September 2026, ICASA initiated a market inquiry into the impact of over-the-top (OTT) services on licensees and South Africa’s regulatory framework, covering the telecommunications, broadcasting, and postal sectors.¹⁰²² The inquiry remains at an initial stage: ICASA has not yet proposed substantive obligations and intends next to publish a Discussion Document for public comment.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

On May 31, 2024, the Department of Communications and Digital Technologies published the final National Data and Cloud Policy.¹⁰²³ The Policy stipulates that “Government data that incorporates content pertaining to the protection and preservation of national security and

¹⁰¹⁹ Independent Communications Authority of South Africa. (2026, May 15). *ICASA Publishes Draft Amendments to the Radio Frequency Spectrum Regulations and Radio Frequency Spectrum Fees Regulations*. <https://www.icasa.org.za/news/2026/icasa-publishes-draft-amendments-to-the-radio-frequency-spectrum-regulations-and-radio-frequency-spectrum-fees-regulations>

¹⁰²⁰ Independent Communications Authority of South Africa. (2026, August 7). *ICASA to Hold Public Hearings on Draft Amendments to Radio Frequency Spectrum Regulations and Fees Regulations*. <https://www.icasa.org.za/news/2026/icasa-to-hold-public-hearings-on-draft-amendments-to-radio-frequency-spectrum-regulations-and-fees-regulations>

¹⁰²¹ Independent Communications Authority of South Africa. (2026, June). *Notice Regarding Licensing Requirements to Operate Satellite Services*. <https://www.icasa.org.za/legislation-and-regulations/notice-regarding-licensing-requirements-to-operate-satellite-services>

¹⁰²² Independent Communications Authority of South Africa. (2026, September 9). *Correction Notice: Notice of Intention to Conduct Market Inquiry into the Impact of OTT Services on Licensees and Regulatory Framework in South Africa*. <https://www.gov.za/documents/notices/independent-communications-authority-south-africa-act-erratum-correction-notice>

¹⁰²³ *Electronic Communications Act 36 of 2005* [South Africa]. (2006). <https://www.gov.za/documents/electronic-communications-act>

sovereignty of the Republic shall be stored only in digital infrastructure located within the borders of South Africa.” The Policy does not further define which government data “pertains” to national security and sovereignty, leaving uncertainty as to the scope of this government-data localization requirement.¹⁰²⁴

Forced Revenue Transfer for Digital News

In November 2025, the Competition Commission released the final report of its Media and Digital Platforms Market Inquiry.¹⁰²⁵ The final report dropped the provisional annual levy and penalty proposals following consultations with digital platforms, but imposed platform-specific remedial actions. Google is required to contribute up to R687.5 million (about \$40 million) over five years through News Showcase payments, a Digital News Transformation Fund, AI innovation funding, and other publisher-support initiatives. Meta is required to provide US\$2.5 million in new funding over three years. Additional remedies apply to Microsoft, TikTok, X/X.AI, and OpenAI, including measures related to publisher monetization, transparency, content controls, and training. The final findings are subject to appellate proceedings. As of 2026, the Competition Tribunal had received six appeals from parties affected by the Commission’s MDPMI findings.¹⁰²⁶

Discriminatory Local Content Quotas and Audiovisual Service Mandates

On July 11, 2025, South Africa published a draft White Paper on Audio and Audiovisual Media Services and Online Safety that would extend the regulatory framework beyond traditional broadcasting to on-demand content services and video-sharing platforms.¹⁰²⁷ The draft proposes registration and notification obligations for these services. It also provides that South African-content obligations may be extended to on-demand content services, as determined in a subsequent consultation. Under existing ICASA regulations, public and community television broadcasters must generally devote a minimum weekly average of 65% of programming to South African content and commercial television broadcasters 45%; subscription television broadcasters instead must spend at least 15% of their annual content-acquisition budget on local television programming and at least 15% of their annual channel-acquisition budget on channels with local television content compiled and uplinked from South Africa. Foreign ownership in commercial broadcasting licensees is currently capped at 20%, although the draft White Paper

¹⁰²⁴ iAfrikan. (2023, June 4). *South Africa Publishes Data & Cloud Plan to Enhance Data Sovereignty*. <https://iafrikan.com/sa-published-cloud-plan/>

¹⁰²⁵ Competition Commission South Africa. (2025, February). *Media and Digital Platforms Market Inquiry: Provisional Report*. https://www.compcom.co.za/wp-content/uploads/2025/02/CC_MDPMI-Provisional-Report_Non-Confidential-Final.pdf

¹⁰²⁶ Competition Tribunal of South Africa. (2026). *Annual Performance Plan 1 April 2026–31 March 2027*. <https://www.thedtic.gov.za/wp-content/uploads/Competition-Tribunal-APP-2026-2027.pdf>

¹⁰²⁷ Department of Communications and Digital Technologies. (2025, July 11). *Draft White Paper on Audio and Audiovisual Media Services and Online Safety*. https://www.gov.za/sites/default/files/gcis_document/202507/52972gen3369.pdf

proposes increasing the cap to a maximum of 49% for linear individual audiovisual-content services. The public-comment deadline was extended to September 26, 2025. As of September 2026, the measure stands as a draft and no final White Paper has been published.

Spain

Discriminatory Local Content Requirements

Spain's audiovisual regulations require on-demand audiovisual media service providers to include at least 30% EU content in their catalogues, with at least half of that content in an official language of Spain, and require broadcasters and VOD providers with revenues exceeding €50 million (approximately \$56 million) to invest 5% of their revenues in the production of EU and Spanish works, with 40% of that investment reserved for works by independent producers in any of Spain's official languages.

Taxation of Digital Products and Services

Spain's digital services tax, effective January 16, 2021, imposes a 3% levy on revenues from online advertising, online intermediation, and transmission of user data attributable to users in Spain.¹⁰²⁸ It applies to businesses with prior-calendar-year worldwide net turnover exceeding €750 million and Spanish taxable digital-services revenues exceeding €3 million, with thresholds assessed at group level where applicable. From 2021 through 2025, Spain has extracted over US\$1.83 billion from this tax.¹⁰²⁹ USTR's 2021 investigation estimated that U.S. companies represented over 64% of companies covered by Spain's DST and U.S. companies were cited throughout legislative debate making the targets clear.¹⁰³⁰ Spain participated in the October 2021 transitional agreement with the United States concerning existing DSTs and OECD Pillar One but that has since expired.¹⁰³¹ Given the moribund status of Pillar 1, and the Section 301 finding of discriminatory and unreasonable burdens, USTR should refresh the 301 record and reconsider what additional steps are necessary to facilitate removal of this tax.

¹⁰²⁸ 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>

¹⁰²⁹ CCIA. (2026). *Status of Key Digital Services Taxes*. <https://ccianet.org/library/2026-status-of-key-digital-services-taxes/>

¹⁰³⁰ Congress of Spain. (2020, June 4). *Diario de Sesiones, 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>. (Debate expressly references Google, Amazon, Facebook, and Apple as intended taxpayers.)

¹⁰³¹ 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>

Barriers to the Deployment and Operation of Network Infrastructure

In August 2026, the Ministry for Ecological Transition published a draft Royal Decree introducing requirements for energy efficiency, environmental sustainability, resilience and digital sovereignty applicable to data centers. The text underwent public consultation and is expected to be published in the coming months. The regulation will make grid access and connection permits for data centers conditional on compliance with a comprehensive set of requirements that go beyond existing EU frameworks. On the energy side, the draft establishes mandatory energy and water efficiency thresholds (PUE/WUE) that are misaligned with existing EU requirements, an 80% renewable energy consumption quota, additionality requirements for power purchase agreements with narrow time windows, and a financial surcharge regime backed by permit revocation for non-compliance. On the sovereignty side, the draft requires that all data, metadata and operational logs derived from the data center operation remain within EU territory. It further prohibits the hosting of public sector data under the National Security Framework unless all data – including telemetry, replicas and backups – is processed and stored exclusively within the EU.

Sri Lanka

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Sri Lanka amended its Personal Data Protection Act through Act No. 22 of 2025, certified on October 30, 2025.¹⁰³² A July 2026 commencement order schedules sections 2 and 3 and Parts I and III, including cross-border transfer requirements, to take effect on January 1, 2027.¹⁰³³ The amended section 26 removes the earlier general restriction on public-sector overseas processing and permits public and private entities to use cross-border transfer mechanisms, subject to safeguards and specified exceptions. However, the Minister may prohibit transfers of designated categories of public-authority personal data. Transfers generally require instruments specified by the Data Protection Authority to secure enforceable safeguards from overseas recipients. The Authority's August 2026 circular confirms that the amendments enable public-sector use of global cloud infrastructure, while referring to a draft transfer directive.¹⁰³⁴ USTR should encourage clear, interoperable transfer mechanisms and narrowly tailored restrictions that preserve Sri Lankan business and consumer access to U.S. cloud services.

¹⁰³² Parliament of Sri Lanka. (2022, March 19). *Personal Data Protection Act, No. 9 of 2022*. <https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf>

¹⁰³³ Government of Sri Lanka. (2026, July 22). *Personal Data Protection Act, No. 9 of 2022: Order under subsection (3) of Section 1, Gazette Extraordinary No. 2498/16*. https://www.dpa.gov.lk/Gazet/2498-16_E.pdf

¹⁰³⁴ Data Protection Authority of Sri Lanka. (2026, August 7). *Application of PDPA in the Public Sector: Personal Data Protection Circular No. 01/2026*, section 4.6. https://www.dpa.gov.lk/media/DPA_Circular_012026_E.pdf

Government-Imposed Content Restrictions and Related Access Barriers

Sri Lanka's Online Safety Act, No. 9 of 2024, certified on February 1, 2024,¹⁰³⁵ creates broadly framed offenses involving false statements and gives an Online Safety Commission extensive content-regulation powers. Section 12 criminalizes false statements that threaten national security, public health or public order, or promote hostility between groups, with penalties of up to five years' imprisonment, a fine of up to LKR 500,000, or both. Other offenses carry different penalties. These provisions raise concerns about restrictions on lawful expression and arbitrary enforcement. The law also allows the Commission to order internet service providers and intermediaries to remove posts declared "prohibited statements."

In February 2026, the Human Rights Commission of Sri Lanka called for a moratorium on use of the Act pending repeal and replacement, warning that its use to suppress expression raises serious constitutional concerns.¹⁰³⁶ The vague definitions of offenses and broad information-gathering powers heighten the risk of arbitrary enforcement against online service providers, including U.S. suppliers. 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." On June 23, 2026, Parliament approved the second reading of a private member's Online Safety (Repeal) Bill and referred it to the Legislative Standing Committee.¹⁰³⁷ The Bill remains unpassed. USTR should encourage reform, including repeal of this bill, that narrows vague speech offenses, strengthens judicial safeguards, and provides predictable obligations for online intermediaries.

In June 2026, MP Faiszer Musthapha proposed a Social Media Minimum Age Bill that would empower the Minister responsible for child affairs to require specified social-media and internet-service providers to restrict children's access to services or features and impose usage-duration and time-of-day limits.¹⁰³⁸ The draft defines children as persons under 16. These proposed restrictions could affect services supplied to Sri Lankan users by U.S. platforms. USTR should encourage clear coverage, proportionate obligations, and privacy-protective implementation.

¹⁰³⁵ Parliament of Sri Lanka. (2024). *Online Safety Act, No. 9 of 2024*.

<https://www.parliament.lk/uploads/acts/gbills/english/6311.pdf>

¹⁰³⁶ Human Rights Commission of Sri Lanka. (2026, February 3). *Statement on the Freedom of Expression and Online Safety in Sri Lanka*.

https://www.hrcsl.lk/wp-content/uploads/2026/02/HRCSL-Statement-on-the-Freedom-of-Expression-and-Online-Safety-in-Sri-Lanka_English_03_02_2026.pdf

¹⁰³⁷ Parliament of Sri Lanka. (2026, June 23). *Business of the House for June 23, 2026*.

<https://www.parliament.lk/en/home/parliament-news/view/5227>

¹⁰³⁸ Newswire. (2026, June 24). *Private Member's Bill seeks social media age limit of 16 in Sri Lanka*.

<https://www.newswire.lk/2026/06/24/private-members-bill-seeks-social-media-age-limit-of-16-in-sri-lanka/>

Switzerland

Threats to the Security of Devices and Services

In January 2025, the Swiss Federal Council launched a public consultation on the Telecommunications Surveillance Ordinances to clarify cooperation obligations for telecommunications and communications service providers.¹⁰³⁹ The January 2025 draft proposed three tiers of obligations for derived communications service providers, including covered cloud services. Depending on the tier, providers would face expanded data-retention, user-identification, and technical surveillance requirements. The Federal Council states that the proposed decryption obligation excludes end-to-end encryption, although expanded identification and retention requirements would still raise privacy and data-security concerns. Following substantial criticism during consultation, the Federal Council announced on February 11, 2026 that the proposal was being revised, with an external regulatory impact assessment examining effects on affected businesses and a second public consultation planned.¹⁰⁴⁰ If adopted, the expanded surveillance, data-retention, and user-identification requirements could increase compliance costs and create privacy and data-security risks for U.S. cloud providers falling within the relevant provider categories.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

On November 24, 2025, *privatim*, the Conference of Swiss Data Protection Officers, published a resolution stating that public bodies may use international SaaS solutions for sensitive personal data or personal data subject to statutory secrecy only where the public body encrypts the data itself and the provider cannot access the key.¹⁰⁴¹ The resolution specifically identifies exposure to the U.S. CLOUD Act, including for data stored in Switzerland. This supervisory position could prejudice public-sector procurement from U.S. providers whose services require access to unencrypted data, but it does not directly impose restrictions. The canton of Glarus opted out of the resolution.

Government-Imposed Content Restrictions and Related Access Barriers

On October 29, 2025, the Federal Council opened consultation on a proposed Federal Act on Communication Platforms and Search Engines; consultation closed on February 16, 2026.¹⁰⁴²

¹⁰³⁹ 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>

¹⁰⁴⁰ Swiss Federal Council. (2026, February 11). *Fernmeldeüberwachung und mitwirkungspflichtige Unternehmen: Bundesrat nimmt Ergebnis des Vernehmlassungsverfahrens zur Kenntnis*. <https://www.admin.ch/de/newsb/EXv-JkPBAZuL>

¹⁰⁴¹ *Privatim*. (2025, November 24). *Publikation: Resolution zur Auslagerung von Datenbearbeitungen in die Cloud*. <https://www.privatim.ch/de/publikation-resolution-zur-auslagerung-von-datenbearbeitungen-in-die-cloud/>

¹⁰⁴² Swiss Federal Office of Communications. (n.d.). *Vernehmlassungen, Anhörungen und Konsultationen*. <https://www.bakom.admin.ch/de/vernehmlassungen-anhoerungen-und-konsultationen>

The draft, modeled on the EU's DSA, covers services that reach at least 10 percent of Switzerland's population. It would impose content-notification and complaint procedures, advertising and recommender-system transparency, data-access obligations, and mandatory Swiss legal representation for covered foreign providers. Certain violations could attract sanctions of up to 6 percent of average worldwide annual turnover over the preceding three financial years. The draft also provides for an annual supervisory levy capped at 0.05 percent of the provider's worldwide profit in the preceding financial year. Where corrective measures prove ineffective or are expected to be ineffective, OFCOM could order telecommunications providers to restrict access to a service, subject to a 30-day opportunity to respond and demonstrate compliance; restrictions could be renewed if violations persist or recur. These requirements could create additional compliance costs and substantial financial exposure for covered U.S. providers.

Forced Revenue Transfers for Digital News

Switzerland's proposed neighboring right for media publishers would require large online services to remunerate publishers for displaying short text and image previews. On June 17, 2026, Parliament completed its decision to return the proposal to the Federal Council for further work addressing AI-related uses of journalistic content.¹⁰⁴³ The original proposal targeted services used by at least 10 percent of the Swiss population. Its revision could extend payment obligations affecting U.S. search, social-media, and AI providers; the scope remains unsettled. USTR should oppose this bill as inconsistent with the Berne Conventions right of quotation (Article 10 (1)).

Taiwan

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Under Taiwan's Financial Supervision Commission (FSC) outsourcing regulations, most recently amended on April 13, 2026, overseas outsourcing of material retail financial business information systems requires prior approval.¹⁰⁴⁴ Applications must include risk assessments, customer-data safeguards, outsourcing plans, and arrangements for regulatory access. Industry urges the FSC to streamline documentation and establish predictable review timelines for U.S. cloud services.

Taiwan has sector-specific outsourcing rules for securities firms, futures commission merchants, and securities investment trust and consulting enterprises, supplemented by cloud-security

¹⁰⁴³ Keystone-SDA. (2026, June 17). *Parlament schickt Leistungsschutz für Medien auf Zusatzrunde*. https://www.parlament.ch/de/services/news/Seiten/2026/20260617094927186194158159026_bsd041.aspx

¹⁰⁴⁴ 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.

guidance. Industry urges consistent, proportionate implementation across these sectors to prevent duplicative compliance requirements from restricting access to U.S. cloud services.

Regulations have also been promulgated in both the financial services and health industries advancing data localization requirements. For financial services, Article 19 generally requires customer data from material retail financial business information systems to be stored in Taiwan, unless the regulatory agency grants an exemption. In the healthcare sector, Article 8 of the Regulations Governing the Creation and Management of Electronic Medical Records by Medical Institutions requires data storage for covered cloud services to be located in Taiwan, unless the central competent authority approves an exception because of special circumstances.

Amendments to the Cyber Security Management Act were promulgated on September 24, 2025, and took effect on December 1, 2025.¹⁰⁴⁵ The amended law requires consultation before critical infrastructure providers are designated and permits investigations of contractors involved in major cybersecurity incidents. Covered entities face expanded governance and reporting obligations, including fines of up to NT\$10 million for failure to report an incident. Industry urges transparent designation criteria and proportionate requirements that avoid unnecessary burdens on U.S. cloud providers.

Taiwan's National Science and Technology Council (NSTC) has issued an administrative ruling restricting government agencies from using public cloud-based generative AI services. While intended to protect sensitive information, the ruling creates significant market access barriers for global cloud service providers (CSPs) and their AI offerings. The ruling's core requirement mandates on-premises deployment for the use of generative AI by government agencies, explicitly prohibiting public cloud-based AI services for government data processing. This creates a *de facto* data localization requirement and restricts the use of public cloud through technical specifications.

Forced Revenue Transfers for Digital News

Legislators from the Kuomintang, Democratic Progressive Party, and Taiwan People's Party have proposed news-media bargaining legislation.¹⁰⁴⁶ The Legislative Yuan's Transportation Committee held a public hearing on June 12, 2025, involving government officials, academics, journalists and media associations.¹⁰⁴⁷ Proposals discussed included mandatory bargaining

¹⁰⁴⁵ 數位發展部 [Ministry of Digital Affairs, Taiwan]. 資通安全管理法 [Cyber Security Management Act]. 主管法規共用系統 [Laws and Regulations Retrieving System]. <https://law.moda.gov.tw/LawContent.aspx?id=FL088622>.

¹⁰⁴⁶ Shan, S. (2023, May 23). MODA to create model for news media bargaining act. *Taipei Times*. <https://www.taipetimes.com/News/taiwan/archives/2023/05/23/2003800275>.

¹⁰⁴⁷ 信傳媒 [CM Media]. (2025, June 12). 記者變代工、新血轉行送外送 傳播學者、媒體業齊聲促立《媒體議價法》：政府別「只講不做」 [Journalists Reduced to Piecework, New Blood Turning to Food Delivery: Communications Scholars and Media Industry Jointly Urge Passage of the Media Bargaining Act]. <https://www.cmmedia.com.tw/home/articles/54896>.

between digital platforms and news organizations and a fund supporting smaller news outlets. 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. Mandatory bargaining or funding obligations could impose costs on covered digital platforms, including U.S. suppliers. Whether the resulting framework would discriminate against foreign suppliers would depend on its coverage, designation criteria, and treatment of comparable domestic services. 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

Taiwan promulgated the Fraud Crime Hazard Prevention Act on July 31, 2024.¹⁰⁴⁸ Covered online advertising platforms must verify advertisers and advertising funders, disclose specified advertising information, publish annual fraud-prevention transparency reports, and remove fraudulent advertisements within applicable notification deadlines. The AI disclosure requirement concerns deepfakes or AI-generated images of individuals, rather than all generative-AI use. MODA's 2026 legislative report records four penalties against Meta totaling NT\$18.5 million in 2025 and confirms that all four covered operators published transparency reports by the end of December 2025. Industry urges proportionate enforcement, clear notice procedures, and workable compliance deadlines.

Industry remains concerned that Taiwan's sectoral intermediary-liability rules expose platforms to liability for third-party content without sufficiently clear safeguards. The Tobacco Hazards Prevention Act penalizes advertising and media operators for prohibited tobacco advertising, while also providing penalties for commissioning clients and other persons responsible for unlawful promotion. Industry urges USTR to seek clear distinctions between paid advertising and organic user content, proportionate platform obligations, and safe harbors for intermediaries acting promptly on valid notices.

Restrictions on Cross-Border Data Flows

Article 21 of Taiwan's Personal Data Protection Act permits authorities to restrict international transfers in specified circumstances, including inadequate protection in the receiving jurisdiction.¹⁰⁴⁹ Industry is concerned that any Taiwan-specific standard contractual clauses could create duplicative obligations unless they are interoperable with established international

¹⁰⁴⁸Taiwan Legislative Yuan (2024). *Fraud Crime Hazard Prevention Act* . <https://law.moj.gov.tw/ENG/LawClass/LawHistory.aspx?pcode=D0080226> .

¹⁰⁴⁹ Ministry of Justice (Taiwan). (2023). Personal Data Protection Act, Article 21. Laws & Regulations Database of the Republic of China (Taiwan). <https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021> .

mechanisms and remain flexible enough to accommodate equivalent safeguards. 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 Tanzania Communications Regulatory Authority (TCRA) required individuals and organizations whose work necessitates VPN use to declare their VPN details, including IP addresses.¹⁰⁵⁰ The notice invoked Regulation 16(2) of the Electronic and Postal Communications (Online Content) Regulations, 2020, which prohibits tools that facilitate access to prohibited content. That offense carries a minimum fine of TZS 5 million, imprisonment of at least 12 months, or both.

On August 30, 2024, several ISPs blocked access to X for nearly 24 hours, without a public explanation, coinciding with an online campaign concerning alleged murders, kidnappings, and disappearances.¹⁰⁵¹ In October 2024, TCRA suspended Mwananchi Communications Ltd.'s online content licenses for 30 days over content it alleged harmed the country's image and national unity.¹⁰⁵²

Restrictions escalated in 2025. Authorities blocked X in May, and a nationwide internet shutdown ran from October 29 to November 3 during and after the general election.¹⁰⁵³ These disruptions prevented access to online platforms and interrupted the delivery of digital services to Tanzanian users. The restriction on X was also challenged in constitutional proceedings before

¹⁰⁵⁰ Tanzania Communications Regulatory Authority. (2023, October 13). *Declaration of Use of Virtual Private Network (VPN)*. <https://www.tcra.go.tz/news/public-notice-declaration-of-use-of-virtual-private-network-vpn>

¹⁰⁵¹ 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/> and 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/>

¹⁰⁵² 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/>

¹⁰⁵³ Tech & Media Convergency. (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/>

the High Court of Tanzania in 2026, with the applicants contesting its legal basis and proportionality.¹⁰⁵⁴

January 2025 amendments to the Online Content Regulations require internet service providers to block prohibited content and social media platform owners to deploy mechanisms to filter and remove it.¹⁰⁵⁵ These obligations impose additional content-control requirements on platforms serving Tanzania.

Taxation of Digital Products and Services

Effective July 1, 2026, Tanzania increased its digital services tax from 2% to 3% of gross payments under the Finance Act, 2026.¹⁰⁵⁶ The tax applies to non-resident providers receiving Tanzanian-sourced payments from individuals not conducting business for electronic services. No registration threshold applies, bringing small non-resident providers within the regime regardless of their volume of covered sales. Also in July, Tanzania also extended excise duties to specified services supplied electronically by non-residents to customers in Mainland Tanzania who are neither registered nor required to file excise returns for the relevant service. Rates include 17% for electronic communications, 7% for pay television and subscription video-on-demand, and 10% for money transfer and payment services and betting, gaming, or lottery advertising. Covered suppliers face registration and monthly filing and payment obligations, adding tax and compliance costs for U.S. providers.

Tanzania requires covered data controllers and processors to register with the Personal Data Protection Commission (PDPC) and obtain a permit before transferring personal data outside the country. Transfer applications must identify the data, purpose, destination, and recipient and demonstrate appropriate safeguards. PDPC may approve, seek additional information, or reject an application. These requirements subject international data transfers supporting digital services to regulatory authorization. In August 2026, PDPC announced that it had begun compliance inspections of institutions and businesses collecting or processing personal data.¹⁰⁵⁷

¹⁰⁵⁴ Southern Africa Litigation Centre. (2026, March 5). *Tanzania: Challenging the Restriction of X (formerly Twitter)*. <https://www.southernafricalitigationcentre.org/tanzania-challenging-the-restriction-of-x-formerly-twitter/>

¹⁰⁵⁵ United Republic of Tanzania. (2025, January 28). *Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2025, Government Notice No. 57*. https://www.tcra.go.tz/tcra-tovuti/2025/mamlaka-website/documents/regulations/en_1738833320_Online_Content_Amendment_Regulations_2025_GN_No_57_of_28_January_2025_fad57339dc.pdf

¹⁰⁵⁶ United Republic of Tanzania. (2026, June 30). *Finance Act, 2026, Act No. 2, sections 2 and 24*. <https://oagmis.oag.go.tz/portal/acts/337/download>

¹⁰⁵⁷ Personal Data Protection Commission. (2026, August 28). *PDPC yaanza ukaguzi kwa wakusanyaji na wachakataji wa taarifa binafsi nchini*. <https://pdpc.go.tz/news/pdpc-yaanza-ukaguzi-kwa-wakusanyaji-na-wachakataji-wa-taarifa-binafsi-nchini/>

Thailand

Asymmetric Platform Regulation

The Royal Decree on the Operation of Digital Platform Service Businesses That Are Subject to Prior Notification, B.E. 2565¹⁰⁵⁸ took effect on August 21, 2023, and requires covered digital platform services to notify the Electronic Transactions Development Agency (ETDA), with large-scale or high-impact services subject to additional obligations. Offshore operators subject to the Decree must appoint a coordinator located in Thailand to serve as a point of contact with ETDA. ETDA has separately developed self-regulatory guidance and Codes of Conduct addressing issues including identity verification and online advertising, including guidance concerning the use of digital identification.

On July 9, 2025, the Royal Gazette initially designated 19 online marketplaces as services required to comply with additional obligations under Section 20 of the Royal Decree, and ETDA subsequently expanded the list.¹⁰⁵⁹ The definition of online marketplaces threatens to expand ecommerce obligations to online digital advertising, by treating advertising as selling. Additional requirements for designated online marketplaces took effect on December 31, 2025, with 21 platforms subject to obligations including verification of sellers and information concerning regulated products, monitoring of products subject to Thai regulatory standards, notice-and-takedown procedures, reporting requirements, and measures to suspend or remove noncompliant products.¹⁰⁶⁰ These additional obligations substantially increase the compliance burden for covered platforms and provide ETDA significant discretion over the operation of online marketplaces. The list of designated platforms will be reviewed annually, creating ongoing regulatory uncertainty for affected services.

In August and September 2026, ETDA conducted consultations on a further expansion of obligations applicable to digital platform services under the Royal Decree. The proposals contemplate horizontal requirements concerning transparency reporting, notice-and-action mechanisms, automated decision-making, service-level standards, labeling of AI-generated content, user interface design, and treatment of business users, alongside sector-specific requirements for online marketplaces, social media, sharing-economy services, audiovisual and

¹⁰⁵⁸ 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>.

¹⁰⁵⁹ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) [Electronic Transactions Development Agency]. (2025, October 2). ETDA ประกาศรายชื่อแพลตฟอร์มตลาดสินค้า เพิ่ม! ตามกฎหมายกำกับดูแลธุรกิจแพลตฟอร์มดิจิทัล [ETDA Announces Additional Marketplace Platforms Under the Digital Platform Services Law]. https://www.etda.or.th/th/pr-news/dps_announce.aspx.

¹⁰⁶⁰ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) [Electronic Transactions Development Agency]. ETDA เผย ประกาศ การดำเนินการอื่นสำหรับแพลตฟอร์มดิจิทัลประเภทตลาดสินค้า ตาม ม.18 (2) มีผลบังคับใช้ [ETDA Announces That the Notification on Other Operations for Marketplace-Type Digital Platforms Under Section 18(2) Takes Effect]. https://www.etda.or.th/th/pr-news/announce_dpslaw18.aspx.

music-sharing platforms, and virtual assistants. Among other provisions, the proposals contemplate anti-self-preferencing rules, ranking and algorithm transparency requirements, external algorithm audits for certain platforms, restrictions on profiling, seller and advertiser verification, and additional content-management obligations. Many of these measures resemble elements of the EU Digital Services Act and Digital Markets Act and, if adopted without appropriate tailoring, could significantly increase regulatory burdens on U.S. digital services suppliers.

ETDA's August–September 2026 consultations explored potential legislation establishing “gatekeeper” platforms and imposing obligations including restrictions on self-preferencing and the use of non-public business-user data. Industry recommends that the U.S. government continue to monitor the proposal and encourage Thailand to avoid ex ante or asymmetric obligations that disproportionately burden U.S. online marketplaces, app stores, and other digital services suppliers.

In March 2026, the Trade Competition Commission of Thailand (TCCT) adopted Guidelines on Unfair Trade Practices, Monopolization, and Conduct Restricting Competition in Multi-Sided Digital Platform Businesses, which entered into force later that month.¹⁰⁶¹ The Guidelines establish a framework for applying the Trade Competition Act to e-commerce platforms and address both pricing and non-price conduct, including algorithmic practices, preferential treatment of sellers or affiliated services, restrictions involving logistics and payment providers, and allegedly excessive or discriminatory fees. Although enforcement is intended to proceed on a case-by-case basis, affected platforms have raised concerns regarding the need for proportionate algorithmic transparency requirements, recognition of legitimate operational requirements, and sufficient flexibility in designing fee structures and integrated services. The Guidelines represent a significant expansion of Thailand's regulatory scrutiny of digital platform business models.

Thailand is drafting legislation to regulate digital services, adopting concepts from the EU's Digital Services Act (DSA) and Digital Markets Act (DMA). Under this proposed law, cloud services could be classified as 'intermediaries' and may become subject to 'gatekeeper' obligations. During the previous administration, development of the law was paused due to concerns about potential impacts on digital innovation and possible creation of trade barriers. However, with the recent change in government, the initiative has been revived. The new administration announced its intention to pursue this legislation in its policy statement in late September 2025. The government, as of today, is still working on the draft.

¹⁰⁶¹ Tilleke & Gibbins. (2026, March 30). Thailand Issues New Competition Guidelines for Multi-Sided and E-Commerce Platforms. <https://www.tilleke.com/insights/thailand-issues-new-competition-guidelines-for-multi-sided-and-e-commerce-platforms/>.

Customs-related Restrictions and Import Barriers for Goods

Thailand's Electronic Transactions Development Agency (ETDA) is developing a regulation that would require e-commerce marketplaces to provide buyers and sellers with a choice of at least three logistics carriers. The proposal has not been publicly circulated, raising concerns about limited consultation and whether the requirements adequately reflect the diversity of marketplace business models and cross-border delivery arrangements. A mandatory minimum number of logistics providers could restrict commercial flexibility and impose disproportionate operational burdens on U.S. online marketplaces. Thailand should conduct meaningful public consultations and ensure that any final requirements preserve competition, consumer choice and commercially viable logistics arrangements.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Thailand is developing a new national regulatory framework for data center operations.¹⁰⁶² In August 2026, the government established a Data Center Business Policy Committee, which held its first meeting on September 4, 2026. Following that meeting, the government asked operators of approximately 49 data center projects under construction to pause work while approval decisions for more than 117 additional projects were held pending development of new national standards. The government has tasked several subcommittees with developing minimum standards concerning economic benefits, infrastructure, siting, and environmental impacts. Separately, in September 2026, the Office of the National Broadcasting and Telecommunications Commission proposed new data center licensing criteria.¹⁰⁶³ Reported draft criteria would require applicants to be Thai juridical persons and would impose post-licensing commitments including use of at least 50 percent domestically sourced materials in specified construction, structural, and electrical-system inputs, subject to exceptions where qualifying domestic products are unavailable or unsuitable. As of September 2026, these licensing and local-content criteria remain proposed and have not taken effect.

Thailand has continued to develop its “Cloud First” framework for government use of cloud services. In January 2026, the Digital Government Development Agency (DGA) conducted a public consultation on draft standards addressing government cloud management, cloud usage, cloud service provider qualification, and provider assessment and certification.¹⁰⁶⁴ Under the

¹⁰⁶² สำนักงานนายกรัฐมนตรี [Office of the Prime Minister of Thailand]. (2026, August 13). ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยคณะกรรมการนโยบายการประกอบกิจการดาต้าเซ็นเตอร์ พ.ศ. ๒๕๖๔ [Office of the Prime Minister Regulation on the Data Center Business Policy Committee, B.E. 2569 (2026)], ราชกิจจานุเบกษา [Royal Gazette], Vol. 143, Special Part 192. <https://ratchakitcha.soc.go.th/documents/125826.pdf>.

¹⁰⁶³ คัมภา, ช. [Khampha, C.]. (2026, September 9). กสทช. ชี้ดเส้น Data Center Hub ต้องปลอดภัย ยื่น 5 กฎเหล็กคุมเข้ม [NBTC Draws the Line: Data Center Hub Must Be Secure, Proposes Five Strict Rules]. ฐานเศรษฐกิจ [Thansettakij]. <https://www.thansettakij.com/technology/668490>.

¹⁰⁶⁴ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) [Digital Government Development Agency]. (2025). ประชาพิจารณ์ (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) เพื่อเป็นกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ ตามนโยบายการใช้คลาวด์เป็นหลัก [Public Hearing on Draft Digital Government Standards as a Framework for Government Cloud Management under the Cloud-First Policy]. <https://standard.dga.or.th/35031/>.

draft provider standard, applicants seeking qualification would need to be legal entities established under Thai law, although an applicant may act as an authorized representative or distributor of an underlying cloud service provider. Providers seeking qualification for the highest tier would also have to meet requirements concerning sovereign or hybrid cloud services.

Separately, the National Cyber Security Committee's Cloud Security Standard B.E. 2567 took effect on September 10, 2026.¹⁰⁶⁵ The standard applies to cloud use by government agencies, regulatory or supervisory agencies, and Critical Information Infrastructure organizations and, through contractual requirements, to public cloud service providers serving those entities. National Cyber Security Agency guidance states that covered cloud providers must maintain a primary data center in Thailand and a backup data center in Thailand or specified nearby regional locations. For systems assessed as high impact, use of a cloud service with a primary data center in Thailand is required, although an exception process is available in specified circumstances. Foreign cloud service providers are not categorically excluded, but covered customers must contractually require their providers to comply with the applicable standard.

Despite the policy intent of increasing cloud adoption and accelerating digital transformation, the proposed guidelines 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.

Government-Imposed Content Restrictions and Related Access Barriers

CCIA has previously raised concerns with the Computer Crime Act, amended in 2016.¹⁰⁶⁶ 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

¹⁰⁶⁵ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ [National Cyber Security Committee of Thailand]. (2024, September 10). ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ [Notification on Cloud System Cybersecurity Standards, B.E. 2567 (2024)], ราชกิจจานุเบกษา [Royal Gazette], Vol. 141, Special Part 248. <https://ratchakitcha.soc.go.th/documents/43184.pdf>.

¹⁰⁶⁶ 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>.

Act, which has been leveraged to expand oversight of content and identify millions of posts.¹⁰⁶⁷ 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 July 2026, the Ministry of Digital Economy and Society issued a notification under Section 20 of the Computer Crime Act establishing an expedited procedure for government applications to a court to suspend dissemination of or remove computer data in cases of “urgent necessity.”¹⁰⁶⁸ The notification was published on July 17, 2026, and took effect the following day. It permits designated officials to seek expedited court orders where delay in suppressing the relevant data may affect specified interests, including national security, religion, the monarchy, good morals, social culture, or public order. The notification expands the circumstances in which the government may seek accelerated judicial removal of online content.

In August 2026, Thailand’s National Cyber Security Committee released proposed amendments to the Cybersecurity Act that would further expand the law’s potential impact on U.S. technology suppliers.¹⁰⁶⁹ Among other provisions, the draft would expand cyber-incident reporting requirements to additional private-sector entities and would designate external service providers including cloud, enterprise software, AI, outsourcing, and other technology providers as Critical Information Infrastructure organizations, subjecting them to indirect regulatory oversight. Covered organizations would be required to monitor their external providers for compliance with prescribed cybersecurity requirements, and providers that fail to remedy alleged noncompliance could be identified to government agencies, supervisory authorities, and CII organizations and face discontinuation of their services. The proposed framework raises concerns regarding due process, regulatory transparency, and market access for foreign technology suppliers, particularly where providers may be effectively excluded from customers or public-sector opportunities without an adequate opportunity to contest a finding of noncompliance.

The amended Emergency Decree on Measures for the Prevention and Suppression of Cybercrimes took effect on April 13, 2025 and established a liability framework for certain service providers, including online platforms, in connection with technology-enabled fraud.¹⁰⁷⁰

¹⁰⁶⁷ 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>.

¹⁰⁶⁸ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม [Ministry of Digital Economy and Society of Thailand]. (2026, July 17). ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง การยื่นคำร้องต่อศาลขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ ในกรณีที่มีเหตุจำเป็นเร่งด่วน พ.ศ. ๒๕๖๔ [Notification on Applying to the Court for an Order to Suspend Dissemination of or Delete Computer Data from a Computer System in Cases of Urgent Necessity, B.E. 2569 (2026)], ราชกิจจานุเบกษา [Royal Gazette], Vol. 143, Special Part 176. <https://ratchakitcha.soc.go.th/documents/120935.pdf>.

¹⁰⁶⁹ Tilleke & Gibbins. (2025, August 1). Major Draft Amendments to Thai Cybersecurity Act Released for Public Hearing.

<https://www.tilleke.com/insights/major-draft-amendments-to-thai-cybersecurity-act-released-for-public-hearing/>

¹⁰⁷⁰ Rajah & Tann Asia. (2025, April 28). New Regulation on Technology Crimes. <https://www.rajahtannasia.com/viewpoints/new-regulation-on-technology-crimes/>.

Online platforms may be required to share responsibility for losses where they fail to comply with regulator-prescribed fraud-prevention standards.

In May 2026, the Electronic Transactions Commission issued the Notification on Measures for Prevention of Technology Crime for Online Social Media (No. 2), which is scheduled to take effect on November 1, 2026.¹⁰⁷¹ The notification requires covered social media service providers that receive advertising payments to verify advertisers' identities, including with biometric linkage before publishing advertisements, subject to specified rules concerning prior verification, and to retain prescribed advertiser information for at least 90 days following the end of the advertising period. Where advertising fees are paid by a third party, specified information concerning the payer must also be retained. The notification forms part of the fraud-prevention framework under the Emergency Decree on Measures for the Prevention and Suppression of Technological Crimes.

In December 2025, Thailand enacted amendments to its Penal Code establishing new offenses for sexual harassment, including conduct occurring through computer systems or electronic devices, and creating new content-removal obligations for online services.¹⁰⁷² Under Section 284/4, where online sexual harassment involves certain publicly accessible obscene data, a court may order a computer system controller or service provider to suspend dissemination and remove the content within a specified period. Failure to comply with such an order may result in criminal penalties. In January 2026, Thailand's judiciary launched an expedited online process through which victims can seek these takedown orders. While the judicial oversight incorporated into the framework provides safeguards not present in some other Thai content-removal mechanisms, U.S. online services may nevertheless face additional compliance and legal exposure. Thailand should ensure that implementing procedures provide clear definitions, appropriate notice, reasonable compliance periods, and proportionate liability for intermediaries acting on court orders.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

¹⁰⁷¹ กรมประชาสัมพันธ์ [Government Public Relations Department of Thailand]. (2026, June 11). ยกระดับความปลอดภัยทางดิจิทัล: มาตรการป้องกันอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) [Raising Digital Safety: Measures for the Prevention of Technology Crime (No. 2)]. <https://www.prd.go.th/th/content/category/detail/id/31/iid/511206>.

¹⁰⁷² พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ ๓๐) พ.ศ. ๒๕๖๘ [Act Amending the Penal Code (No. 30), B.E. 2568 (2025)]. (2025, December 29). ราชกิจจานุเบกษา [Royal Gazette], Vol. 142, Part 90 ก. <https://ratchakitcha.soc.go.th/documents/94160.pdf>

Thailand has been considering a dedicated regulatory framework for over-the-top (OTT) and online streaming platforms.¹⁰⁷³ Government proposals under consideration include requirements for foreign platforms serving Thai users to obtain licenses and submit to Thai regulatory jurisdiction, additional content and identity-verification requirements, privacy obligations, competition-related restrictions, and measures intended to promote domestic platform providers. The government has also considered requiring OTT platforms earning revenue from Thai users to pay tax in Thailand. Depending on their final design, these measures could impose significant new market-access and operational burdens on foreign digital services suppliers and should be developed through transparent consultation and applied in a non-discriminatory manner.

Challenges to AI Development

In July 2026, ETDA published a draft Artificial Intelligence Act for public consultation.¹⁰⁷⁴ The consultation closed on August 14, 2026, and the draft has yet to be introduced in the Thai National Assembly. The draft would apply to AI developers, providers, deployers, and platform operators, including specified offshore entities, and would establish restrictions and obligations for certain prohibited and high-risk AI systems, transparency requirements for specified AI uses and AI-generated content, and regulatory enforcement powers. The draft also contemplates specific requirements for AI vendors serving government agencies or Critical Information Infrastructure organizations, including contractual and data-location requirements. This draft AI Act introduces sovereignty requirements for AI services: invoking national strategic autonomy, regulators can dictate the contract terms of AI and data processing services supplied to government and critical infrastructure, require those services to be processed inside Thailand, and obtain court orders to access providers' technical documentation and training data. Foreign providers of high-risk systems must also establish an in-country presence, and providers and deployers face joint liability for AI-related damage regardless of fault — stricter than any regime in the region and in key respects stricter than the EU. The combined effect favors domestic providers. USTR should engage with Thailand to press for the elimination of unreasonable and/or discriminatory policies.

Restrictions on Cross-Border Data Flows

The principal substantive provisions of Thailand's Personal Data Protection Act (PDPA) went into effect on June 1, 2022.¹⁰⁷⁵ On February 17, 2026, a regulation establishing a formal process

¹⁰⁷³ The Legal Co., Ltd. (2026, June 9). NBTC's Third Broadcasting and Television Master Plan (2026–2030): Expanded Oversight of OTT Platforms and the Future of Digital Broadcasting. <https://thelegal.co.th/2026/06/09/nbtcs-third-broadcasting-and-television-master-plan-2026-2030-expanded-oversight-of-ott-platforms-and-the-future-of-digital-broadcasting/>.

¹⁰⁷⁴ Baker McKenzie. (2026, July). Thailand: Draft AI Act – Seven Key Implications. <https://www.bakermckenzie.com/en/insight/publications/2026/07/thailand-draft-ai-act--seven-key-implications>.

¹⁰⁷⁵ Phakdeetham, J. (2022, June 1). Explainer: What is PDPA, Thailand's new data law? *Bangkok 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.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?)

for the examination and certification of Binding Corporate Rules took effect, providing a mechanism for qualifying intra-group cross-border transfers, and the PDPC has subsequently approved BCRs in practice. Separately, members of the House of Representatives introduced draft amendments to the PDPA concerning government entities and legal bases for processing; public consultation ran from July 16 through August 15, 2026. Those proposed amendments do not alter Section 5's territorial-scope rules.

Other Barriers to Digital Trade

Under Electronic Transactions Commission (ETC) Notification No. 2 on Prevention of Technology Crime for Online Social Media (published in the Royal Gazette May 5, 2026; mandatory from November 1, 2026), social media platforms must verify the identity of every advertiser before an ad is published — using either a government-issued reference standard or a certified digital verification system — and retain the advertiser's identity and contact information for at least 90 days after the advertising relationship ends, with annual re-verification required. The requirement currently applies to social media advertising specifically rather than e-commerce marketplaces generally, but is a precedent worth monitoring for extension.

ETDA issued a voluntary guideline (Announcement No. THPD 3/2569, September 2026) directing marketplace platforms to disclose a consolidated "Total Take Rate" combining all platform fees, with advance notice required before fee changes take effect and a calculator tool to be made available to sellers. The guideline is voluntary for now, but ETDA has indicated it may be codified as a binding requirement under a forthcoming Digital Platform Services Law if industry compliance is deemed insufficient. Industry has urged that any future codification include objective, bright-line criteria for distinguishing "additional service" fees from "basic" fees, a quantified trigger for mandatory fee-increase warnings rather than an undefined "significant impact" standard, and a reasonable phase-in period before mandatory compliance.

Threats to the Security of Devices and Services

Thailand is developing a Draft Amendment to the Cybersecurity Act that would expand regulatory authority over decryption, monitoring, and real-time data access.¹⁰⁷⁶ As drafted, the

<https://www.pwc.com/th/en/tax/personal-data-protection-act.html>; Hunton. (2022, June 1). *Thailand's Personal Data Protection Act Enters into Force*.

<https://www.huntonprivacyblog.com/2022/06/01/thailands-personal-data-protection-act-enters-into-force/>.

¹⁰⁷⁶ Thailand National Assembly. (2026) *Draft Cyber Security Act*.

https://law.go.th/listeningDetail?survey_id=NzM2N0RH0V9MOVdfRIJPTIRFTkO=.

amendment would grant officials authority to compel any person to decrypt data pursuant to a court order, without providing a mechanism to challenge such an order; industry has raised concerns that this authority could create encryption backdoors and undermine end-to-end encryption and data security. The draft also would permit the authority to order monitoring of, or system access concerning, any person “connected with or affected by” a cyber threat without a court order, and to compel any person loosely connected to a serious or critical cyber threat to provide continuous, real-time data without a court order or right of appeal. These provisions, as currently drafted, would increase regulatory risk, uncertainty, and compliance costs for system owners and operators in Thailand. USTR should monitor the amendment’s development and encourage Thailand to narrow these authorities and incorporate judicial oversight and appeal mechanisms consistent with due process.

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.¹⁰⁷⁷ 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 obstruct U.S. services suppliers’ operations in Türkiye.¹⁰⁷⁸ The proposed amendments remain pending in 2026; in the meantime, digital-market competition issues continue to be governed by the existing provisions of Law No. 4054.

Separate restrictions arise under Law No. 6563¹⁰⁷⁹ and its e-commerce-focused implementing regulation, entered into force on January 1, 2023. The framework generally prohibits intermediary platforms from selling their own branded goods and imposes additional obligations

¹⁰⁷⁷ 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>.

¹⁰⁷⁸ 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>; and

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>.

¹⁰⁷⁹ Sozer, C. (2023, January 2). *New E-Commerce Regulation Published*. Esin. <https://www.esin.av.tr/2023/01/02/24398/>.

according to transaction volume. For 2026, the medium-scale net transaction-volume threshold is TRY 79,180,975,103 (approximately US\$1.62 billion), triggering restrictions on intermediary platforms' use of seller and buyer data to compete with third-party sellers. The very-large-scale threshold is TRY 475,085,850,615 (approximately US\$9.73 billion), together with more than 100,000 transactions annually, triggers additional restrictions involving payment services and delivery operations. Qualifying providers also face licensing obligations. These requirements significantly constrain common business models and increase compliance costs for U.S. suppliers.

On June 5, 2026, the Turkish Competition Authority issued interim measures against Meta, alleging that the integration of first-party AI features with messaging services constitutes unlawful data tying and anti-competitive foreclosure. The Turkish Competition Authority ordered the platform to provide unhindered economic and technical access to third-party AI developers within 30 days.¹⁰⁸⁰ Forcing digital platforms to share infrastructure and unbundle proprietary AI models severely restricts U.S. technology exporters from deploying integrated AI features in Türkiye. CCIA urges USTR to raise these *ex-ante* AI access mandates during bilateral trade discussions.

Customs-Related Restrictions and Import Barriers for Goods

Effective February 6, 2026, Presidential Decision No. 10813 removed simplified customs clearance for ordinary B2C e-commerce imports valued at €30 or less. These shipments now require regular customs declarations and compliance with applicable import requirements, increasing processing costs and potential delays for cross-border sellers and platforms.

Discriminatory Local Content Quotas and Audiovisual Service Mandates

An omnibus signed into law on July 30, 2026, creates a new annual financial contribution obligation on subscription video services licensed under the Broadcasting Law (Law No. 6112).¹⁰⁸¹ Covered platforms, including licensed streaming services such as AMP, Netflix, Disney+, Amazon Prime Video, BluTV, Exxen, Gain, and MUBI, and internet platform operators such as Spotify, would contribute 2% of their annual net sales revenue in Türkiye to the Ministry of Culture and Tourism's Cinema Support Fund, with the President authorized to adjust the rate between 1% and 4%. The contribution is turnover-based, regardless of profitability, with the Ministry authorized to request platform revenue information. This turnover-based,

¹⁰⁸⁰ Rekabet Kurulu [Turkish Competition Board]. (2026, June 5). Meta Platforms, Inc., Meta Platforms Ireland Limited, WhatsApp LLC ve Meta Platforms İstanbul Bilişim Hizmetleri Ltd. Şti., Decision No. 26-18/536-193, as reported in Alomaliye, Rekabet Kurulu'ndan Meta Kararı: Soruşturma Açıldı, Geçici Tedbir Uygulanacak (2026, June 5).

<https://www.alomaliye.com/2026/06/05/rekabet-kurulundan-meta-karari-sorusturma-acildi-gecici-tedbir-uygulanacak>.

¹⁰⁸¹ Türkiye National Assembly. (2026) *Draft Law 2/3764*.

<https://www.tbmm.gov.tr/Yasama/KanunTeklifi/da9978b9-5655-4725-8ffa-019f273b6db5>

profitability-independent contribution raises trade concerns as a discriminatory, sector-specific burden on foreign streaming and platform operators; USTR should monitor potential movement on this proposal.

Forced Revenue Transfers for Digital News

A bill submitted on February 10, 2026 would require covered digital platforms to negotiate and pay remuneration for economically valuable uses of online news, including previews and summaries.¹⁰⁸² Enhanced obligations would apply to platforms exceeding TRY 100 million in annual Türkiye-sourced digital-service revenue or one million average monthly active users. The proposal includes restrictions on reducing news visibility during negotiations, algorithmic reporting, local representation, and revenue-based penalties. These measures could impose additional costs and constrain U.S. platforms' content-ranking decisions. The bill remains under discussion in the parliamentary committee and warrants ongoing monitoring.

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.¹⁰⁸³ CCIA has previously identified laws that preemptively block websites on vague grounds and specific instances of blocking by Turkish authorities.¹⁰⁸⁴ On September 7-8, 2025, access to X, YouTube, Instagram, Facebook, TikTok, and WhatsApp was restricted across multiple Turkish networks amid political unrest. NetBlocks reported that access was restored approximately one day after the restrictions began. The USITC estimated that disruptions to U.S. social-media and user-generated-video services caused US\$14.6 million in losses to Türkiye's economy in 2020.¹⁰⁸⁵

¹⁰⁸² Grand National Assembly of Türkiye. (2026). *Digital Copyright and Online News Content Law Proposal*. <https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y4/T2/WebOnergeMetni/b7006396-020f-42b1-8739-c472cec6019d.pdf>.

¹⁰⁸³ Freedom House. (2023). *Freedom on the Net 2023: Türkiye*. <https://freedomhouse.org/country/turkey/freedom-net/2023>.

¹⁰⁸⁴ 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-Turkiye/>; 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/Turkiye-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://Turkeyblocks.org/2017/06/05/major-internet-access-issues-Turkiye-cloudflare-knocked-offline/>;

¹⁰⁸⁵ 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>.

Law No. 7418 expanded these obligations in October 2022 and introduced a criminal disinformation offense.¹⁰⁸⁶ It permits regulatory demands for information about algorithms and data-processing mechanisms and requires disclosure of information identifying users implicated in specified criminal offenses. Depending on the breach, sanctions include fines of up to 3% of the preceding calendar year's global turnover and court-ordered bandwidth restrictions reaching 90%.

Law No. 7578, published on May 1, 2026, introduces additional requirements effective November 1, 2026.¹⁰⁸⁷ Social network providers must prevent access by children under 15, implement age-verification measures, and provide parental controls. Platforms are barred from using industry-standard, risk-based age assurance and must verify all new and existing users exclusively via Türkiye's state portal (e-Devlet). Because e-Devlet cannot automate transfers to third-party credential tools, users must manually generate and upload a state token.¹⁰⁸⁸ Platforms must build a bespoke teen architecture and cross-OS, Turkish-language parental controls (governing screen time and spending).¹⁰⁸⁹ Providers exceeding ten million daily accesses from Türkiye must implement specified emergency content-removal orders within one hour and prevent republication of content covered by relevant orders.

The law also introduces age-rating and parental-control requirements for gaming platforms. Foreign gaming platforms exceeding 100,000 daily accesses from Türkiye must appoint a local representative. Unrated games may be offered under an adult rating. Persistent noncompliance can trigger escalating fines of up to 3% of global turnover and court-ordered bandwidth reductions ranging from 50%-90%, creating additional compliance costs and service-disruption risks.¹⁰⁹⁰

¹⁰⁸⁶ ELIG Gürkaynak Attorneys-at-Law. (2022, October 28). *Law No. 7418 on Amendment of Press Law and Certain Laws is Published*. <https://www.gurkaynak.av.tr/Content/dosya/1507/law-no-7418-on-amendment-of-press-law-and-certain-laws-is-published-32865-17977.pdf>

¹⁰⁸⁷ Paksoy. (2026, July 22). Dijital oyun platformları için yeni dönem: 5651 sayılı Kanun'da kritik değişiklikler [A New Era for Digital Game Platforms: Critical Changes to Law No. 5651]. <https://paksoy.av.tr/2026/07/dijital-oyun-platformlari-icin-yeni-donem-5651-sayili-kanunda-kritik-degisiklikler/>

¹⁰⁸⁸ İfade Özgürlüğü Derneği [Freedom of Expression Association]. (2026, October 13). Uyardığımız gün geldi: 1 Kasım'dan itibaren kimliksiz sosyal medya yok [The day we warned about has come: from 1 November, no social media without ID]. <https://ifade.org.tr/basin-bultenleri-ve-duyurular/uyardigimiz-gun-geldi-1-kasimdan-ibaren-kimliksiz-sosyal-medya-yok>.

¹⁰⁸⁹ Kaya, M. B. (2026, October 10). Sosyal medyada çocukların korunması ve yaş doğrulama (15 yaş sınırı düzenlemesi) [Protection of children on social media and age verification (the 15-year age limit regulation)], arts. 8–9. mbkaya.com. <https://mbkaya.com/sosyal-medya-cocuk-yas-dogrulama-yonetmeli-sgb>.

¹⁰⁹⁰ İfade Özgürlüğü Derneği [Freedom of Expression Association]. (2026, October 13). Uyardığımız gün geldi: 1 Kasım'dan itibaren kimliksiz sosyal medya yok [The day we warned about has come: from 1 November, no social media without ID]. <https://ifade.org.tr/basin-bultenleri-ve-duyurular/uyardigimiz-gun-geldi-1-kasimdan-ibaren-kimliksiz-sosyal-medya-yok>.

Law No. 7590, effective July 31, 2026, transferred internet-content enforcement and supervision of social-network and gaming-platform obligations from the ICTA to the Cybersecurity Directorate.¹⁰⁹¹ The Directorate may also require operators, access providers, data centers, and content and hosting providers to implement specified urgent measures within two hours.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Türkiye maintains data-localization requirements for specified public-sector data and regulated financial activities, restricting the use of global cloud infrastructure. USTR reports that payment-sector localization requirements led to at least one prominent U.S. supplier to suspend operations in Türkiye.¹⁰⁹²

Presidential Circular No. 2019/12,¹⁰⁹³ published on July 6, 2019, requires domestic storage of critical information and data, including population, health, communications, genetic, and biometric records. It also prohibits public institutions from storing data in cloud services other than their own private systems or domestic service providers under their control. The Information and Communication Security Guide implements the Circular for public institutions and critical-infrastructure service providers. These requirements restrict the use of global cloud services.

The Regulation on Banks' Information Systems and Electronic Banking Services, published on March 15, 2020, requires banks to maintain their primary and secondary information systems in Türkiye. Outsourcing and cloud arrangements supporting those systems must comply with the regulation's domestic-hosting requirements.¹⁰⁹⁴

Law No. 6493¹⁰⁹⁵ and its implementing rules require licensed payment and electronic-money institutions to be established as Turkish joint-stock companies and meet applicable capital and own-funds requirements. Effective June 30, 2026, minimum funds are TRY 20 million for bill-payment-only institutions, TRY 40 million for other covered payment institutions, and TRY 105 million for electronic-money institutions. Account-information-only institutions are exempt from the payment-institution minimum.

¹⁰⁹¹ Küstür, S. (2026, July 31). BTK'nın internet yetkileri SGB'ye geçti [BTK's Internet Powers Have Passed to the Cybersecurity Directorate]. Teknoblog. <https://www.teknoblog.com/btk-nin-internet-yetkileri-sgb-ye-gecti/>.

¹⁰⁹² U.S. Department of State. (2024). *2024 Investment Climate Statement: Turkey*. <https://www.state.gov/reports/2024-investment-climate-statements/turkey/>.

¹⁰⁹³ *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>.

¹⁰⁹⁴ 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>.

¹⁰⁹⁵ *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>.

Records relating to activities covered by the law must be retained domestically for at least ten years. Implementing rules require domestic hosting of primary and secondary systems, including relevant outsourced payment-processing systems. Since October 2023, necessary and proportionate data sharing for customer-requested cross-border payments has been permitted where one party is abroad, subject to continued domestic storage and applicable personal-data transfer rules. These requirements constrain global infrastructure arrangements and raise entry costs for foreign suppliers. Operating without the required license can expose responsible individuals to imprisonment of one to three years and judicial fines.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

Law No. 7418 amended the Electronic Communications Law to bring OTT communications services within the ICTA's authorization and supervisory powers.¹⁰⁹⁶ The framework provides for local establishment and sanctions for unauthorized provision, including fines, bandwidth restrictions reaching 95%, and eventual access blocking.

On March 21, 2025, the ICTA published draft implementing measures addressing authorization, service scope, and notification requirements. The proposals would generally require providers with at least one million monthly unique users to obtain authorization through a Turkish company, pay authorization fees, and contribute to universal service funding. Exemptions would apply to certain services where interpersonal communication is ancillary. The proposals also contemplate reporting and other operator obligations. These requirements would increase the cost of supplying communications services across borders and impose additional burdens on U.S. providers.

Restrictions on Cross-Border Data Flows

Türkiye substantially revised Article 9 of the Personal Data Protection Law in 2024,¹⁰⁹⁷ introducing a framework based on adequacy decisions, appropriate safeguards, and limited derogations. Available safeguards include standard contracts, approved binding corporate rules, and Board-approved undertakings. Standard contracts do not require prior Board approval but must be notified to the authority within five business days of signature. January 2025 guidance clarified these mechanisms and confirmed that remote access from abroad can constitute an international transfer. These reforms facilitate cross-border processing, although Turkish contractual and notification requirements and separate sectoral localization rules continue to create compliance burdens.

¹⁰⁹⁶ Necipoğlu, C. (Pekin & Pekin). (2025, April 4). OTT Hizmet Sağlayıcılar için Yetkilendirme Zorunluluğu [Authorization Requirement for OTT Service Providers].

<https://pekin.com.tr/2025/04/04/ott-hizmet-saglayicilar-icin-yetkilendirme-zorunlulugu/>.

¹⁰⁹⁷ *Law on the Protection of Personal Data* [Türkiye] No. 6698. (2016).

<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aea97a33-089b-4e7d-85cb-694adb57bed3.pdf>.

Taxation of Digital Products and Services

Türkiye's DST, originally introduced at 7.5% on March 1, 2020, was reduced to 5% for revenues generated from January 1, 2026 under Presidential Decision No. 10767. A further reduction to 2.5% is scheduled for January 1, 2027. The revenue thresholds for covered digital services are €750 million worldwide and TRY 20 million in Türkiye, meaning that the measure disproportionately targets U.S. firms. 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."¹⁰⁹⁸ Foreign providers exceeding the Turkish revenue threshold but claiming exemption because their worldwide covered revenue remains below the global threshold must substantiate that exemption through an independent audit report.¹⁰⁹⁹ In November 2021, Türkiye and the United States agreed to a temporary arrangement governing the transition from the DST to the OECD's Pillar One framework. Given the moribund status of Pillar 1, and USTR's 301 finding of the tax's unreasonable and discriminatory burden on U.S. firms, USTR should refresh the record of its finding and consider further steps necessary to remove this barrier.

Law No. 7524 amended Türkiye's income- and corporate-tax legislation to require covered intermediaries to withhold tax on payments to sellers and service providers for e-commerce transactions.¹¹⁰⁰ Presidential Decision No. 9284 set the rate at 1%, effective January 1, 2025. Communiqué No. 330 generally applies withholding to gross sales or service payments excluding VAT and accommodation tax, without deducting platform commissions. Although creditable against the recipient's income or corporate tax, the requirement adds collection, reporting, and reconciliation burdens for covered platforms.

¹⁰⁹⁸ 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>.

¹⁰⁹⁹ KPMG. (2020). *Türkiye: Digital Services Tax, A Primer*.
https://kpmgvergi.com/Content/Service/Pdf/DijitalHizmetVergisiDanismanligi16112020_081732365687.pdf.

¹¹⁰⁰ PwC Türkiye. (2024, December 31). Elektronik Ticarete Hizmet Sağlayıcılarına Yapılan Ödemelerde Tevkifatla İlgili Tebliğ [Communiqué on Withholding on Payments Made to Service Providers in Electronic Commerce] (Vergi Bülteni 2024/74).
<https://www.pwc.com.tr/tr/hizmetlerimiz/vergi/bultenler/2024/elektronik-ticarete-hizmet-saglayicilarina-yapilan-odemelerde-tevkifatla-ilgili-teblig.html>.

Other Barriers to Digital Trade

Digital Copyrights Bill, No. 2/3417, introduced on December 11, 2025, remains in committee. It would require covered intermediaries to deploy automated copyright-recognition systems, prevent or remove infringements, conduct licensing negotiations, and report on enforcement and revenue sharing.¹¹⁰¹ Enhanced obligations would apply above 250,000 average daily unique users or a revenue threshold to be set by the proposed regulator. These requirements could increase compliance costs for U.S. platforms.

An e-commerce regulation effective January 1, 2023¹¹⁰² requires marketplaces to remove product listings within 48 hours after receiving a qualifying intellectual-property complaint and notify the seller and right holder. Where the seller submits a properly supported objection establishing its merits, the marketplace must restore the listing within 24 hours. Repeat complaints concerning the same product and claim require new information or documents. Judicial and administrative remedies remain available.

A Constitutional Court decision published on June 2, 2026 annulled the e-commerce intermediary liability exemption in Article 9(1) of Law No. 6563 insofar as it applies to consumer contracts, together with a related limitation concerning defective-goods claims.¹¹⁰³ The annulments take effect nine months after publication, on March 2, 2027, increasing prospective liability exposure for online marketplaces.

Bill No. 2/3803, submitted on August 10, 2026 and pending in committee, would establish a separate authorization regime for foreign digital accommodation platforms.¹¹⁰⁴ It proposes a TRY 5 million fee for a two-year permit, local representation, a 17% ceiling on platform charges, and tourism-promotion contributions. Platforms operating without a valid permit could face access blocking. These requirements would create additional entry and operating restrictions for foreign suppliers.

¹¹⁰¹ Türkiye Büyük Millet Meclisi [Grand National Assembly of Türkiye]. (2025, December 11). Dijital Telif Hakları Kanun Teklifi (2/3417) [Digital Copyrights Law Proposal]. <https://www.tbmm.gov.tr/Yasama/KanunTeklifi/a42a07fd-169f-4802-a27d-019b0c8059bd>.

¹¹⁰² 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>.

¹¹⁰³ Esin Attorney Partnership. (2026, June 25). Anayasa Mahkemesi'nden E-ticaret Sektörü İçin Önemli İptal Kararı [An Important Annulment Decision from the Constitutional Court for the E-Commerce Sector]. <https://www.esin.av.tr/tr/2026/06/25/anayasa-mahkemesinden-e-ticaret-sektoru-icin-onemli-iptal-karari/>

¹¹⁰⁴ Türkiye Büyük Millet Meclisi [Grand National Assembly of Türkiye]. (2026, August 10). Yabancı Dijital Konaklama Platformları Kanunu Teklifi (2/3803) [Foreign Digital Accommodation Platforms Law Proposal]. <https://www.tbmm.gov.tr/Yasama/KanunTeklifi/e17a32b2-7929-4ed2-8a2c-019febe41323>

Amendments to the Commercial Advertising and Unfair Commercial Practices Regulation took effect on August 1, 2026.¹¹⁰⁵ Covered targeted advertising must explain the targeting criteria and how consumers can change them; profiling-based targeting is prohibited where the consumer is known or reasonably understood to be a child. Specified uses of AI in advertising require disclosure, including realistic synthetic characters. These rules add transparency and advertising-design requirements for covered platforms.

Implementation of Cybersecurity Law No. 7545 advanced on May 5, 2026, when the Cybersecurity Council designated 15 critical-infrastructure sectors, including digital infrastructure, digital services, and electronic communications.¹¹⁰⁶ The law establishes a preference for domestic and national cybersecurity products and requires cybersecurity products, systems, and services used by public institutions and critical infrastructure to be procured from Directorate-authorized and certified suppliers. These provisions can constrain procurement opportunities for U.S. cybersecurity suppliers and add authorization and certification burdens.

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.¹¹⁰⁷ While the Act does not explicitly subject companies to data localization requirements, the Bank of Uganda has interpreted it to require 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.

On February 20, 2026, Uganda's Personal Data Protection Office ordered WhatsApp to submit an assessment of protections and safeguards for international data transfers and a data protection impact assessment covering intra-group sharing within 90 days.¹¹⁰⁸ These requirements impose

¹¹⁰⁵ T.C. Ticaret Bakanlığı [Ministry of Trade of the Republic of Türkiye]. (2026, July 27). Aldatıcı Reklam ve Haksız Ticari Uygulamalarla Mücadelede Yeni Dönem Başlıyor [A New Era Begins in Combating Deceptive Advertising and Unfair Commercial Practices].

<https://ticaret.gov.tr/haberler/aldaticici-reklam-ve-haksiz-ticari-uygulamalarla-mucadelede-yeni-donem-basliyor>

¹¹⁰⁶ Türkiye Büyük Millet Meclisi [Grand National Assembly of Türkiye]. (2025, March 19). 7545 sayılı Siber Güvenlik Kanunu [Cybersecurity Law No. 7545]. Resmî Gazete No. 32846.

<https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm>

¹¹⁰⁷ Republic of Uganda. (2011). *Computer Misuse Act, Chapter 96*, sections 31(5)(c) and 33.

<https://www.nita.go.ug/sites/default/files/2026-09/Computer%20Misuse%20Act%20Cap%2096.pdf>

¹¹⁰⁸ Personal Data Protection Office. (2026, February 20). *Decision in Adlegal International Limited v. WhatsApp LLC and Meta Platforms, Inc., Complaint No. PDPO 086/2025*.

<https://adlegalug.com/wp-content/uploads/2026/02/PDPO-Decision-in-Ad-legal-International-Ltd-v-WhatsApp-LLC-Meta-Platforms-Inc.pdf>

additional compliance obligations on cross-border digital services. In July 2026, the regulator confirmed that WhatsApp had implemented the required corrective measures.¹¹⁰⁹

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, 2023.¹¹¹⁰ 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. Covered U.S. digital services providers face the DST from their first dollar of taxable revenue because the regime has no minimum revenue threshold. The Income Tax (Amendment) Act, 2026, effective July 1, 2026, expressly includes software in the definition of royalties and excludes royalty income from the DST.¹¹¹¹ Payments classified as royalties instead fall under the applicable royalty withholding-tax rules.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

On January 13, 2026, the Uganda Communications Commission ordered an internet shutdown ahead of the January 15 elections.¹¹¹² General internet access was restored on January 18, while social media and messaging applications remained restricted.¹¹¹³ On January 26, the Commission announced full restoration of internet services.¹¹¹⁴ Such shutdowns interrupt access to cross-border digital services and undermine the predictability of market access for U.S. suppliers.

¹¹⁰⁹ Business Times. (2026, July 29). *WhatsApp Updates Privacy Policies After Uganda Data Protection Enforcement*.

<https://businesstimesug.com/whatsapp-updates-privacy-policies-after-uganda-data-protection-enforcement/>

¹¹¹⁰ Balaba, E. (2026, March 10). *Heightened Enforcement of Digital Services Tax and VAT on Electronic Services in Uganda*. ALN.

<https://aln.africa/insight/heightened-enforcement-of-digital-services-tax-and-vat-on-electronic-services-in-uganda/>

¹¹¹¹ Republic of Uganda. (2026). *Income Tax (Amendment) Act, 2026*, sections 1, 2, and 8.

<https://mrt.tax/wp-content/uploads/2026/08/The-Income-TaxAmendment-Act-2026.pdf>

¹¹¹² Human Rights Watch. (2026, January 15). *Uganda: Blanket Internet Shutdown Violates Rights*.

<https://www.hrw.org/news/2026/01/15/uganda-blanket-internet-shutdown-violates-rights>

¹¹¹³ Uganda Communications Commission. (2026, January 18). *Press Briefing by the Executive Director, Uganda Communications Commission on the Restoration of Public Internet Access*.

<https://www.ucc.co.ug/wp-content/uploads/2026/01/PRESS-BRIEFING-BY-THE-EXECUTIVE-DIRECTOR-UGANDA-COMMUNICATIONS-COMMISSION-ON-THE-RESTORATION-OF-PUBLIC-INTERNET-ACCESS-%E2%80%93-18TH-JANUARY-2026-.pdf>

¹¹¹⁴ Monitor Reporter. (2026, January 26). *Uganda Announces Full Internet Restoration After Tense Polls*. Daily Monitor.

<https://www.monitor.co.ug/uganda/news/national/uganda-announces-full-internet-restoration-after-tense-polls-5338692>

On March 17, 2026, Uganda's Constitutional Court annulled the Computer Misuse (Amendment) Act, 2022, because Parliament had failed to comply with constitutional quorum requirements.¹¹¹⁵ The decision removed provisions criminalizing, among other activities, sharing unsolicited or malicious information and misuse of social media. The Attorney General subsequently advised against an appeal and directed that enforcement of the nullified provisions cease;¹¹¹⁶ the remaining provisions of the Computer Misuse Act continue in force.

Ukraine

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Following Russia's full-scale invasion in February 2022, Ukraine adopted emergency measures permitting public authorities to use cloud infrastructure abroad and allowing banks to use qualifying foreign cloud services.¹¹¹⁷ These measures enabled Ukrainian government entities to work with U.S. cloud service providers. However, the framework for hosting covered state information resources abroad remains temporary, extending through martial law and six months after its termination or cancellation, creating uncertainty over continued cross-border hosting. Cabinet Resolution No. 154 of February 11, 2025 established cloud-provider requirements and a public-sector contracting framework. Resolution No. 1691 of December 17, 2025 extended through December 31, 2026 the transition allowing public users to initiate procurement from providers not yet included in the official provider list.¹¹¹⁸ Resolution No. 1009 of August 6, 2026 expanded this permission to critical-infrastructure operators procuring for critical information infrastructure and to owners or managers of critical information infrastructure.¹¹¹⁹

Industry has raised concerns regarding: 1) remaining gaps in alignment between national requirements and international cloud-security compliance frameworks, notwithstanding the December 2025 amendments expressly recognizing ISO/IEC 27001, 27017, and 27018 standards;¹¹²⁰ 2) mandatory Ukrainian governing law and Ukrainian-court jurisdiction for

¹¹¹⁵ Committee to Protect Journalists. (2026, March 19). *Uganda Declares Criminal Defamation Unconstitutional, Strikes Down Cybercrime Law*.

<https://cpj.org/2026/03/uganda-declares-criminal-defamation-unconstitutional-strikes-down-cybercrime-law/>

¹¹¹⁶ Uganda Broadcasting Corporation. (2026, March 26). *Govt Drops Appeal on Computer Misuse Act Ruling, Opts to Return Law to Parliament*.

<https://ubc.go.ug/2026/03/26/govt-drops-appeal-on-computer-misuse-act-ruling-opts-to-return-law-to-parliament/>

¹¹¹⁷ 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>

¹¹¹⁸ Cabinet of Ministers of Ukraine. (2025, December 17). *Resolution No. 1691: On Amendments to Resolution No. 154 of February 11, 2025*. <https://zakon.rada.gov.ua/laws/show/1691-2025-%D0%BF>

¹¹¹⁹ Cabinet of Ministers of Ukraine. (2026, August 6). *Resolution No. 1009: Certain Issues of Ensuring the Continuity of Operation of State Information Resources*. <https://zakon.rada.gov.ua/laws/show/1009-2026-%D0%BF>

¹¹²⁰ American Chamber of Commerce in Ukraine. (2025, December 17). *Cabinet of Ministers Extended Transitional Period for Public Procurement of Cloud Services*. <https://chamber.ua/success-stories/cabinet-of-ministers-extended-transitional-period-for-public-procurement-of-cloud-services/>

cloud-service agreements serving public users and critical information infrastructure;¹¹²¹ 3) Article 4(3) of the Personal Data Protection Law, which restricts processors of personal data controlled by state or local authorities to those authorities and state- or municipally owned enterprises;¹¹²² and 4) obligations to re-localize certain categories of data to Ukraine that have been temporarily permitted to be stored abroad under martial law.¹¹²³

Taxation of Digital Products and Services

On June 9, 2026, Parliament adopted Bill No. 15111-ð, which taxes income earned through digital platforms.¹¹²⁴ As of September 2026, the measure is still awaiting presidential signature. The adopted text would impose registration, seller-information reporting, and tax-withholding obligations on covered platform operators, including nonresidents, and permit court-ordered access restrictions for failure to register. It specifies registration before January 1, 2027 and an initial reporting period covering 2027, with the first reports due in 2028.

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.¹¹²⁵ 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.

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.¹¹²⁶ 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

¹¹²¹ Verkhovna Rada of Ukraine. (2022, February 17). *Law No. 2075-IX: On Cloud Services*, Article 10(3). <https://zakon.rada.gov.ua/laws/show/2075-20>

¹¹²² Verkhovna Rada of Ukraine. (2010, June 1). *Law No. 2297-VI: On Personal Data Protection*, Article 4(3). <https://zakon.rada.gov.ua/laws/show/2297-17>

¹¹²³ Cabinet of Ministers of Ukraine. (2022, December 30). *Resolution No. 1500: Certain Issues of Ensuring the Functioning of State Information Resources*, paragraph 21 of the procedure governing transfers abroad. <https://zakon.rada.gov.ua/laws/show/1500-2022-%D0%BF>

¹¹²⁴ Verkhovna Rada of Ukraine. (2026, April 6). *Bill No. 15111-ð: Amendments to the Tax Code and Other Legislative Acts Concerning International Automatic Exchange of Information on Income Earned through Digital Platforms and Taxation of Such Income—Legislative Record*. <https://itd.rada.gov.ua/billinfo/Bills/Card/69816>

¹¹²⁵ 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/>

¹¹²⁶ United Arab Emirates Government. (2023, February 6). *National Cloud Security Policy*. <https://uaelegislation.gov.ae/en/policy/details/national-cloud-security-policy>

clearer compliance pathways for foreign CSPs seeking to serve government customers and regulated sectors.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

The UAE restricts unlicensed Voice over Internet Protocol (VoIP) services. The Telecommunications and Digital Government Regulatory Authority (TDRA) permits licensed operators to provide these services and allows third-party providers to operate through collaboration with a licensee or separate TDRA approval.¹¹²⁷ Operators must block unauthorized VoIP services. These licensing, approval, and blocking requirements constrain foreign providers' ability to offer internet calling services directly to UAE customers.

Following the January 31, 2026 compliance deadline, individuals conducting covered social-media advertising activities in the UAE must hold an Advertiser Permit, whether the promotion is paid or unpaid. Exemptions include individuals promoting their own products or services, or those of a company they own, through personal accounts. Visiting foreign advertisers must apply through an approved local advertising or talent-management agency; visitor permits last three months and may be extended to a maximum of six months. These permit and local-intermediary requirements create additional market-entry burdens for foreign creators.

In June 2026, the UAE adopted Cabinet Resolution No. 106 of 2026 regulating children's access to social media.¹¹²⁸ It prohibits personal accounts for children under 15 and requires additional safeguards for users aged 15 but under 16. Covered platforms must verify age rather than rely on self-declaration and disable accounts belonging to underage users. The resolution covers platforms available in the UAE or directed at UAE users and provides a twelve-month transition period from entry into force. These requirements will require affected foreign providers to adapt account-registration, verification, and moderation systems.

Federal Decree-Law No. 26 of 2025 on Child Digital Safety took effect on January 1, 2026 and applies to digital platforms operating in the UAE or targeting UAE users, extending beyond social media.¹¹²⁹ It requires risk-based age verification, parental controls, and parental consent before collecting personal data from children under 13. Existing platform operators have until January 1, 2027 to comply. These obligations require affected foreign suppliers to adapt their age-assurance, data-collection, and parental-control systems.

In addition to data restrictions, the Central Bank of the UAE (CBUAE) issued Notice No. 2058/2026 directing all Licensed Financial Institutions (LFIs) to immediately discontinue the use of instant messaging applications (explicitly naming WhatsApp Messenger) as a channel to

¹¹²⁷ Telecommunications and Digital Government Regulatory Authority. (n.d.). *FAQs*. <https://tdra.gov.ae/en/FAQs>

¹¹²⁸ United Arab Emirates Cabinet. (2026). *Cabinet Resolution No. (106) of 2026 on Regulating Children's Access to Social Media Platforms*. <https://uaelegislation.gov.ae/en/legislations/4506>

¹¹²⁹ United Arab Emirates Government. (2025). *Federal Decree by Law No. (26) of 2025 Regarding Child Digital Safety*. <https://uaelegislation.gov.ae/en/legislations/3912>

deliver financial services or share customer data.¹¹³⁰ The compliance reporting deadline was April 30, 2026. A directive that significantly restricts the use of messaging applications in financial services contexts risks creating friction not only for financial institutions, but for the broader ecosystem of businesses that rely on the platform to serve their customers efficiently and at scale.

United Kingdom

The United States and United Kingdom signed the Technology Prosperity Deal (TPD) in September 2025, but the United States paused implementation of the deal later that year amid broader trade disagreements. Cooperation subsequently resumed in some areas, including civil nuclear cooperation in January 2026, while other elements remained paused. The episode underscores the potential for unresolved trade barriers to complicate broader bilateral technology cooperation. The United States should seek to complete the TPD and build on that with a broader rules-based agreement that addresses concerns including those set out below.

Asymmetric Platform Regulation

On May 24, 2024, the Digital Markets, Competition and Consumers 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.¹¹³¹ Alongside changes to consumer protection and merger rules, the law allows the CMA to designate providers as having Strategic Market Status (SMS), imposing more intrusive obligations on a small set of firms, overwhelmingly U.S. headquartered. The resulting interventions include firm-specific Conduct Requirements (CRs) which can include regulation of prices and other commercial terms allowing the CMA to create transfers to domestic vested interests (including a final offer mechanism similar to the Australian news media bargaining code, but not limited by sector); requiring interoperability and data sharing; determining which services will be offered to consumers and how and when (e.g. choice screens) and imposing 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 Appeal Tribunal to judicial review only and while, in principle, the new law allows for a consideration of consumer benefits, this will be limited in

¹¹³⁰ Fintech News UAE. (2026, April 24). UAE Central Bank enforces WhatsApp banking ban over security risks. <https://fintechnews.ae/31346/security/uae-whatsapp-banking-ban-financial-services>.

¹¹³¹ Department for Business and Trade. (2024, September 9). Implementation of the Digital Markets, Competition and Consumers Act 2024 (Written statement HCWS74). <https://questions-statements.parliament.uk/written-statements/detail/2024-09-09/hcws74>.

important ways (*e.g.*, countervailing consumer benefits being used as a defense after a finding that a conduct requirement has been breached, versus at the outset).

Implementation of the regime has advanced materially. In October 2025, the CMA designated Google’s general search and search advertising services, and Apple’s and Google’s mobile platforms, as having “strategic market status.” In 2026, the CMA imposed two CRs on Google Search addressing how publishers interact with AI Overviews, and how Google ranks results. It is consulting on a further consultation response around choice screens. Commitments concerning Apple’s and Google’s app-store processes and Apple interoperability took effect in April 2026, and the CMA has also proposed further CRs on how Apple governs access to near-field communication technology and Apple and Google’s app store terms and conditions. These have not yet been finalized but would, as proposed, impose utility-style price regulation and see vital app store functions such as trust and safety technology, mandatorily shared and unremunerated.

The CMA has since launched a fourth SMS investigation concerning Microsoft’s business software ecosystem. These interventions have thus far only been applied to U.S.-headquartered firms and include measures affecting commercial terms, interoperability, data use, ranking, and the use of publisher content in AI-enabled search services. USTR should encourage the UK to intervene only where there is clear evidence that barriers to entry are such that consumers are not satisfied with the options available; ensure that any interventions do not undermine the functioning of and ongoing investment in important digital services; and base fines and fees on UK rather than global turnover. The United States should seek a commitment that implementation of the UK’s digital competition regime will not unreasonably or unjustifiably restrict U.S. commerce.

Taxation of Digital Products and Services

On April 1, 2020, the UK instituted a 2% digital services tax. 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,¹¹³² findings later confirmed by USTR.¹¹³³

The burden imposed by the tax is one of the highest globally and continues to increase. HM Revenue and Customs reported that £944 million (approximately \$1.3 billion) was made payable under the DST in 2025–26, an increase of 17 percent from £808 million (approximately \$1.1 billion) in 2024-25. In its November 2025 statutory review, the UK Government reiterated that the DST is intended as an interim measure and that it remains committed to removing the tax

¹¹³² UK Parliament. (2023). *The Digital Services Tax*.

<https://publications.parliament.uk/pa/cm5803/cmselect/cmpubacc/732/report.html>.

¹¹³³ 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>.

once an appropriate global solution to the tax challenges arising from digitalization is in place. It has not, however, established a timetable for repeal. With the OECD process stalled, and USTR's Section 301 finding still valid, and the tax's rapidly growing cost to predominantly U.S. suppliers, USTR should refresh the record in its Section 301 proceeding and consider appropriate countermeasures unless the UK establishes a clear path to repeal the tax.

Online Safety legislation

The UK Government announced a series of measures intended to address safety concerns for young users, but that could affect the ability of US digital services to operate in the UK. While the headline measure was a ban on social media for under-16s (similar in principle to the ban in force in Australia since December 2025) the UK at the same time proposed restrictions on older users (16-17 year olds) including restrictions on personalisation that could severely affect both the economic value of some digital services and their ability to safeguard users. At the same time, it layered these restrictions on the existing child protection duties under the Online Safety Act, producing an increasingly challenging and unjustified cumulative burden regulating services for risks to users who are not allowed to access the platform. Services would remain subject to those duties in respect of children who, under the new rules, are not permitted to use them at all. At the same time, the UK Government announced restrictions on livestreaming, including a ban on under-16s livestreaming themselves on any platform, affecting both livestreaming platforms and US content creators.

USTR should encourage the UK to assess the cumulative impact of these measures on lawful services before adding further duties, to avoid duplicating obligations already imposed under the Online Safety Act, and to align its approach with comparable international frameworks.

Alongside those changes, the UK Government has also proposed multiple restrictions on the use of chatbots by under-18s, including restrictions on intimate features and possible overnight curfews and breaks, which could seriously affect legitimate use. Applying these restrictions would require age assurance, adding friction for 16-18 year old users. This can undermine the adoption of new AI services such as agentic AI, which is a particularly poor fit with restrictions such as curfews.

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.¹¹³⁴ 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

¹¹³⁴ *Investigatory Powers Act* [UK]. (2016). <https://www.legislation.gov.uk/ukpga/2016/25>.

the world, with the potential to create significant conflicts of law. Reports that the UK issued Apple a Technical Capability Notice requiring access to data protected by end-to-end encryption prompted criticism from the U.S. Administration and Congress and led Apple to withdraw its Advanced Data Protection service from the UK and challenge the notice before the Investigatory Powers Tribunal. In August 2025, the U.S. Director of National Intelligence stated that the UK had agreed to drop the portion of its demand that would have enabled access to the encrypted data of U.S. citizens. However, the UK Government has not publicly confirmed the scope of any withdrawal, and Apple's legal challenge remained active in September 2026. U.S. lawmakers continued to seek greater transparency regarding the order and its implications for U.S. users and national security. Government efforts to target digital security in this manner are damaging to U.S. digital exports and the future of online communications.

Concerns over these authorities persist. U.S. stakeholders, including Congressional leaders and senior U.S. national-security officials, have raised concerns that UK implementation of the Investigatory Powers Act and Online Safety Act could weaken the security of products and services supplied by U.S. companies. Particular concerns include requirements that could compel providers to retain the technical capability to decrypt data, prevent or delay deployment of security features, or otherwise weaken end-to-end encryption. USTR should encourage the UK to establish clear safeguards ensuring that neither framework requires U.S. suppliers to weaken product security or creates de facto barriers to the provision of secure digital services, it should also set a clear expectation that any future restrictions, particularly where they might have direct or indirect extra territorial impacts are communicated to relevant U.S. authorities.

On October 26, 2023, the Online Safety Act became law, imposing new obligations on regulated online service providers, with non-compliance potentially resulting in fines of £18 million or 10 percent of qualifying worldwide revenue.¹¹³⁵ Under Section 121, Ofcom may issue a Technology Notice requiring a regulated user-to-user or search service to use accredited technology to identify and address terrorism or child sexual exploitation and abuse content where Ofcom determines that doing so is necessary and proportionate. Section 122 separately requires Ofcom to obtain a skilled person's report before issuing such a notice. Ofcom published final guidance on its Technology Notice powers in May 2026, and the Government published minimum accuracy standards for eligible technologies in September 2026. Before Ofcom can use the accredited-technology power, an accreditation process must be established and relevant technology accredited against those standards. Industry and civil-society stakeholders have warned that future use of these powers against services using end-to-end encryption could require measures that weaken the security or privacy of encrypted communications.

¹¹³⁵ *Online Safety Act* [UK] Bill C. 50. [2023]. <https://bills.parliament.uk/bills/3137>.

Government-Imposed Content Restrictions and Related Access Barriers

The UK is considering extending regulatory preferences for public service media, currently applicable to connected-TV interfaces, to online video and potentially other digital services. The Media Act 2024 establishes a new regime under which designated connected-TV platforms will be required to ensure that designated public service broadcaster services and their content are available and appropriately prominent; implementation of that regime remained underway as of September 2026.¹¹³⁶ Ofcom's 2025 Public Service Media Review recommended exploring prominence on third-party platforms, and in June 2026 the Government formally opened a consultation on extending prominence to third-party video platforms and making 'trustworthy' news sources more discoverable on social media.¹¹³⁷ The Government stated that its preference is for voluntary agreements between platforms and public service media providers but has indicated that legislation could follow if voluntary action is insufficient

Extending prominence requirements into individual online services would be significantly more intrusive than device-level rules.¹¹³⁸ Rather than regulating app placement on home screens or menus, such requirements could affect search, ranking, recommendation, and curated-content systems, potentially forcing U.S. suppliers to re-engineer globally standardized services and override user-preference signals to favor designated UK broadcasters.

These measures could also disadvantage foreign content and suppliers. Giving mandatory prominence to UK PSBs would reduce the visibility of competing material, including content from U.S. media companies, independent producers, journalists, and creators, while imposing asymmetric compliance burdens on predominantly foreign platforms. In practice, such requirements could function as a non-tariff barrier by steering consumer attention toward government-designated domestic providers.

The proposal to make "trustworthy" news sources more discoverable on social media raises distinct concerns. It would require a government-designated standard for which news sources merit preferential treatment, and would require platforms to change how lawful content from other sources, including U.S. publishers, is surfaced to UK users.

¹¹³⁶ Ofcom. (2026, January 14). *Consultation: Prominence and Accessibility on Connected TV Platforms – Draft Code of Practice and Draft Guidance on the Agreement Objectives*. <https://www.ofcom.org.uk/tv-radio-and-on-demand/digital-tv/prominence-and-accessibility-on-connected-tv-platforms-consultation-on-our-draft-code-of-practice-and-draft-guidance-on-the-agreement-objectives>.

¹¹³⁷ Department for Culture, Media and Sport. (2026, June 23). *Watch This Space: A New Strategic Direction for UK Media – Green Paper and Public Consultation*. <https://www.gov.uk/government/consultations/watch-this-space-a-new-strategic-direction-for-uk-media-green-paper-and-public-consultation>.

¹¹³⁸ CCIA. (2026). *Concerns with UK efforts to institute preferences for public broadcasters*. <https://ccianet.org/library/concerns-with-the-uks-efforts-to-institute-preferences-for-public-broadcasters-on-streaming-platforms/>.

The United States should urge the UK not to extend device-level prominence rules into online video, social media, news aggregation, or other digital services. Such preferences also raise concerns under the UK's CPTPP commitments on national treatment for services and investment and non-discriminatory treatment of digital products. USTR should engage early and oppose requirements that compel platforms to alter search, recommendation, ranking, or other content-discovery systems to advantage designated domestic media.

Uzbekistan

Asymmetric Platform Regulation

Uzbekistan's Cabinet of Ministers Resolution No. 256 of May 1, 2024¹¹³⁹ establishes designation criteria and conduct restrictions for digital platforms with a dominant position or superior bargaining power, including AI-based platforms. Resolution No. 175 of April 16, 2026 narrowed the platform-specific regulation to operators registered as legal entities in Uzbekistan. It directs the Competition Committee to submit a separate framework for foreign-registered platform operators to the Cabinet by October 1, 2026; until that framework enters into force, those operators remain subject to the general provisions of the Competition Law. U.S. engagement should encourage transparent consultation and proportionate, non-discriminatory obligations in developing the separate framework. 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.¹¹⁴⁰

Restrictions on Cross-Border Data Flows

Law No. ZRU-1125, effective March 27, 2026,¹¹⁴¹ substantially narrowed Uzbekistan's personal data localization requirements. Mandatory domestic storage now covers biometric data, genetic data, and data of individuals using telecommunications operators active in Uzbekistan. Databases containing these categories remain subject to registration in the State Register of Personal Data Databases. Other personal data may be stored and processed abroad where one of three conditions is met: the destination country is recognized as providing adequate protection; the operator adopts and complies with standard contractual clauses or binding corporate rules meeting regulator-approved requirements; or the operator complies with international data-management and storage standards approved by the regulator. This reform reduces barriers

¹¹³⁹ Kosta Legal. (2024). *Uzbekistan Legal Newsletter for May 2024*.

<https://kostalegal.com/newsletters/uzbekistan-legal-newsletter-for-may-2024>.

¹¹⁴⁰ U.S. Department of State. (2024). *2024 Investment Climate Statements: Uzbekistan*. <https://www.state.gov/reports/2024-investment-climate-statements/uzbekistan/>.

¹¹⁴¹ Law No. ZRU-666 [Uzbekistan]. <https://lex.uz/docs/5220748>.

to cross-border digital services, although the remaining localization requirements continue to constrain international data processing.

Cabinet Resolution No. 415 of July 29, 2026, effective August 3, approved an adequacy list covering 49 countries and territories.¹¹⁴² The U.S. entry applies only to companies participating in the EU–U.S. Data Privacy Framework; other U.S. recipients cannot rely on that adequacy recognition. The resolution directs authorities to approve requirements for standard contractual clauses and binding corporate rules within three months. Its provision for automatic transfers without additional authorization or regulatory notification refers to information systems established under international agreements, creating uncertainty about its application to ordinary commercial transfers. Operators must report data leaks occurring during cross-border transfers to the competent authority within 24 hours of detection and provide details of the causes and remedial measures within 72 hours. U.S. engagement should seek clarification of the commercial transfer provisions and workable alternative transfer mechanisms.

Vietnam

Asymmetric Platform Regulation

In June 2026 the Vietnam Competition Commission and Ministry of Industry and Trade incorporated several DMA-style provisions addressing abuse of dominance into an amendment of its existing competition law.¹¹⁴³ The draft law is pending in the National Assembly but expected to be passed this year. With its rigid definitions of market power, the proposed amendments function as prohibitions on common commercial practices that will only apply to select technology companies.

USTR should urge Vietnam to reconsider this draft and ensure that any amendments to the Competition Law are technology-neutral, proportionate, and based on demonstrated competitive harm, and do not impose discriminatory or unnecessarily prescriptive restrictions on U.S. firms.

The Ministry of Industry and Trade and National Competition Commission published a draft consumer protection circular in August 2026, with the consultation ending in October 2026. This draft circular would maintain a 3 million annual active user threshold for designating a "large digital platform" subject to enhanced obligations, including a short turnaround period for providing algorithm, AI, and seller-verification data to regulators on request, and new

¹¹⁴² Cabinet of Ministers of the Republic of Uzbekistan. (2026). *Resolution No. 415 on Approving the List of Foreign States Ensuring Adequate Protection of Personal Data*. <https://lex.uz/ru/docs/8371371>.

¹¹⁴³ CCIA. (2026). *CCIA Briefer on Vietnam's Proposed Competition Law Draft Amendments*. <https://ccianet.org/library/ccia-briefer-on-vietnams-proposed-competition-law-draft-amendment/>

requirements to halt supply of recalled products within 24 hours and issue a public recall announcement within 3–5 working days depending on risk tier.¹¹⁴⁴

Vietnam is developing draft decrees replacing Decree 51/2019/NĐ-CP (technology-transfer and IP-licensing sanctions) and Decree 119/2017/NĐ-CP (product-quality standards and platform liability), the latter of which would explicitly expand liability to digital platform operators for product quality, e-labelling, traceability, and seller data.¹¹⁴⁵ Industry has urged a notice-and-takedown model over strict or vicarious platform liability, preservation of safe-harbor protection for procedurally compliant platforms, and avoidance of double penalties where product value is already regulated under sector-specific rules.

Customs-Related Restrictions and Import Barriers for Goods

Vietnam continues to require licenses for the import and export of covered products with civil cryptographic functionality. Decree 341/2026/NĐ-CP, effective September 1, 2026, establishes the current licensing framework for civil cryptography products and services, including import and export licenses.¹¹⁴⁶ The Decree introduces clearer procedures, including a six-working-day review period for complete import or export license applications, but maintains licensing and documentation requirements that can increase costs and delay access to necessary IT hardware. USTR should encourage Vietnam to administer these requirements transparently, consistently, and in a manner that does not unnecessarily restrict imports of widely used commercial technology.

Vietnam's import regulations categorize refurbished goods as used products and generally prohibit their importation. An exception exists for imports from countries party to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the EU-Vietnam Free Trade Agreement (EVFTA), but this exception has not been clearly reflected in implementing guidance. The lack of clarity creates uncertainty for U.S. suppliers of refurbished electronics and other goods seeking to access the Vietnamese market, and may result in inconsistent customs treatment. USTR should encourage Vietnam to clarify the scope and application of this exception and ensure consistent, transparent customs treatment of refurbished products from the United States.

¹¹⁴⁴ Vietnam Ministry of Industry and Trade/National Competition Commission. (2026). *Dossier of the draft Circular detailing certain articles of the Law on Protection of Consumer Rights*. <https://moit.gov.vn/du-thao-van-ban/ho-so-du-thao-thong-tu-quy-dinh-chi-tiet-mot-so-dieu-cua-luat-bao-ve-quyen-lo-i-nguoi-tieu-dung.html>.

¹¹⁴⁵ Vietnam Ministry of Science and Technology. (2026). *Dossier of the draft Decree replacing Decree No. 119/2017/NĐ-CP on administrative penalties in the field of standards, metrology and product and goods quality, as amended by Decree No. 126/2021/NĐ-CP*. <https://mst.gov.vn/van-ban-phap-luat/du-thao/2545.htm>.

¹¹⁴⁶ Chính phủ [Government of Vietnam]. (2026, September 1). Nghị định số 341/2026/NĐ-CP quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng về hoạt động mật mã dân sự [Decree No. 341/2026/NĐ-CP Detailing Certain Articles of and Measures to Implement the Cybersecurity Law on Civil Cryptography Activities]. <https://xaydungchinhhsach.chinhphu.vn/nghi-dinh-so-341-2026-nd-cp-quy-dinh-chi-tiet-luat-an-ninh-mang-ve-hoat-dong-mat-ma-dan-su-119260902115256675.htm>.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Article 25 of Vietnam's 2025 Cybersecurity Law (Law No. 116/2025/QH15), effective July 1, 2026, retains data-localization and juridical-presence requirements that can require foreign digital service suppliers to store data locally and establish a presence in Vietnam as a condition of serving Vietnamese users.¹¹⁴⁷ These obligations increase operating costs, restrict cross-border supply, and raise concerns under Vietnam's international commitments relating to the location of computing facilities and local presence. USTR should continue to press Vietnam to eliminate these requirements.

Implementing Decree 333/2026 exempts cross-border companies from these localization and presence requirements, except in specified cases, including where a company declines to comply with a government agency's request to address a violation.¹¹⁴⁸ The Law separately requires service providers to identify users' IP addresses and submit them to local law enforcement upon request, and to connect their systems to the government's cybersecurity force during cybersecurity incidents to support incident response — a requirement that raises concerns about a de facto “backdoor” obligation.

Additionally, the then-Ministry of Information and Communications (MIC) issued Official Letters No.1145/BTTTT-CATTT¹¹⁴⁹ and No. 783/THH-HTDLS¹¹⁵⁰ 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.¹¹⁵¹ 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.¹¹⁵² While the

¹¹⁴⁷ Quốc hội [National Assembly of Vietnam]. (2025, December 10). Luật số 116/2025/QH15 Luật An ninh mạng [Law No. 116/2025/QH15 on Cybersecurity]. <https://vanban.chinhphu.vn/?pageid=27160&docid=216499>.

¹¹⁴⁸ Government of Vietnam. 2026. *Decree 333/2026/ND-CP on the Law on Cybersecurity*. <https://english.luatvietnam.vn/decreed-no-333-2026-nd-cp-dated-august-19-2026-of-the-government-detailing-a-number-of-articles-and-measures-for-implementation-of-the-law-on-cyberse-445089-doc1.html>

¹¹⁴⁹ Vietnam Ministry of Communications. (2020). *Communications No.: 1145/BTTTT-CATTT Regarding guidance on criteria and technical indicators for evaluating and selecting cloud computing platform solutions serving e-Government/e-Administration*.

<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>

¹¹⁵⁰ Vietnam. (2020) *Communication No. 783/THH-HTDLS Regarding the guidance document on the application of cloud computing services and cloud computing service leasing in state agencies*

<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>

¹¹⁵¹ 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>.

¹¹⁵² *Vietnam Net*. (2020, May 23). *Ministry launches digital transformation campaign*. <https://vietnamnet.vn/en/sci-tech-environment/ministry-launches-digital-transformation-campaign-643379.html>.

standards are technically voluntary, in practice, they are expected to be adopted by the Vietnamese public sector.

Vietnam's 2023 Telecommunications Law and implementing Decree 163/2024/NĐ-CP liberalized the treatment of OTT communications, cloud, and data-center services by permitting offshore providers to supply these services cross-border without contracting with a licensed Vietnamese telecommunications operator.¹¹⁵³ However, foreign providers remain subject to notification, contact-point, and other compliance requirements, while cloud and data-center suppliers serving Vietnamese state authorities must store government data in Vietnam. These requirements limit the benefits of the broader liberalization and can disadvantage globally distributed cloud services.

Vietnam's Law on Personal Data Protection (Law No. 91/2025/QH15) and implementing Decree 356/2025/NĐ-CP took effect on January 1, 2026, replacing Decree 13/2023/NĐ-CP.¹¹⁵⁴ The framework requires companies conducting covered cross-border transfers to prepare and submit detailed transfer-impact assessments within 60 days of commencing transfers and grants authorities powers to suspend transfers on national-security grounds. These requirements impose substantial administrative burdens and uncertainty on international digital service providers whose operations depend on routine cross-border processing. USTR should encourage Vietnam to streamline these requirements and ensure that implementation does not unnecessarily restrict legitimate cross-border data flows.

Vietnam's Law on Data (No. 60/2024/QH15), which took effect on July 1, 2025, imposes significant restrictions on the classification, transfer, and processing of data.¹¹⁵⁵ The law and its implementing Decree 165/2025/ND-CP require explicit pre-approval for exports of data deemed "core," and pre-notification for exports of data deemed "important"—neither category of which is clearly defined. Article 12 of the implementing decree also imposes supplemental consent requirements relating to cross-border transfers. These requirements can operate as de facto data-localization measures and significantly disadvantage foreign cloud and digital-service suppliers whose business models depend on globally distributed infrastructure. USTR should press Vietnam to eliminate preapproval and pre-notification requirements for the export of important and core data and remove duplicative consent requirements for cross-border data transfers. Both requirements put cross-border suppliers at a competitive disadvantage as compared to domestic suppliers and thus implicate Vietnam's national treatment obligations in the GATS and other trade agreements.

¹¹⁵³ Lexology. (2025). *Unpacking Vietnam's Decree 163*.

<https://www.lexology.com/library/detail.aspx?g=cd3c405d-3d7f-4714-ac70-9aaf208e2fad>.

¹¹⁵⁴ Government of Vietnam. (2025). *Decree No. 356/2025/NĐ-CP Detailing Certain Articles of and Measures to Implement the Law on Personal Data Protection*.

<https://congbao.chinhphu.vn/van-ban/nghi-dinh-so-356-2025-nd-cp-468371.htm>.

¹¹⁵⁵ National Assembly of Vietnam. (2024) *Law No. 60/2024/QH15 on Data*.

<https://congbao.chinhphu.vn/van-ban/luat-so-60-2024-qh15-43563.htm>.

Decree 252/2026/NĐ-CP, governing tax administration for business activities conducted on e-commerce and digital platforms by households and individuals, requires foreign platforms to collect and store tax identification numbers or personal identification numbers for Vietnamese citizens, and identification information issued by a competent foreign authority for foreign nationals, effective July 1, 2026.¹¹⁵⁶ This collection-and-storage obligation reduces seller privacy and has drawn significant opposition from sellers and taxpayers. It runs counter to the principle of data minimization and compels businesses to build large databases of sensitive information, increasing their exposure as targets for malicious actors. The requirement that cross-border platforms provide information on foreign sellers to Vietnamese tax authorities may also put businesses in conflict with personal data protection regulations in their own country of establishment or that of their sellers. USTR should encourage the Vietnamese government and the Ministry of Finance to comprehensively revise this provision, removing the requirement to store and submit personal information, particularly that of foreign nationals, to safeguard user privacy, reduce compliance burdens, and avoid divergent requirements affecting the global systems of multinational enterprises.

In September 2026, Vietnam's Ministry of Public Security released a Draft Law on Data Security.¹¹⁵⁷ A revised version was submitted to the National Assembly on October 24.¹¹⁵⁸ This proposed law would establish the country's first standalone legal framework governing data security across the full data lifecycle, overlapping with the existing Data Law, Cybersecurity Law, and Personal Data Protection Law. Early drafts introduced a four-tier data classification system, requiring real-time in-country backup and pre-approval for cross-border transfers of data classified as "Important" or "Core," and would impose administrative penalties of up to 5 percent of global annual revenue for multinational violators. The law is targeted for entry into force on July 1, 2027.

A published draft has yet to be made available. Despite reports of improvements from the original draft, concerns over overlaps and duplications with the Data Law, the Personal Data Protection Law, and the AI Law remain. This could result in burdensome obligations for cross border providers, including required approval for cross border data transfers, assessment reports, information provision, logs and incident response cooperation, broad AI training-data requirements. As the leading cloud and AI providers in Vietnam, U.S. companies would bear the brunt. These provisions, if disadvantaging cross-border supply,

¹¹⁵⁶ Government of Vietnam. (2026). *Decree 252-2026 on the Law of Tax Administration*. <https://thuvienphapluat.vn/van-ban/EN/Thue-Phi-Le-Phi/Decree-No-252-2026-ND-CP-implementation-of-the-Law-on-Tax-Administration/720477/tieng-anh.aspx>.

¹¹⁵⁷ Lexology. (2026). *Vietnam's Draft Law on Data Security*. <https://www.lexology.com/library/detail.aspx?g=a801edfa-57e4-4463-87e6-13f24f13f415>.

¹¹⁵⁸ Data Guidance. (2026). *Vietnam: Government Submits Data Security Law to National Assembly*. <https://www.dataguidance.com/news/vietnam-government-submits-draft-data-security-law>

will likely run counter to commitments under the CPTPP, EU-Vietnam FTA, Vietnam's GATS commitments and US-Vietnam bilateral frameworks. USTR should urge Vietnam to suspend action on this legislation pending a public release of drafts and full industry consultation.

Decree No. 363/2026/NĐ-CP,¹¹⁵⁹ effective November 11, 2026, establishes administrative sanctions for a broad range of data-related violations by companies that collect data. Penalties including authority to suspend a platform's cross-border data transfers for a period ranging from three to twelve months — a sanction that would functionally halt in-country operations for an affected platform.

Effective March 1, 2027, e-commerce platforms will be classified as customs declarants and required to connect their systems directly to Vietnam's customs data-processing system, with automated tools used to assess compliance and risk for cross-border transactions. Implementation warrants monitoring, to ensure that requirements are reasonable and technically feasible.

Government-Imposed Content Restrictions and Related Access Barriers

Implementing measures under the 2025 Cybersecurity Law establish broad authorities over online content. Decree 327/2026/NĐ-CP sets procedures for addressing online information and conduct deemed to threaten national security, public order, or social safety; Decree 328/2026/NĐ-CP establishes rules concerning false and misleading information; and Decree 333/2026/NĐ-CP implements additional provisions of the law. These measures impose compliance obligations on domestic and foreign digital service providers and create risks of burdensome or unpredictable enforcement that can restrict access to the Vietnamese market.¹¹⁶⁰

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.¹¹⁶¹ The decree imposes broad obligations on foreign enterprises deemed “Regulated Cross-Border Services,” defined as providers with more than 100,000 monthly visits from

¹¹⁵⁹ Lexology. (2026). *Decree 363/2026/ND-CP*.

<https://www.lexology.com/library/detail.aspx?g=d3648ef1-a13d-4497-88ec-887fa9993ec4>.

¹¹⁶⁰ Government of Vietnam. (2026, August 19). *Decree No. 327/2026/ND-CP on the Prevention and Handling of Information and Conduct Using Information Technology, Computer Networks, Telecommunications Networks and Electronic Means That Infringe National Security, Public Order and Social Safety in Cyberspace* <https://vanban.chinhphu.vn/?pageid=27160&docid=219242>; *Decree No. 328/2026/ND-CP on the Prevention and Combating of Fake and False Information*. <https://vanban.chinhphu.vn/?pageid=27160&docid=219241>; *Decree No. 333/2026/ND-CP Detailing Certain Articles of and Measures to Implement the Cybersecurity Law*. <https://vanban.chinhphu.vn/?pageid=27160&docid=219244>

¹¹⁶¹ Government of Vietnam. (2024) *Law No. 147/2024/ND-CP - Management, Provision, and use of Internet Service and Cyber Information (2024)*. https://www.qtsc.com.vn/uploads/files/2024/12/30/147_2024_ND-CP_636187-eng.pdf.

Vietnam for six consecutive months or those leasing local data center space. The draft mandates intrusive data collection by requiring platforms to verify and store users' full names, dates of birth, and local phone numbers or state-linked ID numbers (VNeID) before allowing them to post, comment, or livestream. Designated entities must also notify the Ministry of Culture Sport and Tourism of a local contact point, take down flagged content within 24 hours, and temporarily block content within 48 hours of user complaints, and enter into “cooperation agreements” with Vietnamese press agencies. These blanket verification requirements conflict with data minimization principles and severely increase the potential for high-risk, high-impact data leakage.

The amendments also impose operationally and technically complex child safety mandates, giving providers an inadequate 120 days to identify and suspend or close all accounts held by users under 16. By forcing new youth accounts to be registered under a parent's identity and blocking all interactive features, the decree institutes blanket bans that completely restrict children's basic access to helpful information, rather than allowing for flexible, parent-supervised experiences. Furthermore, the draft establishes restrictive local-presence mandates for digital platforms hosting user-generated games, requiring foreign owners to operate strictly through a legally authorized Vietnamese entity, which creates unnecessarily significant operational overhead burdens. The draft is scheduled to be submitted to the government for approval in 2026. CCIA welcomed USTR's acknowledgment of these risks in the 2026 National Trade Estimates Report and urges continued U.S. engagement to press back against measures that undermine digital trade, user rights, and market access.

Imposing Legacy Telecommunications Regulations

Decree 242/2026/NĐ-CP, effective July 1, 2026, establishes Vietnam's current framework for radio, television, and related services.¹¹⁶² The Decree continues to extend traditional broadcasting requirements to internet-delivered services: providers of pay television services generally must be enterprises established under Vietnamese law, with foreign-invested enterprises subject to Vietnamese investment requirements, and internet-based services must operate through a “.vn” domain or Internet address managed by Vietnam. These requirements restrict the ability of foreign streaming services to supply services directly on a cross-border basis and can compel U.S. providers to establish or rely on local operations.

Challenges to the Development of Artificial Intelligence

Vietnam enacted the Law on Artificial Intelligence (Law No. 134/2025/QH15), effective March 1, 2026, followed by Decree 142/2026/ND-CP, effective May 1, 2026.¹¹⁶³ The Prime Minister

¹¹⁶² Government of Vietnam. (2026, June 26). Decree No. 242/2026/NĐ-CP. *Detailing and Guiding the Implementation of the Press Law on the Management of Radio and Television Activities and Services*. <https://congbao.chinhphu.vn/van-ban/nghi-dinh-so-242-2026-nd-cp-469887.htm>.

¹¹⁶³

subsequently issued Decision 33/2026/QĐ-TTg, effective August 15, 2026, establishing the list of high-risk AI systems subject to the framework.¹¹⁶⁴ The framework establishes risk-based obligations concerning classification, conformity assessment, documentation, transparency, and oversight, but its implementation could create significant market-access barriers for U.S. AI providers if requirements are overly broad, prescriptive, or imposed before supporting standards and regulatory infrastructure are in place. Key concerns include short compliance timelines; broad “high-risk” classifications that may capture general-purpose or assistive AI; mandatory conformity assessments that could duplicate internationally recognized certifications; and documentation requirements that risk exposing proprietary information. Vietnam should provide sufficient transition periods and phase enforcement as technical standards and conformity-assessment capacity mature. It should also ensure that high-risk classifications remain narrowly tailored to systems that directly determine consequential outcomes, recognize internationally accepted conformity mechanisms, and protect source code, training data, and other trade secrets from compelled disclosure. Vietnam should also avoid rigid, country-specific marking and labeling mandates and clarify that the framework applies only to AI systems commercialized in or specifically directed toward Vietnam. USTR should encourage implementation that is proportionate, interoperable with international standards, and does not impose unnecessary local-presence or Vietnam-specific product-design requirements.

Taxation of Digital Products and Services

Vietnam’s new Tax Administration Law (Law No. 108/2025/QH15), effective July 1, 2026, establishes the current tax-administration framework for cross-border digital commerce.¹¹⁶⁵ Foreign organizations and individuals conducting business through e-commerce or other digital platforms, or providing other services in Vietnam, must directly or through an authorized party declare and pay applicable taxes. The law also requires e-commerce and digital platforms with online ordering and payment functionality to withhold, declare, and remit tax on behalf of household and individual sellers using their services. This Foreign Contractor Tax (FCT) is a discriminatory tax that burdens U.S. commerce in Vietnam. It specifically targets foreign companies and industries operating in the digital economy, where U.S. 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 U.S. commerce in Vietnam, and enables Vietnam to assert first right to tax over the US tax base. Foreign suppliers may seek relief under applicable bilateral tax treaties, but Vietnam’s administration of double-tax-relief applications can create significant barriers for U.S. industries. U.S. companies face significant barriers in their applications for double tax relief under the relevant bilateral tax treaties entered into

¹¹⁶⁴ Prime Minister of Vietnam. (2026). *Decision No. 33/2026/QĐ-TTg on the List of High-Risk Artificial Intelligence Systems*. <https://vanban.chinhphu.vn/?pageid=27160&docid=218658>.

¹¹⁶⁵ Quốc hội [National Assembly of Vietnam]. (2025) *Law No. 108/2025/QH15 on Tax Administration*. <https://congbao.chinhphu.vn/van-ban/luat-so-108-2025-qh15-468670.htm>.

by the Vietnamese government with other governments. Despite complying with domestic tax law, regulations and procedures in Vietnam, these U.S. 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.

Vietnam's corporate income tax regime continues to apply the foreign contractor tax to transactions involving the transfer of ownership of finished goods between manufacturers and distributors, as well as between the domestic and foreign legal entities of a single manufacturer, where the transaction takes place within Vietnamese territory.¹¹⁶⁶ Vietnam's theory is that the transferring enterprise generates Vietnam-sourced revenue. These transactions are, by nature, internal financial and accounting transfers within an enterprise and do not generate revenue in the course of the transfer; taxing them functions as a *de facto* tariff on intra-firm goods movements that are integral to global manufacturing and distribution chains routed through Vietnam.

Other Barriers to Digital Trade

Vietnam's new E-Commerce Law (Law No. 122/2025/QH15) and implementing Decree 248/2026/ND-CP took effect on July 1, 2026, replacing the prior framework under Decree 85.¹¹⁶⁷ The law imposes differentiated requirements on foreign e-commerce platforms depending on their functionality, including obligations to appoint an authorized representative or, for certain platforms with online ordering functions, establish a legal entity in Vietnam. Where treaty commitments preclude a local-establishment requirement, implementing rules impose alternative conditions, including a substantial bank-deposit requirement for certain foreign platforms. The framework also expands obligations relating to seller verification, livestream commerce, and other platform activities, increasing compliance and market-entry costs for foreign suppliers. Existing platforms registered under the prior regime may continue operating under their existing registrations through June 30, 2027 while transitioning to the new requirements.

¹¹⁶⁶ Vietnam National Assembly. (2025). *Law 67/2025 QH15 on Corporate Income Tax*. <https://thuvienphapluat.vn/van-ban/Doanh-nghiep/Luat-Thue-thu-nhap-doanh-nghiep-2025-so-67-2025-QH15-580524.aspx> and <https://thuvienphapluat.vn/van-ban/Doanh-nghiep/Nghi-dinh-320-2025-ND-CP-huong-dan-Luat-Thue-thu-nhap-doanh-nghiep-665051.aspx>.

¹¹⁶⁷ Office of the Government [of Vietnam]. (2026). *Decree No. 248/2026/ND-CP providing detailed regulations on a number of articles of the Law on E-commerce*. <https://congbao.chinhphu.vn/van-ban/nghi-dinh-so-248-2026-nd-cp-469983/66872.htm>.

Vietnam's amended Advertising Law (No. 75/2025/QH15), effective January 1, 2026, retains the requirement that foreign organizations not operating in Vietnam use Vietnamese advertising service providers to advertise in the Vietnamese market.¹¹⁶⁸ This local-intermediary requirement raises costs and restricts the ability of U.S. advertising suppliers to serve the market directly. It is also clearly inconsistent with Vietnam's GATS commitments covering advertising, as it raises costs and thus puts cross-border suppliers at a competitive disadvantage. Less trade-restrictive alternatives, such as transparency requirements or designation of a local point of contact, could provide regulatory oversight without restricting cross-border supply. USTR should urge Vietnam to remove or suspend enforcement of this requirement.

On July 13, 2026, Vietnam's Ministry of Culture, Sports and Tourism released draft amendments to Decree 147 focused on online video games.¹¹⁶⁹ The draft remains pending. While the amendments would streamline certain procedures for game approvals, they leave intact the core barriers facing foreign game suppliers: pre-launch licensing or notification requirements, a local-establishment mandate that effectively restricts cross-border supply, and a local-server requirement for multiplayer (G1) games.¹¹⁷⁰

These restrictions have contributed to U.S. publishers and distribution platforms curtailing or withdrawing gaming offerings from Vietnam. For G1 games, the draft would eliminate the general service license but retain game-specific approval, leaving the underlying market-access barrier largely unchanged. G2-G4 games would remain subject to advance notification and regulatory confirmation before launch, creating significant administrative burdens and uncertainty. Vietnam should replace these pre-market approval requirements with a simple notification regime that permits publication upon notice, backed by a transparent notice-and-takedown process for noncompliant games. Decree 147 also requires foreign game suppliers to establish an enterprise in Vietnam and subject locally established providers to foreign-equity restrictions, while Article 54 requires G1 games to use servers located in Vietnam. These local-presence, investment, and computing requirements are inconsistent with Vietnam's international trade commitments and should be eliminated. The draft amendments would also create a separate licensing regime for platforms that enable users to create and distribute games, further extending pre-market regulation to user-generated gaming services.

¹¹⁶⁸ National Assembly of Vietnam. (2025, August 22). *Law on Advertising*. <https://datafiles.chinhphu.vn/cpp/files/vbpq/2025/8/88-vbhn-vpqh.pdf>

¹¹⁶⁹ Ministry of Culture, Sports and Tourism (Vietnam). (2026). *Amending and supplementing a number of articles of Decree No. 147/2024/NĐ-CP: Establishing a modern, transparent, and stable digital legal framework*. <https://bvhttdl.gov.vn/sua-doi-bo-sung-mot-so-dieu-cua-nghi-dinh-so-1472024nd-cp-xay-dung-mot-khuon-kho-phap-ly-so-hien-dai-minh-bach-on-dinh.htm>

¹¹⁷⁰ CCIA. (2026). *Vietnam's Online Gaming Regulations*. <https://ccianet.org/library/vietnam-online-gaming-regulations/>

IV. CONCLUSION

As the global internet continues to grow and becomes even more tightly intertwined with international commerce, CCIA remains focussed on the proliferation of digital trade barriers like those discussed above. Identifying and addressing these barriers as they arise 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.