Where the Sidewalk Ends: The Death of the Internet

Joshua Moon

8 Jul 2021

Contents

The Internet is becoming smaller, fragmenting down national borders, and succumbing to regulations imposed by governments and various special interests.

An internet is a network made of smaller networks. *The Internet* is the single international network you are using right now. The Internet is enormous. The Internet spans from research facilities in Antarctica up into outer space. The Internet is how I'm writing this in Europe for a website in the United States which is accessible almost everywhere in the world.

The Internet is also very fragile. It has many moving parts and drives the politics of our world today. For this reason, it will die, and it will die very soon. Our big-I Internet is being broken apart and will soon become many little-i internets. Every large country or trade union will have its own local and strictly regulated internet. Connections between internets will occur on the vestigial remains of the big-I Internet, requiring a special business permits to access.

China and the DPRK already work like this. If you want to communicate through the Great Firewall, you must have a registered business and specific need to do so. Russia has recently tested isolating itself from the Internet. The European Union continues to pursue aggressive censorship measures like TERREG, which would allow any member state of the EU to demand a web service hosted in any other EU member remove content within one hour, or be fined up to 4% of their global turnover in the last business year. The Internet cannot survive this sort of meddling for long.

While more centralized governments have the authority to shape their internet as they see fit, our politicians in the west have cumbersome obstacles to overcome, such as constitutional protections and a judicial process. Until these can be discarded, the government can simply bypass the courts and have companies to do the job for them. Companies are not restricted by the constitution in the same way as government, so as megacorp and government interests continue to mesh into one giant malaise, one can act for the other without causing problems. Even if the US Government cannot legislate a vague concept like 'hate speech', nothing stops the large social media companies from doing it for them.

"Build your own Internet"

To demonstrate how delicate the Internet is, I will enumerate the moving parts required to get content to your screen. Keep in mind that if any of these parts break, you're off the Internet until you can replace it. A website can function only with the assent of, and collaboration with, dozens of other companies. Each of these can be a different company with a different ethos.

First, you need a server. Most people trying to get a website up cannot afford one, so they rent a 'virtual private server' (VPS) from a company like DigitalOcean or Linode.

These are big companies and will censor offensive content. If you're lucky, they won't just delete your VPS without warning.

Second, you need an IP address and an 'autonomous system number' (ASN). These are allocated by Regional Internet Registries (RIRs). ARIN is the RIR for the United States, and there are 5 in total for the entire world. If ARIN says you don't get any Internet resources, you have no appeals process because they are a private company, and you *need* their resources. When you rent a server from a company, these issues are handled for you. If you're not allowed to use a VPS, you have to do it all yourself. It's both very expensive and very technical.

Third, you need an upstream service provider (ISP) to connect you to the Internet. Your upstream is important, because you have to physically connect your server to their network. Your area has a limited number of available ISPs, and they are private companies which can terminate your service at any time for any reason or no reason. ColoCrossing in Buffalo physically unplugged my servers in 2019 for hosting the Kiwi Farms and Encyclopedia Dramatica.

Fourth, you need peers. Peers are other ISPs that talk to your ISP. Peering is how the Internet actually works. When data traverses the Internet most of its route is done through third party networks, not your upstream directly. If your content is offensive enough that peers start refusing to deliver content to or from your IPs, you can essentially be cut out from the world wide web. NTT refuses to peer with any company that peers with my subnet, for instance.

Fifth, you'll need a domain name. All the above simply routes traffic to an IP. While you can run a website with just an IP (see 1.1.1.1), most people would prefer to type in "zerohedge.com". This requires the blessing of two more companies: The registrar which leases the domain to the customer, and the Network Information Center (NIC) which owns the top-level domain. As an example: ZeroHedge uses EasyDNS as its registrar, and all .COM domains are controlled by Verisign. Getting permission from Verisign to sell .COM addresses costs $3,500 and an additional $4,000 a year. Without this permission, you must rely on a 3rd party registrar for your domain, and they may seize your domain for any reason or no reason at all.

When DreamHost (a company I bought my first domain from when I was 16 in April 2009) tells me "you can't host kiwifarms.net with us anymore and we're closing your account with us in 14 days", it puts me in a difficult spot. If I just dump Kiwi Farms's domain on another company, then they may be less kind and simply seize the domain! Nothing stops them from doing so.

I've moved the Kiwi Farms domain to Cloudflare's domain registrar. This is a very risky decision, because in the past the mob would direct its noise at both Dreamhost and Cloudflare. Now, there's a more centralized point of failure. I am ordinarily afraid to even say the name Cloudflare, as if speaking it aloud could remind them I exist and compel them to step on me.

Why is Cloudflare special?

To recap: I own my own servers (roughly $20,000 in equipment). I also own my own IPs and ASN ($2,000/yr). I have my upstream ($500/mo). I could become my own .NET domain registrar ($3,500 + $4,000/yr). I have, to the best of my ability, within the limits of a 28-year-old's budget, "built my own Internet".

Despite all that, the Internet has one more weak point: Denial of Service Attacks. These attacks use compromised computers to send massive amounts of junk data to a single point, blotting out legitimate traffic and potentially overwhelming target devices.

DoS attacks are cheap. Botnet resellers are easy to find. They're easy to use. However, they are not cheap to mitigate. A 10Gbps attack costs less than $100 for a month, but a 10Gbps line costs $750/mo. 10Gbps-capable routers costs thousands. That is already excessive, but attacks frequently top 100Gbps or even 1000Gbps. Few companies can handle this job. Those companies come under intense political scrutiny. Cloudflare is the biggest, and I use them.

Websites that many people would prefer to stop existing, such as mine, are kept protected by the whims of one man. I've never met him and I've never spoken to him. I am sure he knows I exist only because of the outrage directed at him that my website causes.

Matthew Prince, the CEO of Cloudflare, is an outlier in the elite of Silicon Valley. He is the one person whose default position on censorship is "no". Cloudflare has removed two websites explicitly aligned with neo-Nazism, but ordinarily, they refuse to buckle to the mob. Why? I don't know. Maybe he's just libertarian. Maybe he wants the Internet to be free, like it used to be. Maybe he's a government informant (there's a popular conspiracy theory that Cloudflare is a large man-in-the-middle spyware operation). Even if he is, I don't care. My website is legal and there's nothing on it that's not public anyways.

Prince is just one man, however, and I have no doubt that when he retires he will be replaced by less of a man. Some political activists who endeavor to censor the Internet are simply waiting for the day he's gone. There are other DDoS mitigation services, but they're much smaller, often not as capable, and not in as strong a position to say "no". When he is out of power, it will cause a vacuum that will negatively impact the health of the Internet, and he will not be readily replaced by anything.

What few alternatives to Cloudflare exist are politically active. Voxility, Path, X4B, and others are competitors. Voxility is one of the worst in terms of being politically active. X4B is in Australia and beholden to strange, foreign laws about speech which are irreconcilable with the United States. Path peers with NTT and are unavailable to me because of NTT's embargo on my subnet. DDoS-Guard is a Russian alternative, but dealing with Mother Russia has its own issues.

“Build your own Internet somewhere else?”

The Internet is developing its own herd immunity to controversial material. Once a certain number of ISPs say they won’t peer you, you’re screwed. These companies are consolidating all the time, your list of options are smaller every year, and the group of people actually making decisions shrinks with it.

No company has management with spine. People just want to make as much money as possible and with as little noise as possible. Few companies will take a financial hit on principle. The mob takes advantage of this to censor the Internet with great effect. This is a precursor of things to come.

What if I moved everything out of the US to a ‘free’ country like Russia? Now I have Russian hardware, Russian IPs, a Russian upstream, Russian peers, Russian DDoS mitigation, and a nice .RU domain to top it off. What happens next?

Assuming there were no issues with local laws and government (there would be) and assuming I would not be extorted by officials, it would only kick the can down down the road. Just as moving VPS companies kicked the can to the next VPS company. Just as getting my own IPs kicked the can to upstream. Just as getting a stable upstream kicked the can to DDoS mitigation. This would kick the can another few years down the road to the upcoming Internet schism, where my website will suddenly be on the Russian side of the new regional internets.

I have spent thousands of dollars consulting with attorneys, solicitors, and advocates across the world regarding the legal protections of Internet services in their countries. Whatever is out there, it is not better than what is back at home.

We must resolve to fixing the problems we have here in the United States instead of trying to offload the responsibilities of the Internet and our freedoms onto a random country. Russia will not go out of its way to protect American’s free speech.

> “Whatever America hopes to bring to pass in the world must first come to pass in the heart of America.” — Dwight D. Eisenhower

The Broader Impact

In 2007, thousands of websites competed for traffic. By 2014, that number was 35 (source). In 2021, Google and YouTube (subsidiaries of Alphabet LLC) make up enough traffic by themselves to beat the next 30 top websites combined.

ISPs are consolidating too, and telecom as an industry is harder to break into. You will need to lay cables to do business, and most areas have one-company rights for those cables. Meanwhile, Google and Amazon set up their own infrastructure and get what they need. Google’s Cloud and Amazon’s AWS are nation-state sized internets by themselves, controlling a massive amount of global traffic.

We have a competition crisis. Think of all the startups hoping to compete with Google, YouTube, and Twitter that have come and gone in the last few years. Nobody can stand up to this tide, and the few willing to try are destroyed by the whims of these mega-corporations (enriched with government contracts) who have no interest in seeing ordinary people challenge their absolute, totalitarian control over all online media.

For every Kiwi Farms, Gab, 8chan, and Bitchute which tried to deal with these problems head on, there are a hundred others who (wisely) realized at the first set of hurdles that this was a challenge out of the budget and reach of an ordinary person. Our Internet could be so vibrant and healthy if the artificial limitations imposed by third parties were removed.

What can be done?

The Legislative Fix

Section 230 protects all of these service providers from civil liability for hosting my website. Few of them are willing to wield it like a shield to resist censorship, but rather as a sword to cut down with impunity. 230(c)(1) gives them immunity from civil action from what they *do* host, while 230(c)(2) gives immunity to civil actions from people they choose to censor.

The legislative solution (altering Section 230 to discourage censorship) requires editing Paragraph (2) without killing Paragraph (1) in the process. This requires a surgical precision. While there are many proposals for changing Section 230, they are terrible.

Republicans tend to clumsily address the issue while either not fixing the core problem or just creating new ones. Sen. Hagerty's bill, for instance, rewrites Section 230 as Section 232 and provides sweeping common carrier rules and consumer protections, while exempting broadband providers. Thereby, he encumbers providers while not addressing the core issues at all.

Democrats tend to hijack the issue, making services liable only for 'extremist content' and 'hate speech'. See Sen. Mark Werner's "SAFE Tech" act.

I am extremely hesitant to ever suggest modifying Section 230. However, simply striking or modifying a single paragraph – 230(c)(2) – would be enough to allow us to sue businesses interfering with our business. There are some proposals to try this:

1. Sen. Kelly Loeffler's 9-month-old Stop Suppressing Speech Act of 2020 with zero cosponsors. This removes vague wording so that providers can't remove everything they want. House counterpart H.R.7808 has some traction.

2. Sen. Wicker's Online Freedom and Viewpoint Diversity Act, which has a similar 230(c)(2) rewrite and more cosponsors. It also modifies a definition so that upstream providers are more liable for censorship and business interference.

These bills are now mostly idle after Trump left office, but they're still there if you're eager to write your representatives.

The Financial Fix

The issue of financial censorship, which I wrote about in *Section 230 Isn't The Problem, Payment Networks Are*, is present here as well. In summary: MasterCard, Visa, Discover, and Amex controls almost all consumer spending in the United States, and they will frequently stop payments to specific websites, companies, and individuals with intention of destroying them financially for political purposes.

A lot of small companies don't have to choice to say "no" to the mob, because payment networks will say "yes" for them. Regulating these payment networks, setting up an alternative (the Federal Reserve is trying to set up an instant bank-to-bank transfer service called FedNow), and mainstreaming alternative currency payments (cryptocurrency or even precious metals) are ways around this financial censorship.

At the very end of the Trump administration, the Comptroller of Currency passed regulation titled *Fair Access to Financial Services*. The week Biden entered office, it was put on permanent hold. This would have been a huge step towards alt-tech gaining a foothold.

The Onion Fix

Some people suggest moving to a .ONION domain on the Tor Network, which requires a special browser to access. However, I believe that all US legal content should be accessible by a regular person with an ordinary web browser, and found without hassle on search engines. Allowing our speech to be covered up, hidden, and sidelined is a losing strategy.

Tor is great for protecting people accessing websites. By hiding the route traffic takes, people in non-free countries can find censored materials safely through Tor.

Websites can set up what's called a "hidden service". Having a hidden service bypasses requirements for domain name registration and hides the origin of traffic, making it effectively impossible for anyone to do anything about content hosted on Tor. There is some wisdom in this, but hiding minimizes the accessibility of those services and simply yields more ground to the mob. Mainstream browsers like Brave natively supporting access to the Tor network is helping on this issue.

There are Tor-like services attempting to use cryptocurrency concepts to create a strong, private network which has all the benefits of Tor, plus built-in tools to circumvent financial censorship. I pay attention to OXEN in particular, but it is not yet a drop-in replacement for Tor or a ready solution for general purpose websites.

The Real Fix

The most powerful and readily accessible fix to censorship is also completely free and available to everyone. More than anything, what our free Internet requires to stay free is for free men to have the courage to stand up to the mob, and use their positions to be the change they want to see in the world. We need more than one Matthew Prince if we are going to keep our big-I Internet. All anyone ever needed to do is tell these people is “no”, as in: ***No***, I will not take down anything without a court order. It feels good to say it, trust me.

Joshua Moon
Where the Sidewalk Ends: The Death of the Internet
8 Jul 2021

<madattheinternet.substack.com/p/where-the-sidewalk-ends-the-death>

www.thetedkarchive.com