

Jun 29, 2026

Dear Chairman Issa and Ranking Member Johnson,

The undersigned organizations write to reiterate our strong opposition to discussion drafts of site blocking legislation that has been shared with stakeholders over the past year—including H.R.791, the Foreign Anti-Digital Piracy Act. Despite some improvements over earlier proposals, the proposals are all fundamentally flawed. They misunderstand the technology, underestimate the danger faced by third parties caught up in overblocking, and are based on a PR campaign that papers over the gross failures of these systems in Europe.

1. **Site blocking in Europe has been chaotic, irregular, and caused widespread outages** due to overblocking. In Italy, site blocking has “disrupt[ed] [hundreds](#) of legitimate, non-streaming websites ... [while bad actors have] evaded enforcement by migrating to new infrastructure and unfiltered IP address space.” In Spain, overblocking has caused outages to [payment processors](#) and a [national healthcare provider](#), as well as giving rise to multiple [grassroots movements](#) against site-blocking. The idea that site blocking is a “solved problem,” politically or technologically, is a myth.
2. **Small businesses and nonprofits face the greatest risks, and have the fewest protections.** In Italy, overblocking has [brought down](#) digital infrastructure for hotels, car mechanics, retail shops, telehealth programs, and even a nunnery. The ones bearing the cost of overblocking are the ones least poised to bear it---and the ones who have no remedy for the days or weeks (or more) of lost business that results from an overzealous blocking order. America’s small businesses cannot afford to be treated as “acceptable collateral damage” for multibillion dollar entertainment and sports industries.
3. **Subjecting global DNS services to blocking orders is ineffective and costly.** Over 90% of DNS resolution in the United States is handled by last-mile ISPs, who set themselves as the default resolver. For moderately technically savvy users, switching DNS resolvers is a trivially easy task that can be completed in under 5 minutes. Users who are technically sophisticated enough to utilize alt-DNS resolvers in the first place will not be stopped by a blocking order; they will simply switch to another resolver, use a Virtual Private Network (VPN), or simply type the banned IP address into their search bar and connect directly. Subjecting alt-DNS resolvers to this framework imposes massive costs, with zero return.
4. **Ex parte proceedings are fundamentally flawed.** The system envisioned in current proposals depends on issuing default judgments to absentee website operators. Given the First Amendment issues at play, this ex parte format is simply too dangerous. Safeguards such as an adequately funded public advocate or guardian ad litem could improve matters, but they would never have the full knowledge of the facts necessary to adequately represent the accused website, potential collaterally-harmed parties, or the public interest.

5. **This proposal puts user privacy at risk.** Site blocking is often ineffective, as it is easily circumvented using privacy-focused tools, such as virtual private networks (or VPNs). VPNs obscure a user's IP address from the websites to which they navigate and apps they use, and can be a useful tool for protecting users' privacy online. At the same time, less reputable VPNs may collect sensitive personal information about their users without their full knowledge and could contain malware. Site-blocking legislation could, therefore, not only be ineffective in meeting its own goals but also sacrifice users' privacy and safety in the process. Additionally, we have seen site blocking efforts in other nations, such as [France](#), "ratchet up" and ensnare VPN service, causing major privacy and security concerns.

In short, the harms generated by this "solution" vastly outweigh any purported public benefit. While much has changed in the world since the landmark protests that helped prevent the Stop Online Piracy Act and the PROTECT IP Act (SOPA/PIPA) from passing more than a decade ago, one thing has not: our broad and diverse coalition of stakeholder groups opposes site blocking. It has caused significant damage in Europe, and threatens to harm small businesses and censor free speech at home. We simply do not believe site-blocking legislation is needed or appropriate at this time.

Respectfully,

CCIA
Electronic Frontier Foundation
Fight for the Future
Internet Infrastructure Coalition (i2Coalition)
Public Knowledge
R Street Institute