Before the
OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE
Washington, DC 20508

In the Matter of	)	
	)	
Significant Foreign Trade Barriers for the 2025 National Trade Estimate Report	)	Docket No. USTR-2024-0015

Comments of the Internet Infrastructure Coalition

Pursuant to the request for comments published by the Office of the United States Trade Representative (USTR) in the Federal Register on Sept. 3, 2024, the Internet Infrastructure Coalition (i2Coalition) submits the following comments concerning Significant Foreign Trade Barriers for the 2025 National Trade Estimate Report. The i2Coalition is made up mainly of small to medium-sized businesses, which are cloud providers, data centers, web hosting companies, registrars, registries, and other foundational Internet enterprises.

I. Introduction

The global Internet fosters economic growth and international trade, empowering small and medium-sized U.S. enterprises to reach new markets. However, the rising implementation of Internet shutdowns, global site-blocking regimes, and efforts to block virtual private networks (VPNs) present a significant and growing trade barrier. These actions, often enacted under the guise of domestic policy, threaten to fragment the open Internet and limit and distort access to U.S.-based services and websites, disproportionately affecting smaller U.S. companies and technology service providers. As authoritarian governments adopt restrictive measures targeting U.S. platforms, the risks of censorship, economic exclusion, and the curtailing of Internet freedom intensify.

We urge the USTR to prioritize open, non-discriminatory digital trade frameworks that protect the free flow of information and ensure a secure and resilient global Internet. The open Internet principles championed by the U.S. government for the past twenty years have facilitated the preeminence of the U.S. technology sector. Moreover, they are essential to U.S. exports, economic growth and security, and technological innovation, and must be safeguarded from restrictive policies abroad.

II. Global Principles Related to Internet Access

Governments around the world have recognized the importance of maintaining access to the Internet as an enabler for trade, economic development, and fundamental human rights. From

the U.S. perspective, an open and free Internet is essential for U.S. companies, allowing them to access global markets, connect with international customers, and scale their businesses across borders without unnecessary restrictions. As highlighted by the Declaration for the Future of the Internet[1]—a multilateral initiative supported by the United States—an open and reliable Internet is crucial for economic growth, democratic values, and global cooperation. The Declaration underscores principles such as universal access to the Internet, respect for human rights, and the free flow of information across borders.

Disruption or limitation of access to the global Internet has been identified as inconsistent with applicable international law when the disruption is not proportionate to the harm. The Office of the United Nations High Commissioner for Human Rights has set out six essential requirements for restrictions on Internet access. Restrictions must be: (1) clearly grounded in unambiguous publicly-available law; (2) necessary to achieve a legitimate aim; (3) proportional to the legitimate aim and the least intrusive means to achieving the end, so, accordingly, they should be as narrow as possible, in terms of duration, geographical scope and the networks and services affected; (4) subject to prior authorization by a court or another independent adjudicatory body; (5) communicated in advance to the public and telecommunications providers; and (6) subject to meaningful redress mechanisms available to those whose rights have been affected.[2] Blocking efforts with indiscriminate and widespread impacts, like Internet shutdowns, very rarely meet the proportionality test.[3]

Similarly, the Freedom Online Coalition, a worldwide organization of 41 government members, has condemned Internet shutdowns and network disruptions because of the impact on human rights and encouraged governments to address the economic, social and political risk of these sorts of network disruptions in bilateral and multilateral engagements, encouraging partners to refrain from such intentional disruptions.[4] The European Court of Human Rights has also weighed in on questions of website blocking, ruling that website blocking that results in collateral blocking of non-targeted websites and does not provide proper safeguards against abuse violates the European Convention on Human Rights,[5] and that decisions to block access to

---

[1] Declaration for the Future of the Internet, available at https://www.state.gov/declaration-for-the-future-of-the-internet.

[2] Report of the Office of the United Nations High Commissioner for Human Rights. "Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights," 13 May 2022, available at https://documents.un.org/doc/undoc/gen/g22/341/55/pdf/g2234155.pdf.

[3] Id.

[4] See Freedom Online Coalition Joint Statement on Internet Shutdowns and Elections (October 2023) available at https://freedomonlinecoalition.com/joint-statement-internet-shutdowns-and-elections/ and FOC Joint Statement on State Sponsored Network Disruptions (March 2017) available at https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-and-Accompanying-Good-Practices-for-Government-on-State-Sponsored-Network-Disruptions.pdf.

[5] Vladimir Kharitonov v. Russia (application no. 10795/14), OOO Flavus and Others v. Russia (application nos 12468/15, 23489/15, and 19074/16), Bulgakov v. Russia (no. 20159/15), and Engels v. Russia (no. 61919/16), ECHR 183 (2020).

entire websites when the website was not provided notice or an opportunity to remove allegedly illegal material was "unlawful and disproportionate."[6]

The international law mandates, some of which are highlighted above, are clear. Governments must avoid limiting Internet access except in exceptional circumstances, ensure that any limits are proportional in geographical scope and the services and content affected, and provide due process and redress mechanisms. Notwithstanding these clear legal principles, governments around the world are using shutdowns and network-based blocking as a sweeping, first-step tool to address a range of harms, often without adequate oversight or controls. Because these network-blocking efforts can be circumvented due to the nature of the global Internet, governments have also recently begun pushing to extend these network-blocking efforts to global Internet infrastructure providers, including VPNs, content delivery networks (CDNs), and global Domain Name System (DNS) providers. These regimes are not reflective of international norms that emphasize the importance of free trade and digital connectivity. They also set a dangerous precedent by promoting Internet fragmentation, which can lead to a patchwork of restrictions that limit the Internet's full economic potential.

III. Government-Imposed Internet Shutdowns and Network-Blocking as a Trade Barrier

Efforts to limit the free flow of information through Internet shutdowns or network blocking lead to significant disruptions to digital trade, restricting the ability of U.S. businesses to reach international markets and customers. Such barriers distort the natural dynamics of commerce, skewing competition and placing U.S. companies at a disadvantage in the global economy.

For U.S. companies whose only meaningful mechanism for reaching a particular market is through the Internet, Internet shutdowns or limitations cut off access to the market. Businesses face lost revenue, business disruption, and difficulty in maintaining customer relationships, among other harms. The significant economic costs of Internet shutdowns are felt both within the country and among the country's trading partners.

Government-mandated network blocking, particularly when applied to global Internet services, poses significant trade and operational concerns for U.S. businesses and Internet services. Such restrictions, often introduced under the guise of protecting national interests or preventing illegal content, fundamentally threaten the free and open nature of the Internet. They create formidable barriers for U.S. businesses that rely on global Internet infrastructure to market and deliver goods and services in global commerce.

Although blocking regimes where governments issue orders to local Internet Service Providers (ISPs) to prevent access to content is not new, network blocking efforts have ballooned in recent

[6] Taganrog LRO and others v. Russia, ECHR 179 (2022) available at https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-217535%22]}

years, expanding to new types of providers, new jurisdictions, and new types of content. These blocking regimes often lack adequate controls or oversight by independent parties, resulting in significant amounts of collateral blocking of untargeted content with no opportunity for redress. In addition, because the global Internet offers a wide range of opportunities to circumvent an ISP's efforts to block, countries have sought to expand their blocking regimes to global cloud, DNS, and VPN providers, ignoring legal requirements for restrictions to be proportional and threatening to splinter the global Internet.

Network-based blocking impacts the foundational layer of the Internet, making it a uniquely potent form of censorship. It targets domain names or IP addresses, preventing users from resolving websites and effectively making entire digital services unreachable. When governments impose such blocks, they result in severe economic and operational consequences that disproportionately affect U.S. companies, particularly small and medium-sized enterprises (SMEs) reliant on cross-border access to provide their services. With blocking regimes emerging as a non-tariff barrier, the increased cost of compliance is likely to have a disproportionate impact on small businesses. In the United States, small businesses are the backbone of the U.S. economy and the primary source of jobs for Americans. The success of small businesses is crucial for the national economy, as they make up 99.7% of all companies in the United States.[7] Trade presents a tremendous opportunity for small businesses to grow, with 95% of the world's customers living outside U.S. borders.[8]

These consequences are exacerbated when governments fail to implement appropriate controls or checks on blocking activity and apply network blocks that extend far beyond targeted content. There have been numerous examples, for instance, of ISPs blocking the IP addresses of cloud infrastructure in order to block a single website, even though the same IP address is used to access hundreds, thousands, or even tens of thousands of unrelated websites.

Digital trade distortion concerns erupt when network blocking is enforced globally on global providers, as actions taken by one nation-state can have far-reaching consequences beyond its borders. This extraterritorial application of censorship disrupts the availability of U.S. digital services worldwide, reducing market access and undermining trade principles established by international agreements and bodies like the World Trade Organization (WTO). Moreover, such measures often lack transparency, due process, and safeguards against overreach, leading to an arbitrary application of restrictions and a chilling effect on free speech.

Blocking at the global DNS resolver level is especially problematic. By refusing to return an IP address in response to requests for a particular website, a DNS resolver can make it appear like an entire website has effectively disappeared from the Internet to an individual using that resolver. A block in a resolver doesn't preclude an Internet user from navigating to a website in

[7] https://advocacy.sba.gov/wp-content/uploads/2023/03/Frequently-Asked-Questions-About-Small-Business-March-2023-508c.pdf

[8] https://www.sba.gov/business-guide/grow-your-business/export-products#:~:text=Nearly%2096%25%20of%20consumers%20live,power%20is%20in%20foreign%20countries.

a myriad of other ways. A user can use an alternative resolver, build their own resolver, or simply type in the website's IP address. Furthermore, the way DNS blocking works — declining to return an IP address — typically means there is no explanation provided to an individual as to why they were unable to access the website at issue. Although there have been proposals for protocols that would allow an error code to be returned in such cases, nothing has yet been implemented. DNS level blocking, therefore, not only restricts access but can fragment the global Internet, jeopardizing the trust and integrity of the DNS as a core global infrastructure. As highlighted, it clearly incentivizes the use of circumvention tools, potentially pushing users toward less secure alternatives, thereby increasing cybersecurity risks and exacerbating digital divide issues.

While governments may seek to justify DNS blocking as necessary for immediate national security, public safety, or other law enforcement reasons, the long-term trade implications are vast. U.S. services are left vulnerable to inconsistent, non-transparent enforcement actions that lack international cooperation, putting them at a disadvantage in foreign markets. U.S. firms face economic harm from reduced access to consumers, lost advertising revenue, and operational disruptions, further amplified in markets where alternative services are controlled or heavily influenced by state actors.

To address these concerns, the USTR should advocate for digital trade policies that limit government-imposed blocking to narrowly defined, transparent, and legally sound circumstances. Such restrictions should be subject to international standards, ensuring that enforcement actions align with principles of necessity, minimal restrictiveness, and due process. By doing so, the USTR can help safeguard the openness and accessibility of the global Internet while promoting fair market access for U.S. technology firms.

IV. Threats of Internet Fragmentation

Internet fragmentation divides the global Internet into distinct, often regionally or nationally controlled, sections, harming the free flow of digital commerce and information across borders. This fragmentation occurs when countries implement restrictive regulations, such as Internet shutdowns or site-blocking regimes, which limit access to certain online content or services. Fragmentation also creates isolated national or regional networks, where access to global content is curtailed by government-imposed restrictions. This undermines the very idea of the Internet as a unified, open platform for innovation, communication, and trade. As a result, businesses—particularly those based in the United States and other open Internet economies—face challenges in accessing global markets. U.S. companies that rely on the free exchange of information and goods across borders are particularly vulnerable, as they are unable to reach customers or markets where site-blocking is in effect, stifling digital trade and innovation.

The methods used for network-based blocking also increase the risks and impacts of Internet Fragmentation. DNS services play a foundational role in the functioning of the Internet by translating human-readable domain names into IP addresses that devices utilize for

communication. At its core, the DNS is and always has been structured to reflect a single, unified global system anchored in the root zone managed by neutral global entities. DNS resolvers copy and cache the data from the root zone to provide users with seamless and reliable access to websites and services, facilitating the interconnectedness that drives digital trade and global communication.

When governments impose restrictions at the DNS resolver level, they introduce inconsistencies that fragment this carefully structured system. Essentially, these restrictions require DNS operators to alter their responses in this global system depending on where a user might be located based on government direction. Fragmentation of the DNS undermines the principle of a single, global Internet by creating “splintered” networks, where the experience and access to content differ depending on a user’s geographic location or their resolver’s restrictions. In addition, although a locally operated private DNS resolver operated by a telecommunications company that operates only in a single country might be able to modify *all* of its responses to comply with a government order, the compliance of a global DNS resolver is necessarily far more complicated. Either the DNS operator alters their answer for all users around the world - resulting in a global blocking of the site - or the DNS operator must determine where a user is located and maintain an extensive list of what answers must be returned in each location. This is entirely contrary to the idea of a single, unified global system.

Such actions imposed on the DNS not only disrupt the open flow of information but also interfere with trade, as businesses and consumers are unable to reliably connect across borders. For USTR, the concern is clear: a fractured Internet impairs the global economy by limiting market access, harming innovation, and undermining the free flow of goods and services that rely on a unified Internet. Fragmentation threatens U.S. companies’ ability to reach international markets, depriving them of opportunities for growth, and leaving them vulnerable to uneven market access.

The consequences of this fragmentation are not limited to businesses. Consumers are also denied the opportunity to benefit from the global digital economy, as they may be restricted from accessing educational resources, entertainment platforms, or e-commerce sites that operate internationally. This erosion of Internet openness threatens to reduce global connectivity, prevent knowledge sharing, and restrict the benefits of technological progress.

Preserving the integrity of the global DNS is crucial for maintaining an open, secure, and resilient Internet that supports international trade. USTR has a vested interest in ensuring that the global digital marketplace remains cohesive, avoiding policies that could splinter the Internet or unfairly target neutral intermediaries. By advocating for a unified approach to Internet governance and resisting policies that promote fragmentation, USTR can protect the future of digital trade and uphold the principles of an open global economy.

V. Alignment with U.S. Government's Efforts to Promote Competitiveness

The i2Coalition's recommendations align with the U.S. government's broader trade goals, such as those highlighted by the Department of Commerce's International Trade Administration (ITA). Their recent initiatives emphasize the importance of supporting SMEs in global digital trade, particularly through policies promoting data flows and addressing trade barriers. Similarly, USTR must ensure that site-blocking regimes and Internet fragmentation do not undermine these goals, as they pose significant risks to the competitiveness of the very businesses that have led the world in successfully building and operating the global Internet and which the ITA seeks to support.[9]

VI. Country-Specific Concerns

Given the increasing number of countries employing Internet shutdowns and network blocking to control access to the availability of services within their borders, it is challenging to document all instances where countries have limited digital trade through such network restrictions and blocking. The Internet Society, for example, has identified more than 120 Internet shutdowns so far in 2024.[10] In its most recent Freedom on the Net report, Freedom House has estimated that 65 percent of the world's Internet users live in countries where websites hosting political, social, or religious content is blocked, and 48 percent of the world's Internet users live in countries where authorities disconnect Internet or mobile networks, often for political reasons.[11] Nonetheless, some specific, illustrative examples of countries using Internet shutdowns or network blocking in ways that impact trade are included below.

A. Bangladesh

In July 2024, the Bangladesh government implemented a ten-day complete mobile Internet blackout across the country, largely considered a government tactic to suppress legitimate citizen protests regarding perceived government injustices.

Bangladesh has a thriving tech sector with 4,500 companies that employ more than 750,000 people and generate around USD 1.4 billion per year in export income from clients in about 80 countries. The blackout resulted in estimated losses of at least USD 300 million[12], illustrating the economic significance of Bangladesh's digital sector. Telecom operators reported daily losses of

---

[9] https://www.trade.gov/press-release/international-trade-administration-announces-efforts-advance-us-competitiveness-and; https://www.commerce.gov/news/fact-sheets/2024/09/fact-sheet-international-trade-administration-efforts-advance-us

[10] https://pulse.internetsociety.org/shutdowns

[11] https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf at 3.

[12] https://restofworld.org/2024/bangladesh-internet-blackout-tech-industry/

USD 2.9 million due to the Internet outage, while the digital commerce sector (e-commerce, logistics, and ride-hailing services) reported losses of USD 5 million per day.[13] In addition, with one of the fastest-growing developer populations and the world's second-largest online freelance workforce, Bangladesh has about 650,000 freelancers[14] that rely on Internet connectivity in order to support their technology clients from around the world, including those in the U.S.[15]

The Internet shutdown also significantly impacted global business in Bangladesh. Global companies struggled to communicate with their employees, vendors, suppliers, and customers. Global technology companies had challenges delivering Internet-based technology products and services to Bangladesh customers during this period. Physical supply chains, from ports to airports, were also significantly disrupted from the outage, which particularly impacted the global fast-moving consumer goods (FMCG) sector, in which Bangladesh increasingly plays a key role. Bangladesh Bank data reflects that net FDI inflow decreased to USD 3.8 billion in the July-May period, down 6.5 percent from USD 4 billion during the same period in 2023[16].

B. France

France has a number of laws that enable regulators or other stakeholders to use network blocking as a mechanism to prevent the dissemination of certain types of content. Article L. 333-10 of the French Sports Code, for example, allows sports broadcasting rights holders to bring accelerated court proceedings seeking "proportionate" measures to stop unauthorized broadcasting of sporting competitions or events. These measures have been interpreted to include network blocking.

In June 2024, a French court ordered three global DNS providers (Google, Cloudflare, and Cisco) to return incorrect information in their DNS resolvers for a number of websites under the law in order to prevent users of the alternative DNS from accessing the content.[17] The court ordered the blocking despite the entry of evidence in the case that the impact on piracy would be minimal, that it might require the sites to be blocked globally, and that it would require companies to build new technology on top of the global DNS systems that make up the Internet in order to comply. The court provided no opportunity for a stay of the order pending appeal as to whether the blocking was proportionate and consistent with EU human rights requirements,

---

[13] Id.

[14] https://www.reuters.com/world/asia-pacific/bangladeshs-internet-shutdown-isolates-citizens-disrupts-business-2024-07-26/

[15] https://restofworld.org/2024/bangladesh-internet-blackout-tech-industry/

[16] https://www.thedailystar.net/business/economy/news/internet-outage-curfew-leave-foreign-investors-bind-3663536

[17] https://circleid.com/posts/20240618-french-court-orders-google-cloudflare-cisco-to-poison-dns-in-anti-piracy-crackdown

creating a risk that companies simply operating part of the global Internet would face penalties for not complying with French requirements. As a result of that decision, one of the three companies opted to stop providing their global DNS service within France.

C. India

For the last six years, India has been a leading nation in ordering Internet shutdowns. The digital rights group Access Now reported that India had 116 localized Internet disruptions in 2023, with the longest shutdown lasting 212 days.[18]

Indian state governments have permanently blocked access to tens of thousands of websites and applications (nearly 55,000 between 2015-2022[19]), providing little to no transparency about the blocks.[20] Indian courts have also routinely ordered blocking of business websites that they view as failing to comply with Indian orders. In 2023, Indian courts ordered the blocking of websites for five major global Internet registrars based on their alleged failure to comply with Indian court orders to take down domain names globally. This type of blocking was particularly problematic as it resulted in the registrars' customers, the domain name holders themselves, being unable to control certain technical aspects of their sites.[21]

In 2022, India put in a requirement for VPN providers to have physical servers within India and to collect details on their customers. This action resulted in several high-profile global VPN providers leaving the country.[22]

The economic consequences of India's Internet blocks and shutdowns are staggering – for example, estimates put total losses to India's economy for the first half of 2023 alone at USD 1.6 billion, FDI losses of around USD 118 million, and job losses totalling approximately 21,000[23]. Prolonged Internet shutdowns have devastated local economies In India by making it impossible for local workers to perform tasks that require an Internet connection.

Global VPN, Internet infrastructure, and cloud businesses have struggled to stay in the Indian market given the barriers caused by blocking and regulatory requirements, as well as the high operational and compliance burdens from the complex regulatory landscape.[24]

---

[18] https://www.accessnow.org/press-release/india-keepiton-internet-shutdowns-2023-en/

[19] https://sflc.in/recent-content-blocking-in-india/

[20] https://cis-india.org/internet-governance/how-india-censors-the-web-websci

[21] https://www.medianama.com/2023/03/223-namecheap-domain-registrars-blocked-india-3/

[22] https://www.wired.com/story/vpn-firms-flee-india-data-collection-law/

[23] https://economictimes.indiatimes.com/tech/technology/internet-shutdowns-cost-1-9-billion-to-india-in-jan-jun-2023-report/articleshow/101368283

[24] https://techcrunch.com/2024/01/03/india-tech-regulation/

D. Iran

The Iranian government has increasingly been limiting its citizens' access to the Internet. The idea of an “Iranian Internet” was first proposed in 2005 — one that was consistent with the policies and principles of the Iranian government as opposed to how the Internet operated overseas. This was followed by a requirement a few years later that ISPs would need approval from the government to operate and were required to filter content in order to continue to gain that approval.

In 2013, Iran began work on a National Infrastructure Network (NIN), with the aim of recreating within Iran all the essential Internet services like search and messaging that had traditionally been provided by organizations outside of Iran. It was coupled with policies that subsidized and encouraged the use of these local services; which, as they were hosted domestically, made monitoring and filtering much more feasible.[25] This policy received huge pushback from citizens, with an increased use of VPNs to access websites that were not readily available.

Iran’s authoritarian regime’s approach to limiting Internet access amounts to an extreme version of blocking, relying on infrastructure to recreate core services locally. Despite their efforts, however, traffic from the major Iranian networks to network providers like Cloudflare has picked up substantially, demonstrating the inherent value of a free and open Internet without country-specific borders.

E. Italy

In February 2024, Italy implemented its Piracy Shield, a new system that was designed to combat online piracy in Italy. The system was originally implemented to protect the large sports rights holders, with the aim of blocking unauthorized viewing of live coverage of events like Serie A football, the UEFA Champions League, and the Italian Cup basketball matches.[26] The Piracy Shield mandates that a variety of providers comply with blocking orders issued by the rights holders without judicial review and within 30 minutes of reporting, with no mechanism for recourse.[27] The failure to include controls on blocking has resulted in numerous instances of blocking of large cloud providers that service significant numbers of websites, thereby causing users to lose access to large numbers of global websites with no connection to piracy.[28]

---

[25] https://blog.cloudflare.com/two-months-later-internet-use-in-iran-during-the-mahsa-amini-protests/

[26] https://advanced-television.com/2024/02/19/italy-piracy-shield-live-but-needs-retweaking/

[27] https://project-disco.org/european-union/italys-piracy-shield-lessons-learned-and-mistakes-to-avoid/

[28] https://torrentfreak.com/piracy-shield-cloudflare-disaster-blocks-countless-sites-fires-up-opposition-240226/

Rather than address the significant concerns with overblocking of innocent websites and lack of redress mechanisms in the Piracy Shield, Italy has expanded the program. Italy's Senate Budget and Finance Committees approved amended legal proposals that require VPN and DNS services located anywhere in the world to block pirated content flagged by rights holders.[29] These sweeping, broadened requirements, now in effect, could indiscriminately disrupt global services and access to the Internet without adequate oversight and are inconsistent with international norms.

Piracy Shield-mandated blocking has adversely impacted both U.S. network providers and U.S. businesses whose websites were inappropriately blocked as a result of Italy's inadequate safeguards. The system has led not only to frustrations amongst users and cloud providers, but has also led some VPN providers to stop operating in Italy due to the burdensome requirements of the Piracy Shield.

F. Malaysia

In early September 2024, the Malaysian Communications and Multimedia Commission (MCMC) directed Malaysian ISPs to redirect all DNS traffic to local DNS servers in order to prevent access to certain online content. This approach would have effectively made it impossible for Malaysian Internet users to use any non-Malaysian DNS resolver services as a means of preventing access to certain content. While ISPs received instructions from the regulator, there was no public statement or landing page to inform users of this unilateral decision to redirect traffic away from third-party global DNS providers. After the directive was met with massive backlash and accusations of government overreach from politicians, cybersecurity practitioners, and individuals, it was suspended[30] pending stakeholder consultations. It is unclear if the policy has been halted completely or will re-emerge.

Malaysia's goal is for the digital economy to contribute at least 25.5% to its GDP by 2025[31]. This is currently on track, with Malaysia set to receive U.S. technology investments worth USD 14.7 billion[32] in 2024. Amazon Web Services, Google, Microsoft, Oracle, Abbott Laboratories, and Boeing are among the U.S. companies that have committed investments. However, recent unilateral policy decisions such as the proposed DNS redirection signal growing censorship and protectionism, ultimately creating challenges for U.S. companies. This decision is also at odds with the Malaysia Digital Bill of Guarantees - a set of fiscal and non-fiscal incentives, rights, and privileges granted to digital investors by the Government of Malaysia[33]. Bill of Guarantee No. 7 states that the government will ensure no censorship of the Internet.

---

[29] https://torrentfreak.com/italy-approves-piracy-shield-vpn-dns-proposal-risk-of-prison-for-isps-intact-241001/

[30] MCMC asked not to proceed with DNS redirection method

[31] https://www.bernama.com/en/news.php/news.php?id=2349783

[32] https://www.bernama.com/en/news.php?id=2350323

[33] https://ccs-co.com/wp-content/uploads/137.2-Malaysia-Digital-Bill-of-Guarantees-%E2%80%98MD-BoGs.pdf

G. Myanmar

Since the 2021 coup, the Myanmar military junta has implemented various types of Internet blocks and shutdowns. The regime imposed Internet blackouts – first nationwide, followed by more targeted shutdowns aimed at resistance strongholds. It also blocked access to news outlets and social media platforms, including Facebook. Although people in Myanmar initially turned to global VPNs as a way to circumvent the censorship, the junta blocked VPNs and banned their use starting in May 2024. The police conduct random checks of citizens' phones, and those found to have Facebook or VPN apps are arrested under anti-terrorism laws.[34]

While this crackdown is mainly aimed at stifling dissent, it has impacted Myanmar's local economy, as the vast majority of Myanmar's small businesses operate through Facebook. Since the military regime's bans, traders have stopped online sales due to fear of repercussions. In addition, although many users circumvent the blocks using non-blocked VPNs, this is at great risk of harm, including arrest and cyber threats (phishing and malware from malicious free VPNs being advertised by bad actors).[35]

With current blocks and bans in place, the disruption to global business in Myanmar has been significant. Analysts expect international businesses operating in Myanmar to be pressured to comply with the junta's directives regarding website blocking and Internet shutdowns, with resistance to these directives leading to operational difficulties and legal scrutiny for global businesses.

H. Pakistan

Internet censorship and shutdowns are frequent in Pakistan, especially during politically sensitive periods. In 2023, Internet shutdowns cost Pakistan over USD 237.6 million, affecting 83 million people and lasting 259 hours.[36] This year, on February 8, the day of Pakistan's general elections, the government shut down mobile and Internet services, citing national security concerns.[37] Recently, the Pakistani government has also been implementing a persistent and disruptive Internet slowdown. While initially attributed to submarine cable repairs, digital rights groups speculate that the slowdowns are part of a deliberate government strategy to control information through the implementation of a nationwide firewall.[38]

---

[34] https://www.accessnow.org/myanmar-vpn-ban/

[35] https://fulcrum.sg/myanmar-juntas-internet-controls-expose-citizens-to-more-cyber-threats/

[36] https://www.thenews.com.pk/print/1224269-internet-shutdown-caused-rs65bn-loss-to-pakistan-in-2023

[37] https://tribune.com.pk/story/2494322/govt-refuses-to-disclose-reasons-for-election-day-mobile-internet-shutdown

[38] https://www.globalissues.org/news/2024/10/09/37914

One of the most severely impacted groups is Pakistan's growing global freelance workforce, which relies on the Internet for their livelihoods. Pakistan is ranked among the top five countries for freelancers globally, with many utilizing U.S-based gig economy platforms.[39] Pakistan's freelancers, however, have suffered lowered ratings on U.S. platforms due to being offline for long periods of time during the Internet shutdowns and slowdowns. Freelancers who use VPN services to circumvent the slowdown have had their accounts disabled upon detection of location inconsistencies.

While Internet slowdowns and shutdowns have a direct impact on Pakistan's local economy, it also has significantly affected global business interests in Pakistan, with many multinational corporations reportedly having left Pakistan as a direct result of continued poor Internet availability[40]. Many technology sectors in Pakistan – such as payments, social media, and 'daily use apps' – are dominated by global providers, which have lost viability due to the shutdowns and drops in Internet latency. Pakistani businesses that rely on fast and reliable Internet connectivity services from global providers, such as call centers and e-commerce companies, confront a chaotic situation stemming from Pakistan's Internet shutdowns and slowdowns[41].

I. Russia

Over the last five years, the Russian government has taken steps to tighten its control of a sovereign Internet within Russia's borders, including laws requiring Russian ISPs to install equipment allowing the government to monitor and block any Internet activity and implementing periodic Internet shutdowns. Russia is also seeking to develop its own national DNS service, making it easier for the government to disconnect Russia from the global Internet and redirect Internet inquiries to alternate websites.[42]

Authorities in Russia have also implemented a series of blocking actions against services, websites, and operators that they find objectionable. Russian authorities have targeted popular social media sites like YouTube, Facebook, Instagram, and Twitter, as well as Russian language outlets based outside the country.[43] Many mainstream social media and news websites (BBC, LinkedIn) are also currently blocked, and there is a strong push to move away from Western tech giants and towards Russian alternatives such as Yandex.[44] Authorities have also used a

[39] https://www.washingtonpost.com/world/2024/10/11/pakistan-internet-slowdown/

[40] https://www.arabnews.com/node/2567759/pakistan

[41] https://restofworld.org/2024/pakistan-internet-firewall/

[42] https://worldcrunch.com/focus/russia-blocking-internet

[43] https://cepa.org/article/russias-window-on-the-world-is-now-closing/;

https://www.theguardian.com/world/2022/mar/21/russia-bans-facebook-and-instagram-under-extremism-law

[44]https://pulse.internetsociety.org/blog/how-isolated-is-the-russian-internet-consequences-of-the-war-in-ukraine

range of techniques, including network blocking, to restrict access to VPNs and other tools that can be used to access the global Internet.

The extreme example of Russia demonstrates the significant importance of maintaining access to a secure Internet to citizens when authoritarian regimes attempt to assert information control. Beyond highlighting the negative impact on global trade and the fact that US companies are unable to operate in Russia, it emphasizes the need for a free and open Internet.

J. South Korea

In December 2023, the South Korean national legislature revised its Network Act to include requirements for CDN providers to block access to illegal content within South Korea[45]. This costly, world-first requirement will create a significant barrier to delivering global CDN services within the South Korean market.

South Korea's government already directs a robust blocking regime that is implemented by Korea's largest ISPs. There is a wide range of content deemed illegal in South Korea, with Korean authorities reportedly approving over 100,000 blocks each year[46]. However, despite having this established blocking regime, starting in July 2024, global CDN providers are also expected to block the same instances of illegal content.

Notably, as CDN providers do not host websites, and as such, they cannot remove websites or their content from the Internet, other countries' laws in this area have similarly recognized that hosting providers have the primary responsibility to address unlawful content and that requirements to remove such content should therefore focus on hosting providers.

Thus, South Korea's world-first requirement for CDN providers to block illegal content will result in multiple technology providers across the Internet ecosystem – from ISPs, hosts, to CDNs – blocking access to the same instances of content, resulting in an unprecedented, redundant, and extremely costly operational and technological compliance regime for U.S. CDN providers, creating a significant barrier for global CDN service delivery in the South Korea market.

VII. Conclusion

In conclusion, the i2Coalition remains deeply concerned about foreign government-imposed shutdown and network blocking as a method of content restriction, particularly when applied to global Internet infrastructure services like VPNs or global DNS resolvers or when applied in ways that are likely to impact many unrelated websites or services. The patchwork of existing blocking regimes across different jurisdictions is also concerning, as U.S. companies have to

---

[45] https://www.fnnews.com/news/202303221823424151

[46] https://freedomhouse.org/country/south-korea/freedom-net/2023

contend with a range of restrictive blocking orders, often under threat of significant penalties and with no recourse. Such measures pose significant risks to the open and interoperable nature of the Internet and disproportionately impact neutral third-party Internet infrastructure providers, whose role is essential in maintaining the functionality and security of global digital networks. Network-level blocking is not only imperfect, but also comes at a high cost to service providers, who have to bear the operational and technical costs in order to comply. We urge USTR to recognize the harm these restrictions can cause, not only to the global flow of information but also to trade and innovation. The i2Coalition strongly believes that enforcement efforts should focus on specific bad actors rather than sweeping in essential Internet infrastructure providers, whose neutral operations are vital to the global digital ecosystem.

To counter these challenges, USTR should work with other nations to facilitate adherence to international norms that prioritize an open and secure Internet. This collaboration can help reduce the impact of site-blocking regimes, support cross-border digital trade, and prevent the balkanization of the global Internet. By advocating for international standards that mandate proportionality and require due process, USTR can protect the economic and social benefits of an interconnected world. USTR can help preserve the integrity of the global digital economy and ensure that U.S. companies continue to benefit from the opportunities offered by an open Internet. Fostering alignment with international norms in this area will help ensure a more inclusive and dynamic global marketplace.

We look forward to continuing our engagement with USTR to ensure that future policies support a free and open Internet while maintaining balanced and effective measures to protect intellectual property and digital services.

Respectfully submitted,

Christian Dawson
Executive Director
Internet Infrastructure Coalition
2920 W. Broad Street, Suite 80
Richmond, VA 23220
dawson@i2coalition.com

October 17, 2024