October 30, 2025

Edward Marcus, Chair
Trade Policy Staff Committee
Office of the United States Trade Representative
600 17th Street NW
Washington, D.C. 20508

**RE: Request for Comments on Significant Foreign Trade Barriers for the 2026 National Trade Estimate Report**

Docket Number USTR-2025-0016

Dear Mr. Marcus,

Cloudflare appreciates the opportunity to submit comments to the Office of the United States Trade Representative (USTR) on its Significant Trade Barriers for the 2026 National Trade Estimate Report. Our comments focus on significant digital trade barriers that contradict global norms, disproportionately impact U.S. technology providers, and hinder market access in some of the countries where we operate.

## I. Background on Cloudflare

Cloudflare, Inc. is the leading connectivity cloud company that runs one of the world's largest most interconnected networks providing security, performance, and reliability services to millions of Internet properties, such as websites, networks, and other applications online. Cloudflare powers Internet requests for 36% of the Fortune 500 and serves over 84 million HTTP requests per second on average. Cloudflare interconnects with approximately 13,000 networks globally, including major Internet Service Providers (ISPs), cloud services, and enterprises from all over the world.

Cloudflare's expansive, interconnected, highly distributed network – with points of presence spanning more than 330 cities in over 125 countries – underpins modern international commerce. By providing essential security services like protection from Distributed Denial of Service (DDoS) and other types of cyber attacks, Cloudflare ensures that over 20 percent of the web sitting behind its network can operate reliably and securely across borders. The broad availability of Cloudflare's services helps mitigate the risk posed by malicious cyber activities, improves the reliability and performance of the Internet for everyone online, and provides

developers with a reliable platform to build and deploy innovative solutions globally through its edge network.

Most recently, Cloudflare's network has been expanded to include GPUs, allowing developers to run generative AI inference and agentic AI tasks globally. This has positioned us as a key infrastructure provider in a growing global AI market supporting scalable, cross border AI deployment. Our customer's traffic is processed at the data center closest to the user, with no backhauling or performance tradeoffs, and the delivery of this traffic can be localized according to our customers' preferences. This means our edge-computing power brings latency-sensitive AI and cloud workloads closer to end-users in markets worldwide.

The scope of Cloudflare's network and user base give us a global view on regulatory efforts that hinder market access and trade for digital services.

## II. European Union

At the European level, the European Commission is due to propose several pieces of legislation which could have negative effects on U.S. technology providers. In particular, the upcoming EU Digital Networks Act (DNA) proposal, due to be presented in December 2025, could have significant adverse impacts on U.S. cloud services companies, including those, like Cloudflare, offering content delivery network (CDN) services.

### A. Digital Networks Act

This DNA is a proposed reform of European telecommunications legislation. The European Commission has considered expanding the scope of regulation to include innovative services such as cloud and CDNs. The potential inclusion of such services in the scope of the DNA would put inappropriate and unnecessary additional regulatory burdens on a variety of U.S. companies for services which 1) are already in scope of other relevant pieces of EU legislation and 2) are services which are clearly distinct from last-mile connectivity services provided by ISPs and thus should not be regulated in the same way. Indeed, the expansion of the regulation has been primarily encouraged by large European telecommunication providers looking to make it more challenging for U.S. companies to compete in the European market. Putting additional regulatory burdens on services such as CDNs and cloud infrastructure which are important technologies for European businesses to scale and grow, would have a detrimental effect and would put European telecommunication providers at a competitive advantage in the market versus U.S. providers of CDN and cloud services.

Including cloud infrastructure and CDNs in scope of the DNA could also include applying an arbitration mechanism for interconnection disputes to those types of infrastructure. This would lead to a "hidden network fee" initiated by large telecommunication providers, as the arbitration by national regulators would inevitably lead to forced paid peering arrangements while over 99% of interconnection agreements currently are settlement free. This would disproportionately affect U.S. providers, such as CDNs, cloud service providers, and content and social media platforms,

and would be inconsistent with the EU-US agreement reached last summer which stipulated the EU would not maintain or introduce network usage fees.[1]

### B. European preference in public procurement.

Considerations around creating a "European preference" in public procurement processes, as well as efforts to establish strict digital sovereignty requirements for technology services such as cloud, AI and digital infrastructure will likely lead to fewer opportunities for U.S. headquartered companies to compete fairly in the EU market. The ongoing negotiations on the EU cloud cybersecurity certification scheme (EUCS) are a clear example of the willingness by some governments in the EU to include far reaching sovereignty requirements in regulation, which many non-EU businesses would not be able to meet. These requirements for EU headquarters, EU-only infrastructure, and access controls limited to EU citizens will effectively limit the ability of U.S. SMEs to access the European single market, creating a significant structural and potentially long-term trade barrier.

## III. Spain

Spanish regulators and courts have enabled processes that disrupt the provision of digital services to further the commercial interests of local entities. Specifically, Spanish courts and legislators[2] have declined to put in limitations or reasonable restrictions on copyright holders that abuse the Spanish legal system by seeking overbroad court orders that enable them to block the services of U.S. network service providers like Cloudflare by blocking IP addresses, each of which serves traffic for thousands of domains.[3] This practice results in the widespread and repeated disruption of tens of thousands of unrelated, legitimate websites, as well as the disruption of digital services, with no judicial opportunity for remedy. These actions, designed to protect a narrow set of commercial interests, have caused significant collateral harm to businesses and users who are not the intended targets, without recourse or the possibility for affected parties to challenge the underlying order.

While acknowledging that such restrictive measures fail to meet internationally recognized principles of proportionality, necessity, and adequacy, the Spanish Government has explicitly

---

[1] See Joint Statement on a United States-European Union framework on an agreement on reciprocal, fair and balanced trade, Eur. Comm'n, Directorate-General for Trade & Economic Security, Aug. 21, 2025, https://policy.trade.ec.europa.eu/news/joint-statement-united-states-european-union-framework-agreement-reciprocal-fair-and-balanced-trade-2025-08-21_en

[2] See Andy Maxwell, Proposal to Prevent LaLiga Site-Blocking Hurting Innocent Sites Rejected in Spain, TorrentFreak, Oct. 25, 2025 at https://torrentfreak.com/proposal-to-prevent-laliga-site-blocking-hurting-innocent-sites-rejected-in-spain-251025/.

[3] See Chiara Castro, Cloudflare wants to fix Spain's blocking of illegal football streams ahead of next LaLiga season, techradar, June 20, 2025, https://www.techradar.com/vpn/vpn-privacy-security/cloudflare-wants-to-fix-spains-blocking-of-illegal-football-streams-ahead-of-next-laliga-season; Kristina Jaruseviciute, Cloudflare Blocks in Spain Disrupt Internet Access Amid LaLiga Anti-Piracy Measures, Techlapse, Oct. 24, 2025, https://techlapse.com/news/cloudflare-blocks-disrupt-internet-in-spain/.

chosen not to intervene in the issue. This has resulted in actions that disproportionately affect U.S. digital service providers by restricting their ability to operate freely in the Spanish market. The loss of market access, service reliability, and consumer confidence has created a significant barrier to digital trade and raises future concerns about the predictability and transparency of Spain's regulatory environment for U.S. companies.

## IV. France

France's current regulatory framework for content protection, relying on network blocking, constitutes a significant non-tariff trade barrier that has been explicitly used to unfairly impact U.S. global digital service providers. This framework includes Article L.333-10 of the French Sports Code, under which courts have issued orders against public Domain Name System (DNS) resolvers to block domains that infringe the broadcasting rights of sports leagues and event organizers. Although France has attempted to compel DNS and Virtual Private Network (VPN) providers to implement blocks through these court decisions, most of these non-hyperscaler global providers do not have the technical capability to comply with these France specific requirements. Indeed, several providers, including U.S. based providers, have ceased offering services in France rather than comply with the requirement.

Furthermore, the most recent legislative proposals, which aim to modify Article L.333-10, would introduce an automated system to enforce compliance from all network service providers. These blocking orders are often directed at foreign intermediaries not based in or regulated by France, who typically lack the technical means for geographically limited blocking. Furthermore, these burdensome obligations are being imposed without any requirement for rightsholders to prove that these targeted global services are actually being used to access infringing content, making the measures disproportionate and unjustified. This proposed mechanism represents a shift in France's approach to content blocking, moving away from a judicially led and supervised process towards an automated system modeled on Italy's "Piracy Shield" (detailed further below).

The introduction of such a system creates significant uncertainty for foreign online platforms, intermediaries, and service providers. It increases the risk of overblocking legitimate content or mistakenly targeting websites that operate lawfully, potentially disrupting cross-border digital services. Moreover, the lack of clear procedural safeguards and transparency could discourage U.S businesses from investing or offering services in France, fearing arbitrary enforcement or inconsistent application of the rules. Such regulatory unpredictability could therefore undermine confidence in France's digital market, complicate trade relations and restrict the free flow of digital goods and services.

## V. Italy

The Italian government and telecommunications and media regulator AGCOM has recently undertaken a series of regulatory measures that are increasingly threatening a number of U.S. businesses, primarily aimed at CDN, DNS and VPN providers. These measures pose significant digital trade barriers that increasingly affect U.S. businesses in Italy.

### A. Regulatory Threats to Content Delivery Networks

The Italian government and its regulator, AGCOM, are pursuing measures that would require registration and new regulatory requirements for CDNs under telecommunication laws, posing major digital trade barriers. AGCOM is seeking to bring all CDNs operating in or offering services in Italy under the general authorization regime of the Italian Electronic Communications Code. This creates a redundant regulatory burden on services that are already governed by existing EU legislation and would lead to increased compliance costs and fewer incentives for U.S. providers to invest in local infrastructure. This approach is also expected to lead to a mandate for CDN providers and Content and Application Providers (CAPs) to pay "network usage fees" to local telecommunication providers for peering arrangements, a requirement that would be inconsistent with the EU-US trade agreement reached last summer, as described above.[4] Such duplicative requirements would unfairly and disproportionately target U.S. companies, as the majority of affected global CDN providers and content providers are American. Any such action by the Italian Ministry could also trigger similar actions at the EU level, setting a harmful precedent for the upcoming EU Digital Networks Act.

### B. Network Blocking Practices ("Piracy Shield")

Italy's "Piracy Shield" system, implemented in February 2024, mandates a rapid automated anti-piracy regime that has unduly impacted a number of U.S. digital services. The system mandates that certain network providers comply with blocking notices within 30 minutes without judicial review or oversight, nor any mechanism for recourse. The failure to include adequate safeguards against collateral damage has led to the inappropriate blocking of shared services of large cloud providers, which are disproportionately American businesses. For instance, the blocking of a Cloudflare IP address resulted in tens of thousands of non-targeted websites being blocked in February 2024. Furthermore, the blocking of the domain "drive.usercontent.google.com" in October denied Italian users access to Google Drive for over 12 hours.

The attempt to expand these blocking requirements to additional service providers like VPN and DNS resolvers, regardless of whether they have a significant presence in Italy, has further threatened market access for digital services in Italy. This system's lack of transparency and legal accountability has led certain VPN providers to cease operations in Italy and risks widespread service disruptions that hinder market access for U.S. providers.

[4] See Joint Statement on a United States-European Union framework on an agreement on reciprocal, fair and balanced trade, Eur. Comm'n, Directorate-General for Trade & Economic Security, Aug. 21, 2025, https://policy.trade.ec.europa.eu/news/joint-statement-united-states-european-union-framework-agreement-reciprocal-fair-and-balanced-trade-2025-08-21_en.

### C. Abuse of the Judicial System

Italy permits domestic rightsholders to abuse its court system to threaten and disrupt U.S. businesses, fundamentally lacking meaningful due process protections. Over the past several years, U.S. service providers have been targeted based on assertions of responsibility for allegedly infringing content. Copyright holders can use emergency ex parte proceedings to obtain orders to block or remove content without first giving companies any opportunity to oppose the order. Once orders are obtained, rightsholders can assert noncompliance with those orders and initiate actions to collect penalties without any prior judicial determination of noncompliance and without the target of these actions having any ability to stay the order pending judicial review. This coercive, penalty-based approach to removal of content, without adequate judicial review or due process protections, is a significant barrier to doing business in Italy.

## VI. Japan

Japan currently imposes two major digital trade barriers that create unfair obstacles to market access and disproportionately affect U.S. technology providers: burdensome registration requirements and the erosion of liability protection for CDNs.

### A. Costly and Burdensome Registration Requirements

Japan has imposed redundant registration requirements under various legal regimes as a means of supervision and control over foreign companies, creating excessive and unnecessary compliance burdens. Under the Telecommunication Business Act, foreign providers like Cloudflare are required to register their services and appoint a local representative if they conduct “continuous transactions.” Furthermore, the Japanese government pressured U.S. technology companies to register their U.S. corporate entity in Japan to facilitate domestic legal proceedings. Compounding this, Japan’s Provider Limitation Liability Act allows individuals to bring lawsuits over allegedly defamatory or infringing content, imposing onerous procedural obligations and penalties. Since registering its corporate headquarters in 2022, Cloudflare has received more civil actions in Japan than the total number of civil actions faced in all other non-U.S. countries combined.

### B. Erosion of Intermediary Liability Protection

Japan’s actions, driven by influential publishing organizations and years of government and industry alignment, have established a significant digital trade barrier for U.S. intermediary services like CDNs, such as Cloudflare, by attempting to impose unprecedented financial liability for third-party copyright infringement. These measures have directly challenged global norms and impact market access for American businesses.

One particular dispute reflects years of effort by Japan’s government and its publishing industry to impose additional obligations on intermediaries like CDNs. A fully adjudicated ruling that finds

CDNs liable for monetary damages for infringing material would set a dangerous global precedent and necessitate U.S. CDN providers to limit the provision of global services to avoid liability, severely restricting market growth and expansion into Asian Pacific markets.

## VII. South Korea

South Korea's digital policies present two major, converging trade barriers that pose significant challenges for U.S. technology companies and create unfair obstacles to market access: new CDN blocking mandates and the established “Sender Pays” network peering regime. Both issues impose disproportionate compliance burdens and excessive costs on U.S. providers, hindering their ability to operate efficiently within the South Korean market.

### A. Redundant Content Delivery Network Blocking

In 2023, the South Korean government made revisions to the Network Act to impose world-first legislative mandates to require CDNs to restrict access to illegal content. This has led to the creation of a duplicative and administratively inefficient blocking regime that places a significant operational burden on U.S. providers. The South Korea Communication Commission (KCC) sends U.S. CDN providers a “block list” of over 1.5 million URLs (with 30,000 new additions monthly) that CDN providers must filter to identify and restrict domains being served through their networks. South Korea imposed this new regulatory requirement primarily on U.S. providers despite the requirement that local ISPs block the same content. This is inconsistent with international practice and places an unprecedented compliance burden on global CDN providers, forcing them to restructure abuse systems and processes to manage significant amounts of abuse reporting for content that is often not even on their network.

### B. “Sender Pays” Network Peering Regime

South Korea is one of a handful of markets where “paid peering” is the norm due to regulatory intervention, acting as a significant trade barrier. The 2016 “Sending Party Network Pays” (SPNP) requirement mandated interconnection fees between the three main South Korean ISPs, which effectively led them to abandon the global norm of settlement-free peering as they no longer needed to compete to cooperate with U.S. Cloud Service Providers. As a result, Cloudflare experiences bandwidth costs in South Korea that are nearly 30 times the cost of Internet transit in the United States. The high fees demanded by large South Korean ISPs affect the ability of Cloudflare and U.S. content providers to serve traffic efficiently, and this network peering overregulation has resulted in major U.S. technology companies reducing or pulling out of the South Korean market.

## VIII. Conclusion

Cloudflare sincerely appreciates the opportunity to submit comments to USTR for the 2026 National Trade Estimate Report. Our submission demonstrates that the challenges faced by U.S. technology providers are not isolated incidents but represent significant, systemic trade

barriers across key global markets—from the judicial abuse and regulatory coercion in Italy and the anti-competitive liability threats in Japan, to the punitive network fees and redundant blocking mandates in South Korea and the digital sovereignty requirements emerging in the EU. Given Cloudflare's role as core Internet infrastructure, securing over 20% of the world's websites, the successful operation of our network is vital to U.S. economic and security interests. We urge the U.S. government to continue its resolute advocacy on behalf of American businesses to dismantle these structural barriers and ensure a global digital environment that rewards innovation and fair trade.

Sincerely,

/s/ Zaid A. Zaid

Zaid A. Zaid
Director, Head of U.S. Public Policy