



United States
**Internet
Preservation
Society**

Joshua Moon
Internet Preservation Society
PO Box 27009
Washington, DC 20038
<moon@usips.org>

May 21st, 2025

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Response to FTC-2025-0023-0001

I am a systems administrator and business owner who specializes in developing antifragile Internet infrastructure. I write on behalf of myself, my businesses, and the non-profit organization the United States Internet Preservation Society in response to FTC's request for public comment and to encourage the FTC to use its regulatory authority over vital Internet Service Providers and Internet Security Providers to:

- Regulate Internet Service Providers (ISPs) and Internet security services as common carriers,
- Require a legitimate reason for ISPs to disconnect services from the Internet,
- Require a reasonable timeline for ISPs to restore service in instances where it is disconnected, and
- Create an appeals and mediation process available to victims of censorship via the FTC.

Background

For the last 13 years I have been fighting against online censorship. My encounters with censorship start at platform specific bans (such as not being allowed to have an account on social media websites I have never used) down to the very core infrastructure of the

Internet (where I have been blacklisted by some of the most powerful Internet service companies holding thousands of miles of fiber optic infrastructure). The United States Internet Preservation Society is a 501(c)(4) founded to help at-risk Internet services find ways around online censorship and to petition the government for meaningful tools to fight against online censorship.

As it is now such a common occurrence, instead of detailing every instance of censorship I have suffered firsthand, I would like to draw your attention to what I believe are the most egregious and anti-competitive sources of censorship that the Federal Trade Commission has the power to deal with.

Internet Backbone Companies

Tier 1 ISPs are enormous companies that are traditionally defined as having connections to all other Tier 1 ISPs . Any two computers connected anywhere in the world will almost certainly need to utilize a Tier 1 ISP to communicate. If Tier 1 ISPs start to block connections to or from specific computers, that computer will find itself disconnected from significant swathes of the worldwide Internet.

I have experienced Tier 1 ISP censorship first hand. Until 2022, it was unheard of for these ISPs to censor specific companies, as their businesses enjoy very little public scrutiny and have traditionally understood their role as important and neutral services. This sensible practice ended when Cogent, a Tier 1 ISP based out of the District of Columbia, began censoring my businesses at an Internet backbone level. Cogent, under CEO Dave Schaeffer, has enjoyed significant income from the US Federal Government, both in contracts for providing Internet access to government agencies, and in grants for the deployment of new Internet infrastructure and can be regulated by the FTC.

Cogent has deliberately and maliciously interfered with my businesses by sabotaging its networking across the world and demanding its customers stop doing business with me. They would 'blackhole' connections to my network. Blackholing is a security practice in which networks pretend the destination network is unreachable, which would cause the connecting client to abort their connection attempt, even if there was a possible route.

This is more aggressive than simply refusing to connect. It is one thing for Cogent to refuse to communicate with another network. By blackholing connections, they lied about the availability of an address: a deliberate and malicious effort to disconnect my service from much of the Internet. This sort of censorship is generally reserved for national security, such as to stop the spread of a computer virus. It is the networking equivalent of Google Maps telling a customer hoping to drive to a store that the store does not exist, despite having actual knowledge of where it is and how to get there.

In an even more gravely concerning move, Cogent would electronically ‘announce’ the network infrastructure of other companies to remove routing for specific IP addresses, on which my services ran, as a means to censor us. I believe these actions were in violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), as they effectively seized and modified computer resources belonging to their own clients without authorization as a means to disable a US-legal website. This happened in the US, but also in Poland, showing that Cogent was dedicated to the world-wide blockade of my community. Also in Poland, Cogent pressured a very large data center owned by Equinix in Warsaw to evict my server, which they did.

Although these are their two most memorable instances of censorship, Cogent will—to this day—continuously block any instance of my website that they can, and I must painstakingly go out of my way to avoid them—an immensely difficult task due to their enormous size. Any time I look for a company to buy resources from, I must first determine if they have a relationship with Cogent, as I cannot do business with any company that does. I have never been a direct customer of Cogent. All of their censorship actions have been against me and my businesses have been through their own customers, or the customers of their customers, or so on.

DDoS Mitigation

The networking industry has known about DDoS attacks since the 1990s. It is a primitive but effective way to shut down Internet resources by using compromised computers to send enormous amounts of bad data to overwhelm their victims. DDoS attacks are frequently used for cyber-extortion, grow larger every year, and can cost

businesses thousands of dollars a day in lost revenue. Mitigating DDoS attacks is now a multi-billion dollar a year industry itself.¹

DDoS mitigation comes broadly in two flavors: application protection and network protection. Application protection is best for most websites and is where a security service directly handles web requests for the protected service. Network protection only deals with high-volume bandwidth saturation attacks, where protected machines are required to do much of their own application security.

I have experienced censorship from both kinds of service.

Cloudflare

Cloudflare is an Internet security company so ubiquitous that even the US Federal Government, all state governments, and many local governments use it to stay online and protect themselves from cyberattacks. In 2024, it was estimated that 20% of all global traffic passed through Cloudflare's networks. The reason for this is simple: websites not protected by Cloudflare do not stay up for long. There does not exist meaningful competition for Cloudflare; they are a *de facto* industry standard.

In August 2022, Cloudflare received significant outcry from gender ideology activists about providing security service to my website, the Kiwi Farms. In a response letter, CEO Matthew Prince explained in excruciating detail why they do not ban any website for any reason, how doing so is fundamentally incompatible with their mission as a security company, how doing so encourages despotic regimes to request censorship of political opponents, and so on.²

Four days later, over a three-day weekend, Matthew Prince blocked the Kiwi Farms. His explanation was that it had encouraged violence.³ It is unknown what he meant, as they never contacted me directly, and still have not. I never received any correspondence with Cloudflare or the police from any country or state. He lied, and I simply discovered my website was disconnected from the Internet and now vulnerable to DDoS attacks.

¹ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/>

² <https://blog.cloudflare.com/cloudflares-abuse-policies-and-approach/>

³ <https://blog.cloudflare.com/kiwifarms-blocked/>

We had no recourse, and the remarks he made to shift blame for his actions onto us damaged our reputation and hampered our ability to recover from his lies and actions.

Since then, we have had to create our own network resilient to DDoS attacks. It has cost tens of thousands of dollars and incurs thousands of dollars in recurrent additional expenses. Our medium-sized community only receives donations through cryptocurrencies, because payment processors like Stripe refuse to allow us to collect payments. The burden shifted onto us by Cloudflare refusing us service is incalculable when considering personal time lost trying to repair the damage, and when considering the loss of site activity from the weeks of downtime endured from not being able to stay on the public Internet as a result of the ensuing DDoS attacks.

Zayo

Zayo is an ISP that directly provides Internet access and also provides DDoS mitigation. Volumetric attack traffic is identified automatically and then disposed of before it reaches your network. This way, you pay for 1Gbps of clean traffic, and an attack of 100Gbps is mitigated before it touches your hardware. This is invaluable and cost-effective for large to enterprise sized companies that have their own sophisticated application security, but not near-infinite bandwidth to handle attack traffic.

Zayo charged us \$2,000 a month for this service, which is about ten times more than regular Internet bandwidth. However, to pay for the amount of bandwidth we'd need to stay online given the size of the attacks we deal with, we'd have to upfront tens of thousands of dollars more anyways.

Two days after receiving protection from Zayo, following the fallout from Cloudflare, Zayo Paris network engineer Blake Willis issued an internal communique suggesting that we should be terminated immediately. Mr. Willis was not involved in my business and did not live in the United States. The resulting disconnection, after months of working with Zayo to get set up and online with them, left my website completely offline for over a week as I scrambled to find ways to stay online. I was not given an opportunity to discuss this with anyone before we were terminated and I was not given notice until after it happened.

Analysis

Internet censorship is real. It is ongoing. It is severely affecting Americans. It is disproportionately impacting small businesses and private individuals. It is an escalating issue made worse every year.

Censorship happens at every level, from specific social media platforms everyday citizens rely on, to the silent workhorses that actually power the trillions of dollars of commercial activity happening in the American online space.

Smaller companies are more severely impacted by censorship. When activists start harassing service providers, they create a situation where freedom of speech is delegated strictly by the size of one's financial ability. Large companies can get away with anything they'd like, as they represent millions of dollars in annual cash flow for ISPs, whereas small companies are seen as simply not worth the effort to deal with if they are controversial in any way.

Regulating ISPs as common carriers gives them a good excuse to disregard pro-censorship harassment campaigns targeting them: they literally cannot censor online content like requested.

Smaller companies also lack the means to meaningfully communicate with the federal government or to initiate legal proceedings against service providers which have abused them. This is especially true for individuals, who have no recourse.

Especially frustrating is the facelessness of this censorship. Life altering decisions to disconnect communities from the Internet and creators from their audiences are made by anonymous platform janitors thousands of miles away in different states and countries. The appeals process is inhuman forms with automated replies. Social media, despite their immense size and impact on daily life, almost never have a telephone number. Americans are being treated like cattle by these platforms and companies. People are sick of being told what they can and cannot do by machines and nameless busybodies citing justification from terms of service that are vague, confusing, and applied with uneven hands showing extreme favoritism and nepotism.

Recommendations

The FTC has the capacity to enact meaningful regulation to support small, speech-oriented American companies and the American people.

1. The FTC should regulate large ISPs and security providers as common carriers. Sufficiently large Internet service providers and security providers should not be permitted to choose their customers. This alone will create a more even playing field where small, pro-free speech websites can compete with larger platforms.
2. The FTC should not do business with ISPs or security providers which do not enact new policies against censorship, including an internal appeals process. This would be particularly relevant to Cloudflare and Cogent.
3. The FTC should open a complaint hotline for companies and individuals to report online censorship so as to collect and analyze trends of online censorship and its impact on Americans. As indicated by the number of responses to this request for comment, there is an urgent need for the Government to accept communication about censorship. This hotline would (a) inform decisions on which service providers the FTC chooses to do business with, (b) allow the FTC to mediate disputes out of court, and (c) provide a basis for the FTC to make recommendations to the Congress for new legislation.

Inter-Agency Recommendations

4. All government agencies should follow FTC guidance developed through Recommendation #2 and require ISPs and security companies they contract with to be content neutral and provide meaningful internal appeals.
5. The Department of Commerce's National Telecommunications and Information Administration (NTIA) is responsible for managing the top-level domain .US, which is contracted out to GoDaddy for management. The NTIA should require .US domains never be censored in any way without a court order, regardless of content, so that Americans can always enjoy protected speech on the top-level domain owned by the Federal Government.
6. The Treasury's Office of the Comptroller of the Currency (OCC) should unpause OCC-2020-0042, the Fair Access to Financial Services rule.

This letter is the culmination of over a decade's worth of experience dealing first hand with the decline of American freedoms online. I hope that the FTC and other agencies will act quickly to ensure equal opportunity access to the Internet and all necessary security systems required to stay online.

Sincerely,

Joshua Moon

President and Treasurer

United States Internet Preservation Society

<moon@usips.org>

A handwritten signature in black ink that reads "Joshua Moon". The script is cursive and fluid, with the first letters of "Joshua" and "Moon" being capitalized and prominent.