Written Statement of Jonathan McHale
Vice President of Digital Trade at CCIA

United States House Ways & Means Trade Subcommittee

"Hearing on American Trade Enforcement Priorities."

Feb. 25, 2025

Digital trade, accounting for $655.5 billion of U.S. services exports annually, is essential to U.S. economic interests and a critical counterbalance to its trade deficit in goods. Demonstrating persistent growth, the export of U.S. digital products and services undergirds the United States' long-term prosperity and global competitiveness; but that growth, and its contribution to the U.S. economy is now in jeopardy, facing an upsurge of restrictive barriers in foreign markets. Without a firm response, including enforcement of existing trade commitments and expanding them to new markets, the remarkable success of U.S. firms to date is at risk. A first step in addressing this risk is chronicling the plethora of barriers to affecting U.S. digital exports, including in USTR's 2025 National Trade Estimate (NTE) report.

This statement provides an overview of some of the main barriers to digital trade, specifically identifying priority measures affecting CCIA members in each category.

A. Taxation of Digital Products and Services

Based on unfounded assertions that digital service suppliers fail to pay their fair share of taxes and should be subject to additional levies in the jurisdictions they serve, many countries have unilaterally introduced measures to tax U.S. online services firms through what are known as digital services taxes (DSTs). CCIA first documented DSTs in its NTE comments in 2018. Since then, a growing number of countries that now totals over a dozen have enacted such measures, costing U.S. companies billions of dollars annually.

DSTs are a tax levied on revenue, not profit, and based on gerrymandered service definitions and revenue thresholds that disproportionately hit U.S. firms. While some governments assert that the criteria for scoping in firms are facially neutral, they by design target U.S. firms who typically pay the bulk of such taxes. In the UK, for example, it is reported that 90% of the tax is borne by U.S. firms.[1] Recent estimates are that such taxes cost U.S. firms upwards of $2 billion annually, a number that will jump when Canada's collection starts at the end of June. These payments serve both to erode the U.S. tax base, and, because they have to be recovered from customers, to put U.S. firms at a competitive disadvantage in the foreign market—since their competitors are largely exempt from such taxes.

DSTs also represent a significant departure from international taxation norms in their focus on revenues (versus profits), ignoring established principles on what constitutes a taxable presence, a narrow, gerrymandered definition of in-scope services. By unilaterally imposing specific countries' preferred solutions, they also undermine any process for reaching consensus reforms on international tax principles to address the challenges associated with shifting business models. These taxes, wherever imposed, warrant a substantial, proportionate response from the United States.

1 https://crsreports.congress.gov/product/pdf/R/R47988#:~:text=In%20the%20UK%2C%2090%25%20of,largely%20or%20completely%20U.S.%20firms.

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

The moratorium has subsequently been renewed at every Ministerial since 2000, contributing to the development of global digital trade and the building of a consensus with respect to the value of the digital economy. Permanent bans on the imposition of customs duties on electronic transmissions now feature prominently in trade agreements around the world, representing a binding commitment by dozens of countries—including all U.S. FTAs over the past two decades, and most concluded by the EU.

Analysis of duties on electronic transmissions for economic development shows that claims of revenue loss are misguided,[2] and the new distortions such a duty would create could seriously undermine development goals.

Key examples of DSTs and other discriminatory taxes include:

- **Australia:** A proposed coercive and discriminatory tax that requires U.S. technology companies to subsidise Australian media companies.
- **Austria:** A DST that imposes 5% tax on advertising revenues of U.S. digital companies.
- **Canada:** A DST that imposes 3% tax, retroactive to 2022, on revenues of U.S. digital companies that spare Canadian competitors in similar sectors.
- **Czechia:** A proposed DST would impose 7% tax on revenues of U.S. digital companies.
- **France:** A DST that imposes 3% tax on revenues of U.S. digital companies, with a recent amendment that would raise the tax rate to 5%. Separately, a 2% tax on video content and video streaming services and a 1.2% tax on revenues of cross-border music streaming providers and social media services licensing and broadcasting music.
- **India**: A so-called "Equalization Levy" imposes a 6% withholding tax based on the gross revenue generated from digital advertising services provided by non-residents to Indian residents, leading to double taxation and contradicting international tax principles.
- **Indonesia:** Customs filing requirements for software and other digital products imported electronically that sets a foundation for imposing customs duties on digital transmissions and results in significant and unnecessary compliance burdens on U.S. businesses.
- **Italy:** A DST that imposes 3% tax on revenues of U.S. digital companies.
- **Kenya**: A Significant Economic Presence Tax that imposes a 3% effective tax rate on revenues of cross-border suppliers, and which, like DSTs, can result in double taxation.
- **Spain:** A DST that imposes 3% tax on revenues of U.S. digital companies.

[2] OECD, Electronic Transmissions and International trade – Shedding New Light on the Moratorium Debate (Nov. 4, 2019), https://one.oecd.org/document/TAD/TC/WP(2019)19/FINAL/en/pdf; ECIPE, The Economic Losses From Ending the WTO Moratorium on Electronic Transmission (Aug. 2019), https://ecipe.org/publications/moratorium/.

- **Türkiye:** A DST that imposes 7.5% tax on revenues of U.S. digital companies.
- **United Kingdom:** A DST that imposes 2% tax on revenues of U.S. digital companies.

B. Mandatory Payment Obligations Benefitting Domestic Competitors

A pervasive and growing phenomenon in digital markets in many jurisdictions is a set of policies characterized by their extractionary and redistributive nature–forcing one set of market participants to subsidise the economic activities of another. This is prevalent in areas as diverse as news, audiovisual production, and telecommunications networks.

→ News: In the past decade, several governments have instituted rules to force certain U.S. (and, so far, only U.S.) online services to fund local news corporations through mandatory negotiations, as a condition for hosting any form of news content including links, snippets and quotes–despite international intellectual property law that guarantees that it can be distributed without compensation. These frameworks circumvent free market dynamics and the symbiotic relationship between these online services and news businesses—a relationship demonstrated by news companies voluntarily posting on social media services, allowing links to be indexed on search engines, and paying for search engine optimization tools. These laws oblige the targeted U.S. firms to choose between paying (typically to large local media conglomerates) or exiting the market.

Examples of these rules include Australia's News Media Bargaining Code, Canada's Online News Act, and Indonesia's online news regulations that force payments from online platforms to news organizations (documented below). The developments in Australia and Canada are particularly concerning given the precedent they have set globally. Both countries that passed these laws and required payments to benefit local incumbents (paid exclusively from U.S. suppliers) were countries with whom the United States has strong free trade commitments. Inevitably, this has emboldened other countries to follow suit. The negative impact of such policies is now well-documented: laws in Germany, Spain, and France resulted in significant decreases in traffic and losses of revenue for local publications.[3]

Key examples include:

- **Australia:** The News Media Bargaining Code requires U.S. online service providers, when designated, to pay Australian news publishers for the links and snippets.
- **Canada:** The *Online News Act* requires specified U.S. technology companies to pay hundreds of millions of dollars annually to Canadian news publishers.
- **Indonesia:** A requirement for digital services providers to pay news firms for content that appears on their platforms, with potential for subsequent burdensome regulations.
- **New Zealand:** Proposed requirement for U.S. online services providers to pay New Zealand media companies to allow for news links to appear in the market.

[3] CCIA, Link Tax Failures: Global Efforts Continue to Uproot the Internet's Foundation and Journalism Ecosystem (May 14, 2024), https://ccianet.org/library/link-tax-failures-global-efforts-continue-to-uproot-internetsfoundation-and-journalism-ecosystem/.

→ Telecommunications: A similar rent-seeking approach favored by certain countries targets online services' revenues to subsidize local internet service providers (ISPs). South Korea pioneered such an approach by forcing domestic online content and application providers (CAPs) to pay ISPs for the traffic that ISPs customers request. In the face of complaints about "fair share" of network costs, policymakers have called on U.S. online services providers to also pay, resulting in proposals that have proliferated and are now in discussion both in South Korea and the European Union, Brazil, the Caribbean Telecommunications Union, and Colombia.

These proposals—effectively taxing U.S. online services providers to subsidize incumbent local ISPs—threaten digital trade between the U.S. and key export markets; undermine the internet ecosystem both locally and globally by establishing sender-party-pays mandates in the mold of telephony; and result in vast inefficiencies for consumers and CAPs alike by disincentivizing the investments online companies make to improve traffic delivery, such as caching servers and data centers.

Key examples include:

- **Brazil**: Proposals to impose "network usage fees" on online service providers to compensate internet service providers (ISPs) for the infrastructure that carries traffic to consumers. These consultations focus on large traffic generators, which would discriminate against U.S. content and application providers in Brazil.
- **European Union**: Persistent efforts to require online service providers to pay ISPs for receiving their traffic, these network usage fees would be disproportionately borne by U.S. companies, given the attention of EU consultations and lawmaker statements to American companies and volume of broadband traffic.
- **Korea:** Requirement for U.S. online content providers to assume liability for network performance, which establishes a basis for requiring payment of significant fees to Korean telecommunications companies.

→ Audio and Audiovisual Content: Countries are increasingly looking to force internet-enabled audio and audiovisual content providers to contribute a certain percentage of revenue towards funding local content, meet carriage quotas, and otherwise institute preferences for local content. These measures, pursued in the name of cultural protection, discount the enormous contributions global streaming services make in both investing in local production and exporting it globally. Often, the definition of local content precludes international firms from qualifying as producers of local content without partnering with a domestic entity and surrendering intellectual property rights. Such regimes are patently discriminatory and undermine the very nature of global streaming services, which depend on large and diverse catalogues to meet consumer demand.

Requirements for audio content are further misaligned with modern day music production, where producers, writers, and musicians are often international by nature, as are ownership rights associated with song catalogues. Requiring content quotas or funding obligations on the

basis of nationality is not only discriminatory for providers and content creators, but can also significantly disrupt the creative ecosystem.

Key examples include:

- **Australia:** Proposed requirements for U.S. online video providers to fund the development and production of Australian content.
- **Brazil**: Proposed Bill No. 2,331/2022 would disproportionately undermine U.S. streaming providers to the benefit of Brazilian broadcasters through levies of up to 3% of annual revenue in-market to fund the development of Brazilian content.
- **Canada:** The *Online Streaming Act* requires U.S. online streaming providers and other internet-enabled services providers to fund and promote Canadian content.
- **China**: Administrative measures restrict the share of foreign content on online streaming services to 30%.

C. Asymmetric Platform Regulation

A general but ill-defined desire for "platform regulation," unsupported by evidence of consumer harm, is spurring digitally-focused ex-ante regulation around the world. Like DSTs, such measures rely on arbitrarily-defined service categories and hand-crafted thresholds to target a subset of suppliers who are predominantly American and rarely local. This trend raises significant concerns that an untested policy is spreading before its effects, both intended and unintended, have been adequately evaluated. In many cases, platform regulation serves as a backdoor for industrial policy explicitly designed to advantage local competitors: while dressed up as competition policy it typically lacks the analytic rigor and factual record that would justify such a prescriptive and one-sided result—disadvantaging U.S. firms at the expense of local and third-country suppliers, including digital players from China. Such rules are often tailored to specifically impede the legitimate business models of U.S. companies, including their administration of app stores, their ability to share data across services, and their ability to integrate products for consumer benefit and increased efficiency.

In all instances, regulators have struggled to separate procompetitive conduct from the hypothetical harms they seek to regulate. The effectiveness of such proposals in promoting innovation in the tech sector is highly questionable. While these prescriptive laws and regulations purportedly promote competitive digital markets, evidence is mounting of adverse consequences that raise prices, stymie innovation, limit choice for consumers and small businesses, and introduce security vulnerabilities.

Key examples include:

- **Australia:** Proposed regulatory regime based on the EU's *Digital Markets Act* that would target specified U.S. companies with discriminatory obligations and subject them to significant fines.
- **Brazil:** Several legislative proposals—including one being developed by the Ministry of Finance—to implement an *ex-ante* regulatory regime that would impose restrictions on how U.S. companies operate in Brazil, which could significantly interfere with American business plans and increase compliance burdens.

- **European Union:** The *Digital Markets Act* imposes aggressive restrictions on U.S. companies' operations and forces the transfer of proprietary data and technology to foreign rivals. Fines of up to 20% of a company's global revenue could be issued. The knock-on effects of this policy have broad ramifications, as some EU member states are seeking to expand the restrictions for targeted firms to include AI and cloud services.
- **Germany:** German *Competition Act* was recently amended to include broad limitations disproportionately imposed on U.S. companies, including mandatory sharing of proprietary data with rivals. This has already resulted in proceedings and findings targeting U.S. firms.
- **India:** Proposed *Digital Competition Bill* would adopt rules based on the EU's *Digital Markets Act* that would subject U.S. companies to strict and discriminatory restrictions.
- **Japan:** The *Act on Promotion of Competition for Specified Smartphone Software (SSCPA)* and proposed implementing regulations would impose extensive limitations on U.S. providers of mobile services, and mandatory sharing of technology, while sparing rivals in Japan and China from the rules.
- **Korea:** Several bills, including one proposed by the government, modeled on the EU's *Digital Markets Act* that would impose significant barriers on U.S. digital companies. The proposed bills would benefit Chinese companies and facilitate their growth in the region, as Chinese competitors would be given preferential treatment compared to U.S. companies. Further, enforcement actions that disproportionately target U.S. firms are evidence of discriminatory treatment, an unreasonable barrier to legitimate commerce.
- **Türkiye**: Amendment to the *Turkish Competition Act* would impose EU-style restrictions and mandatory data-sharing obligations disproportionately on U.S. companies, with fines of up to 20% of annual turnover.
- **United Kingdom:** The *Digital Markets, Competition, and Consumer Act* created regulations targeting U.S. tech firms as designated companies imposing strict "conduct requirements," with potential fines of up to 10% of global revenue.

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

One of the most egregious barriers to digital trade is the growing practices of data localization and mandated use of domestic computing infrastructure. In a 2021 report, the Information Technology and Innovation Foundation found that data localization measures almost doubled from 67 such policies worldwide in 2017 to 144 in 2021.[4] Governments often cite domestic privacy protections, defense against foreign espionage, law enforcement access needs, and local development as motivations for mandating localization. Such rationales are often pretextual, however, simply justifying the intended effect of inhibiting foreign competitors from entering markets or creating an advantage for local suppliers. In recent years there has been an increasingly explicit protectionist angle to these regulations in the pursuit of achieving "technological sovereignty" from mainly U.S. services.

[4] Nigel Cory & Luke Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, Info. Tech. and Innovation Found. (July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-theycost/.

Further, rather than ensuring user privacy or data security, forced localization creates a host of new targets of opportunity for both criminals and foreign intelligence agencies.[5] Such measures also work against data security best practices that emphasize decentralization over single points of failure,[6] while undermining the international cooperation that is necessary to promote cross-border law enforcement access.[7]

The United States leads the world in data processing and storage capacity, so any requirement to move such capacity to a foreign location undermines a clear competitive advantage the U.S. currently enjoys.[8] One state alone (Virginia) boasts 475 data centers,[9] powering a significant portion of global online activity.[10] The United States claimed 5,381 data centers in 2024, with the next largest number being Germany's 521.[11] In short, policies promoting data localization will inevitably result in a net loss for U.S. economic interests, including those of its workers. As digital services proliferate and traditional forms of national and international commerce become ever more data-intensive, the importance of this strategic advantage will grow as will the centrality of these data centers for information flowing worldwide.

Data localization policies significantly harm both U.S. cloud services providers and their customers, both American and foreign; it affects billions of dollars in economic value, and millions of companies, applications, and services reliant on cloud infrastructure and related services.[12]

Even where U.S. firms see a commercial basis for investing in cloud services infrastructure abroad, many jurisdictions are seeking to impose onerous and targeted requirements on such providers that limit their ability to operate in these markets. The regulations and policies pursued globally range from traditional protectionist goals to preference local upstarts at the expense of foreign rivals, to measures seeking greater ability to conduct surveillance over individuals or companies.

Examples include rules that mandate security standards preferential to local firms in France, certification standards aimed at keeping out foreign competitors in Korea and Vietnam, data localization requirements in Indonesia and Mexico, restrictions on virtual private networks in

---

[5] Anupam Chander & Uyên P. Lê, Data Nationalism, 64 EMORY L.J. 677, 718-19 (2015), http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.

[6] See Peter Swire, The Effects of Data Localization on Cybersecurity, Georgia Institute of Tech. (Feb. 18, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4030905.

[7] Vivek Krishnamurthy, Cloudy with a Conflict of Laws, BERKMAN CTR. FOR INTERNET & SOC'Y, Research Publication No. 2016-3 (Feb. 16, 2016), https://ssrn.com/abstract=2733350.

[8] Mattias Bauer et. al., The Cost of Data Localization, ECIPE (2014) https://ecipe.org/wpcontent/uploads/2014/12/OCC32014__1.pdf; Nigel Cory & Luke Dascoli, supra note 74; Jacqueline Brehmer, Data Localization The Unintended Consequences Of Privacy Litigation, 67 Am. U. L. Rev. 927 (2018) https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=2009&context=aulr.

[9] Virginia Data Centers, Data Center Map (last visited Oct. 14, 2024), https://www.datacentermap.com/usa/virginia/.

[10] Antonia Olivo, Northern Va. is the Heart of the Internet. Not Everyone is Happy About That., Wash. Post (Feb. 10, 2023), https://www.washingtonpost.com/dc-md-va/2023/02/10/data-centers-northern-virginia-internet/.

[11] Leading Countries by Number of Data Centers as of March 2024, Statista (Oct. 11, 2024).

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

India, obligations regarding content and possible interception of messages in Malaysia, proposed localization requirements in Saudi Arabia, and a collection of intrusive measures related to intellectual property and business operations imposed in China.

Key examples include:

- **European Union:** The proposed *EU Cybersecurity Certification Scheme for Cloud Services (EUCS)*, which, combined with local laws, could prohibit U.S. cloud providers from access to government contracts and key parts of the EU market unless they enter into joint ventures with European entities. Buttressing this are on-going EU efforts to justify discriminatory treatment of U.S. firms providing other ICT services, and parallel initiatives to embed European preferences in public procurement for 'critical sectors,' including cloud and potentially other ICT services.
- **France:** A mandatory labeling and cybersecurity certification standard, called *SecNumCloud*, that blocks U.S. cloud providers from accessing government contracts and undefined "critical sectors" in the French market.
- **Hungary**: Broad data localization requirements for state and local government bodies and organizations providing essential services.
- **Indonesia:** A series of regulations that require data localization for cloud providers servicing financial services entities.
- **Kenya**: Onerous and restrictive data localization and reporting obligations on providers of "Critical Information Infrastructure," which includes cloud services providers, with increased restrictions and obligations for certain categories of data.
- **Korea:** The *Cloud Security Assurance Program (CSAP)*, a set of requirements for entities servicing public institutions that block U.S. cloud providers from accessing the market.
- **Mexico:** Requirements for electronic payment providers to use cloud vendors from more than one jurisdiction, which risks driving business and data storage to untrustworthy vendors such as Huawei, one of the few non-U.S. vendors in Mexico.
- **Türkiye**: Localization mandates for government workloads determined to be "strategic." The Central Bank of Türkiye imposes similar restrictions on cloud outsourcing.
- **United Arab Emirates**: Strict sovereignty controls that mandate cloud services providers that serve the public sector and certain regulated industries to be solely subject to UAE law; not be subject to foreign jurisdiction and laws; and physically localize data centers as well as engineering, security, maintenance, and support operations and personnel.
- **Vietnam:** The *Law on Cybersecurity* and implementing *Decree 53* both require data localization for U.S. companies operating in the market, severely hindering cross-border supply of cloud services. The *Personal Data Protection Decree* also restricts the movement of data and mandates localization.

E. Potential Challenges to the Development of AI

An emerging trend is the proliferation of AI laws and regulations that could adversely affect investment in or the cross-border supply of AI-enabled services and technologies. As governments seek to advance regulations with the declared aim of promoting safety and privacy, they may also face pressure to slow competitive threats and protect local market

advantage. For U.S. firms, representing leading capabilities in foundational models, research, advanced computing, and end-use tools, the risk of discriminatory treatment is significant.

Traditional threats to digital trade similarly affect AI — including restrictions on the cross-border transfer of data, data localization requirements, and onerous transparency and reporting requirements that infringe on intellectual property rights and trade secrets. More specific threats to AI include forced disclosure of source code, algorithms, and commercially sensitive data, imbalanced applications of copyright law, country-specific onerous technical requirements, and discriminatory treatment of service suppliers. If U.S. leadership in this burgeoning field is to be a priority, the U.S. government should bolster its current efforts to build consensus on best practices for governing AI by ensuring that foreign governments do not impose measures that restrict U.S. firms' AI offerings and impede market access.

Key examples include:

- **Australia**: The Australian government is proposing to classify all general-purpose AI models as high-risk in a new regulatory regime that would add significant compliance burdens to U.S. companies with AI products and services operating in Australia.
- **Brazil:** Proposed AI Bill includes unbalanced copyright requirements that could restrict U.S. companies from conducting AI training and operating in Brazil.
- **Canada:** Proposed *Artificial Intelligence and Data Act* places strict restrictions on "high-impact" AI systems that could include a wide range of services due to vague definitions. The law proposes penalties of up to 3% of global revenue.
- **European Union:** The draft Code of Practice under the *AI Act* could impose stricter limitations on U.S. AI models than those for most EU and Chinese competitors, and could require disclosure of U.S. trade secrets and data to foreign authorities and rivals.
- **Korea** is in the process of implementing its *AI Basic Act*, with initial indications that it could require burdensome and intrusive reporting requirements for a subset of applications where U.S. firms predominate.
- **Spain:** Proposed Collective Licensing Regime would require U.S. companies to pay rightsholders to be able to conduct AI training in Spain.

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

CCIA has long viewed foreign censorship of U.S. internet services as having a trade dimension and is supportive of efforts to identify certain practices that could be actionable under trade rules. CCIA also supports strengthening freedom of expression commitments in trade agreements. The U.S. technology sector is on the front lines in the battle against government censoring, filtering, and blocking of internet content, as well as targeted DNS and site blocking.

In a survey this past year, Freedom House reported that between June 2023 and May 2024, 52% of the world's population that has access to the internet had social media platforms temporarily or permanently restricted by the government.[13] As of September 2024, 25

[13] Allie Funk et. al., Freedom on the Net 2024, FREEDOM HOUSE (2024) https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online.

countries were systematically restricting access to social media or messaging services, with political protests and social unrest often being the impetus for such restrictions.[14] Access Now reported there were 283 internet shutdowns in 39 countries in 2023, the highest ever recorded and a 41% increase from the 201 shutdowns imposed in 40 countries in 2022.[15]

Censorship and denial of market access for foreign internet services have long been the case in restrictive markets like China, where a significant portion of the global internet is simply unavailable. But such practices are becoming increasingly common in emerging digital markets including some traditional large trading partners and accomplished through different tools and methods. Because the business community has a limited technical capacity to assess and respond to interference with cross-border flow of services, products, and information by nationstates, allied governments have a critical role to play in partnering with technology companies and leading in the defense of internet freedom and by embracing and promoting open digital trade principles. To tackle these urgent issues, identifying key barriers is critical.

Government-imposed censorship of digital services and content takes multiple forms, and the risks associated with each can vary greatly. For example, some types of content restrictions may be reasonable and legally permissible in certain contexts but may result in overbroad removals of user speech if attached to filtering or monitoring requirements. Trade concerns also arise where content policies are not applied equally to domestic and foreign websites.

Key examples include:

- **European Union:** The *Digital Services Act* imposes extensive audit requirements, fines of up to 6% of global revenue, and requirements to pay "supervisory fees." U.S. companies are disproportionately impacted by provisions applicable to larger suppliers.
- **Germany:** The *"NetzDG"* law imposes stringent content oversight requirements that subject companies to burdensome procedures.
- **India:** A stringent regulatory climate, including the *IT Act* and *Intermediary Liability Guidelines*, subject primarily U.S. service providers to intrusive audit and mediation requirements, hefty fines, and potential criminal liability. This undermines business operations in a key market and threatens freedom of expression.
- **Singapore:** The *Online Criminal Harms Act* and the *Online Safety Act* grant the government broad oversight of U.S. online service companies to mandate moderation procedures, with the power to demand takedowns and block services as punishment.
- **Türkiye:** Türkiye's Internet Regulatory Authority is proposing amendments to Law No. 5651 that would regulate U.S. service providers' moderation for vaguely-defined speech obligations, with new penalties and revenue-based fines for violations.
- **Vietnam:** Stringent content regulations that require 24-hour removal of vaguely-defined "false" content and information-sharing on users posting this content.

[14] Theodora Skeadas et. al., Digital Disruption: Measuring the Social and Economic Costs of Internet Shutdowns & Throttling of Access to Twitter, TechPolicy (Sept. 25, 2023), https://techpolicy.press/digitaldisruption-measuring-the-social-and-economic-costs-of-internet-shutdowns-throttling-of-access-to-twitter/; SurfShark, Internet Shutdown Tracker (updated Sept. 23, 2024), https://surfshark.com/research/internet-censorship.

[15] The Most Violent Year: Internet Shutdowns in 2023, ACCESS NOW (May 15, 2024), https://www.accessnow.org/internet-shutdowns-2023/.