*Before the*
**United States International Trade Commission**
Washington, DC

*In re*:
Investigation No. 332-585:
Foreign Censorship Part 1: Policies and Practices Affecting U.S. Businesses and Investigation No. 332-586: Foreign Censorship Part 2: Trade and Economic Effects on U.S.Businesses

**COMMENTS OF**
**INTERNET ASSOCIATION**

On behalf of the world's leading internet companies, Internet Association (IA)[1] is pleased to submit the following comments to the United States International Trade Commission's (USITC) investigation of Foreign Censorship. In asking for this investigation, the Senate Finance Committee defined censorship as "the prohibition or suppression of speech or other forms of communication." Foreign governments around the world have taken to using digital policies to enact censorship on their citizens and in turn, restrict digital trade. IA supports policies that promote and enable internet innovation, ensuring that information flows freely and safely across national borders, uninhibited by restrictions that are fundamentally inconsistent with the open and decentralized nature of the internet.

For much of the world, the pandemic has only underlined the importance of digital policy. Business is increasingly conducted online, information flows keep the economy going, and the world has been able to stay connected while remaining socially distant. Nonetheless, countries around the world are increasingly proposing and enacting digital laws intended to censor their citizens and push back on the global nature of the free and open internet. Many of these policies are in direct conflict with Article 19 of the Universal Declaration of Human Rights -- which states that everyone has the right to seek and receive news and express opinions[2] -- as well as Article 20, and the general international requirements of legality, necessity, and proportionality.

China's and Russia's past calls for "cyber sovereignty" and siloed digital economies are now surfacing, in different forms, elsewhere around the world. Notably, since the European elections in 2019, European Union (EU) leaders have actively promoted an aggressive, multi-pronged approach towards "technology sovereignty" as one of the two main policy objectives for the current EU Commission. Under this new policy umbrella, the EU is proposing new regulatory 'ex-ante' rules that would apply almost exclusively to U.S. platforms (under a new, sweeping Digital Services Act (DSA)), as well as restrictions on cloud services, artificial intelligence, and data. EU officials have stated that the purpose of "digital sovereignty" is to create a "new empire" of European industrial powerhouses to resist American rivals. These unilateral regulations appear designed to discriminate against U.S. companies and take aim at a slice of the $517 billion U.S. digital export market.

Over the past year, some foreign governments have also devised new ways of targeting U.S. digital companies as a way to limit their citizens' access to information. Other countries are adopting policies at odds with the U.S. digital economy, and these nations are also actively pressuring their trading partners to adopt such policies. China's recent "Global Initiative on Data Security" is one example of China's desire to promulgate a vision of the internet and digital trade that runs contrary to U.S. interests and values. African nations have increasingly taken to blocking social media access during protests and contentious elections. Countries such as India, Brazil, and Egypt have moved forward with

[1] A complete list of Internet Association's membership can be found at: https://internetassociation.org/our-members/.
[2]United Nations. Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights

website blocking, or even shutting down the internet, as a way to censor citizens. In 2020, there were at least 155 documented internet shutdowns in 29 countries.[3] This follows 33 countries that shut down the internet in 2019 and 25 in 2018.[4] African countries such as Uganda and Nigeria have been at the forefront of partial platform bans and total internet shutdowns in 2021.

The digital industry is finding some of the strongest censorship pressure coming from traditional allies. Over the last few years, censorship laws have been introduced in places such as Germany with the Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG), the UK with the Online Harms bill, Australia with its Sharing of Abhorrent Material law, the EU with the DSA, and most recently Canada's proposed online safety bill. This proliferation of censorship laws by major U.S. allies is deeply concerning to the digital industry and has a significant economic and operational impact on U.S. businesses of all sizes.

A fundamental reason that the internet has enabled trade is its open nature – online platforms can facilitate transactions and communications among millions of businesses and consumers, enabling buyers and sellers around the world to form direct connections. This model works when platforms can host these transactions without automatically being held responsible for the vast amounts of content surrounding each transaction. In the U.S., Section 230 of the Communications Decency Act has enabled the development of digital platforms by ensuring that online services can host user content without being considered the "speaker" of that content. This law enables features such as customer reviews, which have been essential to building customer trust for U.S. small businesses in foreign markets.

However, this core principle, which allows U.S. services to function as platforms for trade and communication, is increasingly under threat at home and abroad. USTR has rightly identified "unreasonable burdens on internet platforms for non-IP-related liability for user-generated content and activity" as a barrier to digital trade in the last three NTE reports. Yet, the state of affairs has not improved. Foreign governments are exerting a heavier hand of control over speech on the internet and are subjecting online platforms to crippling liability or blockages for the actions of individual users for defamation, political dissent, and other non-IP issues. At the same time, foreign governments are making it more difficult for platforms to evolve new approaches for dealing with problematic content.

There is a global race to set the rules for the digital economy. The U.S. government should use trade and other bilateral deals to fight for the adoption of America's digital framework across the world and ensure equal access to the internet for all people. The following list is intended to highlight different forms of censorship policies. This list is not, nor is it intended to be, exhaustive of all troubling digital censorship laws around the world.

**Australia**

The Criminal Code Amendment (Sharing of Abhorrent Material) Act was rushed through Australia's Parliament in early 2019 with no public consultation, putting in place disproportionate and ambiguous provisions targeting the removal of online terrorism content.[5] The broad nature of the act means that citizens are censored for things they post. The act applies to an excessively broad range of technology companies and has increased compliance risks for U.S.-based social media, user-generated content and live streaming services, and hosting services. Its wide-ranging provisions do not consider the different business models of technology companies, nor does it take into account their varying capabilities or roles in facilitating the sharing of abhorrent violent material online. It is markedly out of step with approaches in other countries, particularly in terms of its excessively broad scope and notable differences from the regulatory framework applying to traditional media companies in Australia.[6]

[3] https://www.accessnow.org/keepiton-report-a-year-in-the-fight/
[4]Access Now and the #KeepItOn coalition. "Internet shutdowns report."
https://www.accessnow.org/cms/assets/uploads/2021/03/KeepItOn-report-on-the-2020-data_Mar-2021_3.pdf
[5]https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1201_first-senate/toc_pdf/1908121.pdf;fileType=application%2Fpdf
[6] https://www.nytimes.com/2019/04/03/world/australia/social-media-law.html

**Bangladesh**

The Digital Security Act of 2018 gives the government broad powers to suppress "information published or propagated in digital media that hampers the nation or any part therein in terms of nations unity, financial activities, security, defense, religious values, public discipline or incites racism and hatred", and created new criminal provisions prohibiting publication of content online that may be defamatory, harmful to religious values, or critical of the government.[7] Service providers may only defend themselves if they can prove that they took all possible steps to try to prevent the publication of material that violates the law or they will be subject to criminal penalties, including fines and/or imprisonment.

**Belarus**

Amendments to the Law on Mass Media made in 2018 have resulted in significant fines against media entities, including online blogs; new requirements to filter online content and government powers to mandate its removal; limitations on foreign ownership of media, including online media platforms; restrictions on disseminating foreign-owned content; requirements for identity records be kept on users posting online comments; and criminal liability for online platforms for content posted on their sites.

**Brazil**

Brazil has blocked WhatsApp multiple times as part of legal disputes related to specific users, cutting off access to a U.S.-based messaging service for more than one-hundred million Brazilians in the process.[8]

**Canada**

The Canadian government recently announced plans to combat online hate speech with a new bill dealing with "online harms" (C-36), as well as a forthcoming consultation on new obligations for online platforms to remove harmful content. The broad nature of the proposal means it can include content that is legal but still judged to be harmful, such as abuse that doesn't reach the threshold of criminality, and posts that encourage self-harm and misinformation.[9] Bill C-36 seeks to amend "the Canadian Human Rights Act to define a new discriminatory practice of communicating hate speech online, and to provide individuals with additional remedies to address hate speech; add a definition of "hatred" to section 319 of the Criminal Code based on Supreme Court of Canada decisions; and create a new peace bond in the Criminal Code designed to prevent hate propaganda offenses and hate crimes from being committed, and make related amendments to the Youth Criminal Justice Act."[10] Further, it is expected that the online platforms proposal will include a NetzDG-style model requiring removal of harmful content within specified timeframes, to be administered by a new regulator empowered to fine and block non-compliant sites and services, along with new mandatory reporting obligations to Canadian law enforcement. The overly broad nature of the proposal will likely result in censorship of Canadian speech and collateral harm to U.S. companies carrying such speech. While the digital industry strongly

[7] https://www.cirt.gov.bd/wp-content/uploads/2018/12/Digital-Security-Act-2018-English-version.pdf
[8] *See WhatsApp Officially Un-Banned In Brazil After Third Block in Eight Months*, The Guardian (July 19, 2016), https://www.theguardian.com/world/2016/jul/19/whatsapp-ban-brazil-facebook;https://www.theguardian.com/world/2016/jul/19/whatsapp-ban-brazil-facebook Glen Greenwald & Andrew Fishman, *WhatsApp, Used By 100 Million Brazilians, Was Shut Down Nationwide by a Single Judge* , The Intercept (May 2, 2016), https://theintercept.com/2016/05/02/whatsapp-used-by-100-million-brazilians-was-shut-down-nationwide-today-by-a-single-judge/.https://theintercept.com/2016/05/02/whatsapp-used-by-100-million-brazilians-was-shut-down-nationwide-today-by-a-single-judge/.

[9]Department of Justice Canada. Combating hate speech and hate crimes: Proposed legislative changes to the Canadian Human Rights Act and the Criminal Code. https://www.justice.gc.ca/eng/csj-sjc/pl/chshc-lcdch/index.html
[10]Department of Justice Canada. "News release: Government of Canada takes action to protect Canadians against hate speech and hate crimes" https://www.canada.ca/en/department-justice/news/2021/06/government-of-canada-takes-action-to-protect-canadians-against-hate-speech-and-hate-crimes.html

believes that hate speech is wrong, this proposal risks generating a whole new set of harms for Canadian citizens and digital companies.

The Canadian government also introduced Bill C-10, which extends Canada's broadcasting regulations to online platforms. Under Bill C-10, the Canadian Radio-Television and Telecommunications Commission (CRTC) is empowered to apply new "discoverability" obligations to any site of service hosting audio or audio-visual content (including "social media services") which would compel the service to give preferential treatment to Canadian content and creators. This has profound censorship implications, as it necessarily means non-Canadian audio and audio-visual communications will be demoted.

**China**

China imposes numerous requirements on internet services to host, process, and manage data (personal information and other important data gathered or produced within China) to be stored locally within China, and places significant restrictions on data flows entering and leaving the country.[11] China continues to moderate the public's access to websites and content online. On June 4, 2019, access to CNN was blocked[12] after the media company published a story on Tiananmen Square before the anniversary of the event.

China's restrictive requirements on data localization and cross-border information flows significantly impact foreign companies' ability to operate in the online space; they also create extra burdens and hurt related business prospects. The data localization requirement would extend the scope of Critical Information Infrastructure (CII) to all internet players, and mandates all original users' information be retained within China unless an authority's approval is obtained. A new draft Measures for Security Assessment of Personal Information Cross-border Transfer, released for comments in 2019, imposes cross-border data transfer restrictions on ordinary network operators and requires companies to obtain customer consent for cross-border transfers of their sensitive personal information. Expanding the scope of CII requirements will make ordinary data transfers much more complicated and inflict unnecessary burdens on foreign companies. In addition, an increased burden on MNCs was reflected in the Data Security Law (DSL). The law states that entities face legal liability outside of China if they "engage in data activities that harm the national security, the public interest, or the lawful interests of citizens or organizations" in China. The draft law also states China will establish a data security review mechanism, and data processors shall obtain licenses, cooperate with national security agencies, and go through data review processes for various data-related activities in China. China has also released more measures regarding data security, lacking necessary clarifications on key terms and procedures (e.g. clarification on important data and criteria for triggering a data security review, specific review procedures, etc.), bringing more ambiguity and uncertainty, and increasing the already complex and uncertain compliance burdens on MNCs.

In the world's biggest market, the services of many U.S. internet platforms are either blocked or severely restricted. Barriers to digital trade in China continue to present significant challenges to U.S. exporters.

China imposes numerous requirements on internet services to host, process, and manage data locally within China, and places significant restrictions on cross-border data flows.[13] China actively censors – and often totally blocks – cross-border internet traffic. It has been estimated that approximately 3,000 internet sites are completely blocked from the Chinese marketplace, including many of the most popular websites in the world. High-profile examples of targeted blocking of whole services include China's blocking of IA member companies Dropbox, Facebook, Google, Instagram, LinkedIn, Pinterest, Snapchat, Spotify, Twitch, Twitter, Vimeo, WhatsApp, and YouTube.

**Egypt**

[11] *Data localization,* AmChamChina, http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization

[12] https://techcrunch.com/2019/06/04/china-blocks-cnns-website-and-reuters-stories-about-tiananmen-square/

[13] *Data localization,* AmChamChina, http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization

Egypt President Abdel Fattah al-Sisi ratified a cybercrime law that obliges ISPs to block websites, whether hosted in Egypt or internationally, which are deemed to have committed a cybercrime that threatens national security, under threat of fines and/or imprisonment. Critics state that the law increases censorship and silences political opposition. In March 2019, Egypt's top media regulator, the Supreme Media Regulatory Council (SMRC), with support from President Abdel-Fattah al-Sissi, put into effect tighter restrictions for online content, allowing the government to block websites and social media accounts with over 5,000 followers if they are deemed a threat to national security.[14] State censorship continues, and in April 2019, internet service providers in Egypt blocked 34,000 internet domains to prevent the public from accessing the "Void" campaign opposing amendments to the Egyptian constitution, including U.S. and international NGO websites. Member companies including Facebook, Twitter, and Google continue to operate in Egypt.[15]

In May 2020, the SMRC issued Decree no. 26 of 2020, which enforces a strict licensing regime on Media and Press outlets, as well as both national and international online platforms. The regulation requires a 24-hour window for the removal of harmful content. It also obligates international companies to open a representative office in Egypt, while naming a liable legal and content removal point of contact. The regulation lacks safe harbor protections for international companies and stipulates an average of $200,000 in licensing fees. The fees are argued to exceed the ceiling stipulated in the media law of 2018 and are hence unconstitutional.

**Eritrea**

Eritrea is often ranked as one of the most censored digital countries in the world[16], with only 1% of the population online according to the U.N. International Telecommunication Union.[17] Social media is unable to operate in Eritrea, and reports indicate that citizens are heavily monitored in the event they can go online.

**European Union (EU)**

EU leaders are considering a range of content-related regulations, some aspects of which carry the risk of censoring European users online while increasing operational challenges for U.S. digital companies. The EU is currently debating updates to the E-Commerce Directive as part of the Digital Services Act (DSA).[18] While the digital industry supports the stated objective of the DSA to protect consumers and their fundamental rights online, there are concerns with potential unintended consequences from the proposal.[19] For example, while we acknowledge that not all services have the same level of resources, we see a concerning focus on "very large online platforms." To be truly effective, due diligence obligations should apply consistently to protect against content migrating from mainstream sites to less moderated platforms and social networks in the shadows. This is not a theoretical risk, and indeed migration of content is a worrisome trend that analysts have observed with terrorist content, violent extremism, and child sexual abuse imagery. As part of the debate on the DSA, we are also seeing concerning proposals that would risk infringing fundamental rights of EU users, such as stay-down obligations that would force intermediaries to perform general monitoring and lead to over-blocking of legitimate content. Finally, we would be concerned about further erosion of the country-of-origin principle, a cornerstone of the EU Single Market that ensures digital services have one set of rules rather than 27 different ones. This allows services, including SMEs, to scale up and offer their services across EU borders, and its preservation will be critical for post-COVID recovery.

[14]https://www.haaretz.com/middle-east-news/egypt/egypt-can-now-block-websites-social-media-accounts-deemed-a-threat-1.7041232
[15]https://madamasr.com/en/2019/04/16/news/u/egypt-blocks-over-34000-websites-in-attempt-to-shut-down-constitutional-amendments-opposition-campaign/
[16]Committee to Protect Journalists (CPJ) . Ten Most Censored Countries.
https://cpj.org/reports/2019/09/10-most-censored-eritrea-north-korea-turkmenistan-journalist/
[17]U.N. International Telecommunication Union. Digital Development Dashboard - Eritrea.
https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd_ERI.pdf
[18]https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[19]Summary Report on the open public consultation on the Digital Services Act Package.
https://ec.europa.eu/digital-single-market/en/news/summary-report-open-public-consultation-digital-services-act-package

One of the core objectives of the DSA is to better harmonize content laws across the EU. As the examples below demonstrate, services have had to contend with increasing legal fragmentation and a patchwork of national laws with overlapping and sometimes conflicting obligations.

**Germany**

The German NetzDG law mandates the removal of "obviously illegal" content within 24 hours and other illegal content within seven days. It covers provisions of the German Criminal Code connected to illegal content – including not just obviously illegal content related to terrorism and abuse, but also a wide range of other activities that are criminalized under German law, including incitement to hatred, insults, and defamation. Online services are subject to up to €50 million penalties if they are found to be out of compliance with this law. The law applies to online services with more than 2 million users in Germany, including a wide range of U.S. services. On July 2, 2019, German authorities announced a €2.3 million fine for Facebook for violating the NetzDG law.

It is difficult for online platforms to comply with this law due to its broad nature. A prime example is a court ruling on January 12, 2019. Despite NetzDG, the District Court of Tubingen in Germany ruled that Facebook violated its duties by deleting a comment which insulted right-wing extremists. The court argued that the user had not violated the platform's community standards, and that his comment was "covered by the freedom of opinion that indirectly binds Facebook to its customers in Germany."

Follow-up legislation has produced even more alarming requirements for services that severely undermine user privacy and turn private companies into an arm of law enforcement. The German "Repair Law" has now entered into force, allowing German authorities to request data -- including passwords -- from online providers. An update to the NetzDG, entering into force in 2022, will require social networks and video sharing platforms to share removed content and corresponding user data -- regardless of where the user is located -- automatically via an interface to the German Federal Crime Office. This would occur absent any specific legal process or prior notification to the user.

**Hungary**

In Hungary, legislation enables the order by local authorities of a 365-day ban of online content, such as websites and electronic applications that advertise passenger transport services.[20] More recently, Hungary passed a law prohibiting the portrayal of homosexual or transgender people in the content shown to minors. This deeply offensive law is in flagrant violation of the right to freedom of expression and information, and is immeasurably harmful to these protected groups.

**Hong Kong**

There have been concerns about the ability of Hong Kong to maintain a free and open digital ecosystem after the imposition of a national security law (NSL) on Hong Kong on June 30, 2020. The internet serves as a platform to exchange information and drive collaboration between both the public and private sectors. The Hong Kong government should continue to support a free and open internet, which is the foundation of digital trade.

While there has been no official confirmation, it was widely reported that Hong Kong authorities made use of the NSL to request that a hosting service provider take down websites set up by dissidents, and to also request that local internet service providers block several additional websites. The lack of transparency and reported use of the NSL to take down content and restrict website access raises significant concerns about censorship in Hong Kong.

[20] *See* Marton Dunai, *Hungarian Parliament Passes Law That Could Block Uber Sites*, Business Insider (June 13, 2016), http://www.businessinsider.com/r-hungarian-parliament-passes-law-that-could-block-uber-sites-2016-6.

When the ongoing review of the Personal Data (Privacy) Ordinance was discussed at the Legislative Council in May 2021, the government raised some concerning remarks that the authorities may prosecute the local staff of overseas platforms in case of failure to comply with the authorities' removal requests. Introducing severe sanctions, as well as implementing personal liability for the assessment of content take-down requests, has the consequence of encouraging online platforms to conduct little to no review of requests and instead resort to over-blocking content. This will inevitably have a grave impact on due process and pose long-term risks for freedom of expression and communication. The only way to avoid these sanctions for technology companies would be to avoid investing and offering their services in Hong Kong, thereby depriving Hong Kong businesses and consumers of access to digital services while also creating fresh barriers to trade. In addition, the government remarked that the authorities could block a website from being accessed in Hong Kong if a website consists of doxxing information. While reducing the spread of doxxing content is an important objective, shutting down or blocking the access of websites in their entirety would be a disproportionate response which is not conducive to maintaining a free and open internet.

**India**

Indian regional and local governments engage in a regular pattern of shutting down mobile networks in response to localized unrest, disrupting access to internet-based services.[21] In the National Trade Estimate, USTR correctly highlighted numerous problems with India's non-IP liability framework when it said:

> The absence of a safe harbor framework for Internet intermediaries discourages investment in Internet services that depend on user-generated content. India's 2011 Information Technology Rules have provided an insufficient shield for online intermediaries from liability for third-party user content: any citizen can complain that certain content is "disparaging" or "harmful," and intermediaries must respond by removing that content within 36 hours. Draft regulations announced in late 2018 (the "Information Technology (Intermediary Guidelines) Rules 2018"), threaten to further worsen India's intermediary liability protections. These draft rules would require platforms to become proactive arbiters of "unlawful" content, shifting the onus of the state to private parties. If these draft rules come into force, they will incentivize overly restrictive approaches to policing user-generated content, and will undermine many Internet-based platform services.[22]

Safe harbors from intermediary liability empower digital trade and enable a wide range of U.S. companies to access new markets. Where such safe harbors are incomplete or nonexistent, U.S. stakeholders in the digital sector – and small businesses that rely on consumer reviews or other user-generated content platforms to reach new customers – face significant barriers in accessing these markets.

Unfortunately, the publication of draft rules to amend India's intermediary guidelines include additional problematic requirements on issues such as the "traceability" of originators of the content, local incorporation requiring certain intermediaries to establish a physical office in India, proactive filtering, and compressed timelines for content removal.[23]

At the end of 2018, the IT ministry released draft changes to the Information Technology Act to impose more strict penalties for companies that fail to prohibit the spread of misinformation online. Platform "intermediaries" must trace the origins of information. This follows the IT ministry's attempt to amend Section 69A of the IT Act in 2018, which

[21] *India Shuts Down Kashmir Newspapers Amid Unrest*, Al Jazeera (July 17, 2016), http://www.aljazeera.com/news/2016/07/india-shuts-kashmir-newspapers-unrest-160717134759320.htmlhttp://www.aljazeera.com/news/2016/07/india-shuts-kashmir-newspapers-unrest-160717134759320.html; Betwa Sharma & Pamposh Raina, *YouTube and Facebook Remain Blocked in Kashmir*, New York Times India Ink Blog (Oct. 3, 2012), http://india.blogs.nytimes.com/2012/10/03/youtube-and-facebook-remain-blocked-in-kashmir/?_r=0http://india.blogs.nytimes.com/2012/10/03/youtube-and-facebook-remain-blocked-in-kashmir/?_r=0 (reporting on the practices of the Jammu and Kashmir governments to "increasingly [use] a communication blackout to prevent unrest in the valley.").

[22] https://ustr.gov/sites/default/files/2019_National_Trade_Estimate_Report.pdf

[23] http://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf

would enable the government to block apps and platforms that do not remove false information. On February 23, 2019, the Indian Draft National e-Commerce Policy was published with outlined proposals to change the rules for commerce online. The policy includes monitoring items listed for sale, and requires companies to remove prohibited items from sale no later than 24 hours after the item is flagged, block the seller, and notify relevant authorities. The draft also discusses content liability, stating that "it is important to emphasize on responsibility and liability of these platforms and social media to ensure the genuineness of any information posted on their websites."

The Supreme Court of India recently directed the government to issue guidelines to address social media misuse.[24] In 2018, India's Home Ministry ordered that Facebook, Google, and WhatsApp appoint local grievance officers responsible for establishing content monitoring systems and ensuring the "removal of objectionable/malicious contents from public view." The Ministry also reviewed actions taken to prevent misuse of the platforms to spread rumors, cause unrest, or incite cyber crimes or any activities going against national interest.

The Guidelines have a significant impact on many businesses and users through the imposition of new requirements on a large range of internet-based service providers, with a focus on those that operate social media, messaging, and streaming news and entertainment services. These rules create significant risks to users, businesses, and society at large. The threat of heavy sanctions, including sanctions that apply directly to companies' employees, has the very real potential to incentivize over-blocking of online content, which could have a particularly detrimental effect on political speech.

The rules were ultimately rushed through without final stakeholder engagement or notification, leaving the U.S. industry exposed to substantial compliance burdens and liability exposure—jeopardizing not just the legal stability of the safe harbor, but also the safety of personnel on the ground. Considering the potential chilling effect these rules may have on human rights and future investment, this new legislative framework presents a major challenge from both an economic and societal perspective. The law will lead to over-removal and censorship of legitimate content, including political speech. Social media companies regularly receive overly broad removal requests from both users as well as government agencies. Analyses of cease-and-desist and takedown letters have found that many seek to remove potentially legitimate or protected speech. One analysis of cease and desist and takedown letters found almost 50 percent of requests targeted potentially legitimate or protected speech.[25]

The new legislation's lack of clarity and threat of severe penalties also presents several significant practical and legal challenges, many of which will chill legitimate innovation and investment in services and products that bring benefits to consumers as well as India's general socio-economic development. Overall, broad data retention rules increase privacy risks for users and the right to presumption of innocence. [26] In addition, the threat to employee safety through personal liability provisions (on the Chief Compliance Officer) in the law is particularly worrisome. It is a radical departure from safe harbor provisions afforded to intermediaries under the IT Act, and presents serious human rights concerns by incentivizing over-blocking due to the need to avoid harsh personal sanctions.

There are also significant questions regarding the impact of this law on users that are outside of India, and the potential conflicts of law and related concerns that would arise accordingly. Indeed, the data and law enforcement requirements, in particular, would seem to have an impact on the privacy/other rights of users in other jurisdictions as well. With these requirements, companies would be forced to extend data retention for users regardless of where they are situated, if their content or account was targeted by a removal order, thus having an extra-territorial global application that has extensive ramifications for trade and data protection agreements with third countries, as well as ethics and human rights.

[24] https://www.livemint.com/news/india/sc-flags-tech-pitfalls-asks-centre-to-curb-social-media-misuse-1569350515906.html
[25] https://ncac.org/fepp-articles/will-fair-use-survive-free-expression-in-the-age-of-copyright-control
[26] https://cdt.org/wp-content/uploads/pdfs/CDT_Data_Retention-Five_Pager.pdf

For these and other reasons the Association for Progressive Communications, the Committee to Protect Journalists, Derechos Digitales, the Electronic Frontier Foundation, Human Rights Watch, Mnemonic, Reporters Without Borders, and WITNESS have issued a joint statement urging the Indian government to withdraw the new rules.[27]

**Indonesia**

Indonesia's "Draft Communications & Informatics Ministerial Regulation on the Governance of Electronic Systems Providers for Private Scope" targets online services and would require platforms to take responsibility for a very broad list of content types, including content with no clear definition such as "creating public disturbances and disorder" to be removed with a very short turnaround time (i.e. certain content types must be removed within two hours from the time of notice).[28] This regulation, which is part of the broader package of OTT regulations discussed below, will present significant market access barriers to U.S. providers in Indonesia.

**Mexico**

A bill on cybersecurity establishes certain broad monitoring obligations for ISPs to "discover" possible online crimes and stop that content's transmission (without judicial or administrative order). Further, a broad felony is set forth to criminalize online platforms as intermediaries due to the uploading of illegal content.

**Nigeria**

Nigeria is pursuing new digital laws that censor its citizens. A draft bill to amend the Nigerian Broadcasting Commissions (NBC) Act has been tendered to extend the regulatory powers of the NBC to include all online media.[29] The proposed amendments to the NBC Act significantly extend the existing National Broadcasting Act through pushing penalties for violating licensing terms (Section 2) that (a) confer power on the Commission to ensure regulatory control is applied across all broadcasting services including online broadcast and any other medium of broadcasting; and (b) mandate licensees to comply with terms and conditions of its license, the provisions of the Act and any subsidiary legislation, with liability including fines, imprisonment for up to a year, and forfeiture of property, facilities, installations, and equipment. Additionally, the draft bill excludes court oversight (Section 19D), which gives the NBC power above Nigerian courts and the legislature to issue directions in writing to any licensee regarding the compliance or non-compliance of any license conditions or provisions of the Act. The draft bill gives power to the Minister to give Directives (Section 19R) granting the Minister power to give the Commission directives of a general character relating generally to particular matters concerning the exercise of the Commission's functions under the Bill, effectively hindering accountability and the freedom of Nigerians to question the actions and inactions of their government.

In addition to the proposed broadcasting bill amendment, a significant number of regulatory changes are being proposed to give regulatory oversight powers (licensing, compliance, etc) to ministries and agencies. These include the National Film & Video Censorship, Classification, and Exhibition Regulatory Commission Bill; the National Information Technology Development Agency Bill; and The Press Council bill. Initial review shows that the Ministers in charge would have extensive non-judicial powers to regulate platforms and content providers, including requirements to obtain licenses to operate (often under multiple licensing regimes), and penalties including punitive fines and jail terms.

**North Korea**

The North Korean government actively censors its citizens and completely controls the entire internet within its

[27] https://www.accessnow.org/india-censorship-privacy-free-speech/
[28] https://www.telegeography.com/products/commsupdate/articles/2016/05/05/mcit-issues-draft-regulation-on-ott-in-indonesia/
[29] https://www.premiumtimesng.com/news/headlines/468219-undeterred-by-public-outcry-nigerian-govt-wants-its-media-censorship-to-include-all-online-media.html

borders. IA member companies are unable to operate in North Korea or have access to its citizens, who are unable to use social media and search engines, read news sites, or use torrents or VPNs. The only source of political news in the country is the content created by The Korean Central News Agency (KCNA).[30]

**Pakistan**

In February 2020, the Ministry of Information Technology and Telecommunication (MOITT) posted on its website the Citizens Protection (Against Online Harm) Rules.[31] The Rules contain onerous requirements including forced local office presence, forced storing of user data within Pakistan, and new procedures that would contravene both Pakistani and international laws and norms around disclosure of user data and intermediary moderation of online content. The government announced in March that a committee led by the Pakistan Telecommunication Authority would conduct an "extensive and broad-based consultation process with all relevant segments of civil society and technology companies." However, a revised version of the Rules has not been circulated, and a broad-based consultation has not yet occurred.

**Russia**

Since 2012, Russia has been implementing a Blacklist law initially aimed at protecting children from harmful information online. The Blacklist law keeps getting expanded onto new types and categories of content including extremist, suicide-inciting, drugs-promoting, etc. By this law, intermediaries are envisioned to block certain sites or certain types of content.[32] For example, Russia ordered all of Wikipedia to be blocked due to problematic content on a single page.

On March 18, 2019, Putin signed laws No.30-FZ and No. 31-FZ, which prohibit spreading misinformation and insults of government officials online. The laws target online information that presents "clear disrespect for society, government, state symbols, the constitution, and government institutions." Russian authorities can block websites that do not remove information that the state assesses is not accurate, and the law allows prosecutors to direct complaints to the government about material considered insulting to Russian officials, which can then block websites publishing the information.

On May 1, 2019, Putin signed a new law into effect titled the Internet Sovereignty Bill. The bill was introduced in February 2019 to route Russian web traffic and data through points controlled by state authorities. The law also introduced the building of a national Domain Name System, and provided the installation of network equipment that would be able to identify the source of web traffic and block banned content. The law took effect on November 1, 2019.

In December 2019, Russia adopted a law requiring the pre-installation of Russian software on certain consumer electronic products sold in Russia. The Russian government has not yet identified the types of electronic products which should have Russian software, or the specific applications that will be required for pre-installation. However, there is an understanding that the scope of devices covered will likely include smartphones, computers, tablets, and smart TVs; applications that will be covered are likely search engines, mapping and navigation software, anti-virus software, software that provides access to e-government infrastructure, instant messaging and social network software, and national payment software. The law went into force in January 2021.

**Singapore**

[30]The Korean Central News Agency (KCNA). https://kcnawatch.org/
[31] https://moitt.gov.pk/SiteImage/Misc/files/CP%20(Against%20Online%20Harm)%20Rules%2c%202020.pdf
[32] *See New Russian Anti-Piracy Law Could Block Sites "Forever,"* Torrent Freak (Apr. 25, 2015), https://torrentfreak.com/new-russian-anti-piracy-law-could-block-sites-forever-150425/.

On Oct 2, 2019, Singapore's Protection from Online Falsehoods and Manipulation Bill (Bill No. 10/2019), came into force as a measure to curb misinformation. The law would allow any Minister to instruct a competent authority to issue orders for corrective action, and require online media platforms to carry corrections, when (i) the statement is a false statement of fact *and* (ii) if a correction is in the public interest. The law requires media outlets to correct false news and to "show corrections or display warnings about online falsehoods so that readers or viewers can see all sides and make up their mind about the matter." Internet intermediaries are required to either take down the content or show corrections about the falsehoods on their platforms. The legislation was hastened after the Law Ministry stated that Facebook declined to take down a post the government declared as false.

**Thailand**

Internet service providers who "assist or facilitate" the commission of defamation by another person can be liable as supporters of the defamatory offenses, even if the actor does not realize they are assisting or facilitating the offense.[33] One webmaster faced a sentence of up to 32 years in jail under the "Lèse Majesté" law for allowing comments on an interview with a Thai man known for refusing to stand at attention during the Thai Royal Anthem.[34] Such rules have resulted in the blockage of U.S. online services in Thailand.

**Turkey**

Turkey adopted the "Law on Amendment of the Law on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications" (widely known as the social media law) in July 2020. The law requires social network providers with more than a million users to (i) establish a representative office in Turkey, (ii) respond to individual complaints in 48 hours or comply with official take-down requests of the courts in 24 hours, (iii) report on statistics and categorical information regarding the Requests every 6 months, and (iv) take necessary measures to ensure the data of Turkish resident users are kept in Turkey. In case of noncompliance, social network providers face serious monetary fines and 50-90 percent possible bandwidth reduction to their platform. While these amendments aim to regulate social network providers and enhance the obligations of hosting and content providers to protect the individuals in the internet environment, the vague obligation of data localization may require significant and costly operational changes for businesses, and facilitating the execution of content removal/access blocking decisions raises significant concerns that it may lead to censorship of unwanted contents and may hinder free speech of individuals.

**United Arab Emirates (UAE)**

The National Media Council Content Creators law applies to UAE residents and influencers operating in the UAE, including all social influencers who use their social media channels to promote and/or sell products. The law puts the responsibility on the owner of the account to obtain the license for their activities, and covers a broad scope, including "any paid or unpaid form of presentation and/or promotion of ideas, goods, or services by electronic means, or network applications". Influencers will need to clarify the content that is sponsored and/or paid vs. editorial content on their social channels. The cost of the license is 15,000 AED and is valid for 12 months. The law is very selectively enforced and the NMC has the power to use it to respond to complaints made against a particular individual. Such onerous licensing requirements covering a broad scope of social influencing activities add unnecessary friction to digital trade and inhibit new social influencers, particularly those based outside of the UAE, but they also hinder the UAE market from participating in the UAE digital economy.

[33]https://www.law.uw.edu/media/1423/thailand-intermediary-liability-of-isps-defamation.pdf
[34]https://www.eff.org/deeplinks/2012/05/suspended-sentence-good-news-thai-webmaster-jiew-threat-freedom-expression-remains

UAE's cybercrime laws contain several provisions that can act as market barriers to foreign players engaging and participating in the UAE digital market. These include:

- A penalty of imprisonment and a fine not exceeding AED 1,000,000 may be imposed on any person who creates or runs an electronic site or any IT means, to deride or to damage the reputation or the stature of the UAE or any of its institutions, the President of the UAE, the Vice President, any of the Rulers of the Emirates, the Crown Princes, the Deputy Rulers, the national flag, the national anthem, the emblem of the state, or any of its symbols;
- Producing, transmitting, publishing, and exploiting through an electronic site, gambling and/or pornographic material or any other material that may prejudice public morals;
- Insulting others or attributing to another an incident that may make him/her subject to penalty or contempt by others by using an electronic site;
- Using electronic sites to display contempt for any holy symbols, characters, figures, and rituals of Islam, including the Divinity and the Prophets, and for any other faiths or religions and any of their symbols, characters, figures, and rituals.

**United Kingdom (UK)**

In May 2021, the UK government published a draft Online Safety Bill that, if enacted into law, would lead to significant censorship and create major compliance issues for U.S. companies operating in the UK.[35]In the bill, the UK government proposes, among other things, to apply a new legal "Duty of Care" on a "wide range of companies of all sizes," including user-to-user services and search engines." The Duty of Care would require companies to protect users from a wide range of "online harms." Because the definition of "harmful" content is so vague, the bill pushes services to err on the side of over-removal. The collateral damage is the free expression of UK citizens. In meeting the duties of care, services in scope will have to undergo general monitoring of all the content on their services. Powers given to the regulator could include a requirement to break encryption.

The digital industry is concerned that the scope of the proposal is extremely wide-ranging, and the text complex and unclear. This lack of definition leaves services without a clear picture of what to expect, and how to ensure they are meeting their duties. Definitions are vague, and significant details left to the UK Secretary of State and the regulator to fill in at a later time. Therefore, the unintended consequences for UK citizens and American companies is, by design, still not fully understood.

Any proposal needs to be more targeted and practical for both big and small platforms to implement. As drafted, the proposals would potentially restrict access to key digital services that enable small businesses to grow and reach new markets. The digital industry is also concerned that the proposed rules would disrupt the ability of startups and small businesses to build new digital services and to use existing user review and feedback mechanisms to connect with global customers. The UK Government wants this bill to be world-leading, but it sets a poor -- and dangerous -- example.

**Vietnam**

Vietnam's Ministry of Information and Communications has introduced a new decree on the use of Internet Services and Online Information that includes an excessively short three-hour window for compliance with content takedown requests, as well as numerous other market access barriers highlighted below.[36]

[35]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf
[36] Draft Decree Amending Decree 72/2013-ND-CP on the Management, Provision and Use of Internet Services and Information Content Online.

Unfortunately, the requirements in this decree deviate from international standards on intermediary liability frameworks, and would present significant barriers to companies seeking to do business in Vietnam. Online services often require more than three hours to process, evaluate, and address takedown requests, particularly in situations where there are translation difficulties, different potential interpretations of content, or ambiguities in the governing legal framework.

As USTR identified in the 2016 National Trade Estimate, a similar intermediary liability provision in India has forced U.S. services "to choose between needlessly censoring their customers and subjecting themselves to the possibility of legal action." IA urges USTR to take similar action on this Vietnamese decree and to highlight that this decree would serve as a market access barrier. In addition, IA encourages USTR to work with Vietnam and other countries to develop intermediary liability protections that are consistent with U.S. law and relevant provisions in trade agreements, including Section 230 of the Communications Decency Act and Section 512 of the Digital Millennium Copyright Act.[37]

This draft decree also includes long and inflexible data retention requirements, a requirement for all companies to maintain local servers in Vietnam, local presence requirements for foreign game service providers, requirements to interconnect with local payment support service providers, and other market access barriers that will harm both U.S. and Vietnamese firms.

IA urges the U.S. government to press Vietnam for greater transparency and public input into the development of internet-related proposals. This recent decree was publicized on a Friday, and comments on the decree were due on the following Monday. Such short windows do not provide sufficient time for expert input into the development of complex regulations and are inconsistent with Vietnam's obligations under Chapter 26 of the TPP ("Transparency and Anti-Corruption") to provide for notice-and-comment processes when developing new regulations.

**Conclusion**

Digital policies are increasingly being used by governments around the world to censor their citizens, which harms U.S. digital companies' ability to operate. These censorship laws are found in countries such as China, Russia, and North Korea, but some of the strongest censorship pressure is coming from traditional U.S. allies. The censorship policies have taken the form of complete service blockage and strict rules on how information can be posted or accessed online. To operate in some foreign jurisdictions, U.S. digital companies are forced to limit services, comply with complex rules, and even face criminal exposure. The U.S. government should use trade and other bilateral deals to fight for the adoption of America's digital framework across the world and ensure equal access to the internet for all people.

[37] In particular, Vietnam must at a minimum include express and unambiguous limitations on liability covering the transmitting, caching, storing, and linking functions for its ISP safe harbors; revise Article 5(1) of Joint Circular No. 07/2012 to provide a safe harbor for storage rather than just "temporary" storage; and clarify that it's safe harbor framework does not include any requirements to monitor content and communications.