Anna Mitchell

Professor Nate Persily

INTLPOL 323

December 16, 2018

Hidden Censors: How Indirect Intermediaries Shape Online Speech

1. Introduction

"Literally, I woke up in a bad mood and decided someone shouldn't be allowed on the internet. No one should have that power." After a whirlwind five days of social media protests and internal tension, Matthew Prince, the CEO of Cloudflare, an Internet-services company, decided to terminate its contract with *The Daily Stormer*. The Internet's most popular neo-Nazi website had vanished from the Web.[1]

Cloudflare's content distribution network (CDN), improving the *Stormer*'s performance and protecting it from distributed denial of service (DDoS) attacks, had allowed the site to stay afloat for months or years. But that changed in 2017 during a period of tense racial relations in the United States. From August 11 to 12, the *Daily Stormer* helped organize the white supremacist *Unite the Right* rally in Charlottesville, Virginia. Soon after, it published articles calling murdered protestor Heather Heyer a "sloppy lard ass" and labeling her death an accidental heart attack.[2]

Reaction was swift. The next day, activist Amy Suskind tagged web hosting service GoDaddy in a Twitter post: "@GoDaddy you host The Daily Stormer - they posted this on their site. Please retweet if you think this hate should be taken down & banned."[3] Within 24 hours, GoDaddy responded by withdrawing hosting services. When the *Stormer* tried to switch to Google, it soon followed suit.[4] Zoho refused to provide email service,[5] and Twitter shut down

associated accounts.[6] With multiple major companies withdrawing services, it became increasingly difficult for the *Stormer* to host and propagate content.

Cloudflare held out, continuing to provide CDN services despite widespread opposition. Many of the requests to withdraw protection came from hackers who wanted to DDoS the site, overwhelming its server with requests to remove it from the Internet. Cloudflare, however, had long held a policy of content neutrality, refusing to censor a client for political beliefs.[7] Finally, when Andrew Anglin, the editor of *The Daily Stormer*, gloated about his supposed white supremacist allies within Cloudflare, the company caved. On August 16, 2017, Cloudflare terminated *The Daily Stormer* and published an explanatory blog post.

In the post, CEO Matthew Prince, a constitutional lawyer and self-described "free speech absolutist," made two seemingly contradictory statements. First, he admitted to waking up that morning and deciding Cloudflare should not be on the Internet. The *Stormer*'s blatant accusation of the company being a white supremacist ally had made it impossible to remain neutral. But he also took a stance unlike any of the other tech companies. Prince insisted that unilateral moves by Cloudflare and others must never happen again because they threatened speech on the Internet. Decisions to sever ties must be based on due process, not social media furor.[8]

Refusing to host a site or provide DDoS protection may not pose an obvious threat to speech on the Internet. Discussions about speech revolve around content platforms like Facebook and Twitter, not deeper layers of Internet infrastructure. When we talk about biased censorship on the Internet, we think of YouTube banning accounts or Google twisting search results, not GoDaddy refusing to host a site. But the *Daily Stormer* case revealed that many hidden layers of Internet infrastructure are vital to free speech. A blogger cannot be heard worldwide unless he convinces an Internet hosting company to host his data on their servers, a certificate authority to

offer him a certificate, a DNS resolver to grant him a unique address on the Internet, and a content distribution network to protect him against DDoS attacks. After losing its domain name registrar, DNS proxy services, a DDoS protection service, and hosting provider, the *Stormer* could not reach its readers.

But these multiple layers of Internet infrastructure also present difficult questions about speech on the Internet. The *Daily Stormer* controversy raised many questions about the role of "indirect intermediaries"[1] in regulating online speech. Should these companies offer their services equally to all sites, regardless of their content? Or should they monitor the content passing through their systems, to avoid accidentally abetting neo-Nazis? If such a policy were to exist, how would companies form and apply it in an unbiased manner? While we usually think of Internet service providers (ISPs) when we think of "net neutrality," should these companies be neutral as well? If so, do all categories of Internet infrastructure fit the description of "public utility," or only more monopolistic ones?

Most discussion about how intermediaries curate and censor speech on the Internet has focused on the actions of "direct intermediaries": social media platforms. Little work has examined the role of the "indirect" or "upstream" intermediaries in Internet infrastructure like certificate authorities, web hosts, and DNS resolvers which perform hidden functions allowing websites to exist. Indirect intermediaries are farther removed from content than social media

[1] Internet infrastructure services fall into two categories: direct intermediaries like Facebook and Twitter, which directly publish speech, and indirect or "upstream" intermediaries like web hosts, DDoS protection services, which perform hidden functions enabling websites to exist. Throughout this paper, I refer to hosting providers, certificate authorities, content distribution networks, etc. - as "indirect intermediaries," "upstream intermediaries," or "Internet infrastructure providers." Platforms like Twitter and Facebook are described as "direct intermediaries," "social media platforms," and "content platforms."

platforms and can thus better claim to be "intermediaries"; the answers to the earlier questions, therefore, will be different for indirect intermediaries. This paper examines the role of indirect intermediaries in shaping speech on the Internet in America and argues that these institutions should be content-neutral, serving all customers regardless of their site's content. We first examine how each layer of the Internet functions; then consider historical controversies over censorship at each level and risk factors for future censorship in America.

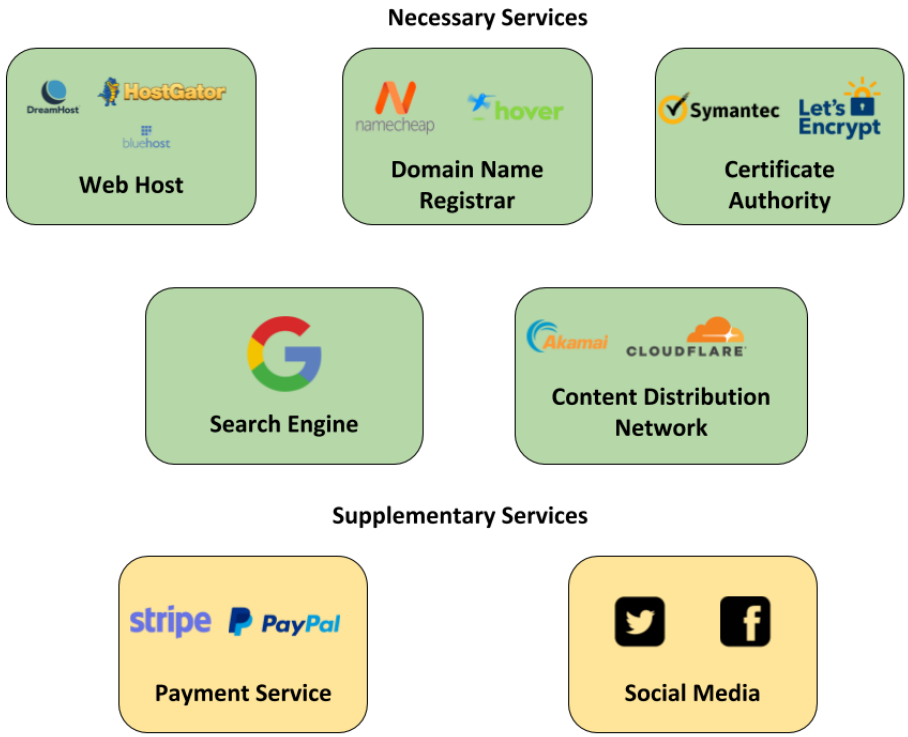
The second half of the paper will consider how companies and lawmakers should address these questions in the future. I argue that the principle of "net neutrality" should apply to all indirect intermediaries, not only ISPs: no Internet infrastructure company should censor content passing through their services. American intermediary liability law exempts Internet infrastructure providers from any legal requirement to actively police and censor illegal content, but also allows companies to set their own content policies. If a conservative service wished to only host conservative sites, it could. However, content neutrality is in the best interests of the Web. Direct hosts like Facebook and Twitter already have difficulty implementing unbiased censorship; indirect intermediaries are farther removed from content and thus even more poorly poised to censor it. At the company level, companies should implement at least due process, and preferably, neutrality provisions that prevent them from removing content unless required to by law enforcement agencies. Internet governance institutions like ICANN would also play a critical role in incentivizing neutrality. Without a renewed commitment to neutrality at the infrastructure level, free speech on the Internet will be in danger.

2. The Life of a Blog Post: A Crash Course in the Internet

Understanding how restrictions at each level would affect speech on the Internet requires a basic understanding of how the Internet works. Imagine yourself as an aspiring blogger. What steps must you follow to publish your work online? Then, consider the steps a site follows to deliver content to its readers. Along the way, a host of gatekeeping institutions potentially block the journey of the reader and the writer, potentially preventing the circulation of online content.

First, imagine you are an amateur political philosopher who reads Locke and Carlyle and analyzes American politics. You hope to win an audience through a personal website. However, putting *tabularasa.com* online requires winning the support of several gatekeepers before the public can read your opinions.

2.1 Publishing a Site



1. Sign up for a ***web host,*** which stores your website's content on its servers. After paying a yearly fee, you upload your HTML, CSS, and JavaScript to the server. Now, any reader's web browser can make a request to view *tabularasa.com* and establish a connection with your server. Upon request, the server will send the site's content to the reader for display.[9] Popular hosting services include Dreamhost, BlueHost, and HostGator.[10]
2. Buy a unique domain name ("tabularasa.com") from a ***domain name registrar***. When the reader types this URL into her web browser, the page should load. Often, a web hosting service will help you pick a name and configure it. Otherwise, you could use a dedicated service such as Namecheap, which sells domain names.[11]
3. Obtain a certificate from a ***certificate authority***. When a reader loads a page in Google Chrome, for example, the green lock icon allows him to check the site's identity by viewing its certificate. Readers can now check that a trusted third party has verified that your website is who it claims to be. For this to happen, you must obtain a certificate from a third-party certificate authority (CA), which will perform cryptographic verification to prove that you own the site you claim to own. Once the verification is done, the CA will provide you a certificate to upload to your web host.[12] Some popular CAs include Symantec and Let's Encrypt.[13]
4. Sign up for a speedier and better-protected site using a ***content distribution network (CDN)***. A CDN improves your site's performance and protects it from attacks by distributing its content across different servers. For example, the CDN might place copies of the blog on servers located in Africa, Asia, and the US. When the reader requests to view the website, it returns the copy of data from whichever server is geographically closer. CDNs also protect a site from distributed denial of service (DDoS). These attacks

overwhelm a server with requests until it crashes. Distributing the website's content across multiple servers makes it unlikely that any one server could be overwhelmed with requests.[14] Popular options include Cloudflare and Akamai.

5. Create a file on your site giving permission to ***search engines*** to crawl it and display it in response to relevant queries. This makes your site discoverable.
6. (Optional) Add a donation form using a ***payment service***. This is a lifeblood for many independent bloggers who earn their living from content creation.
7. (Optional) Post about your blog on ***social media*** accounts. These platforms help you publicize your work.

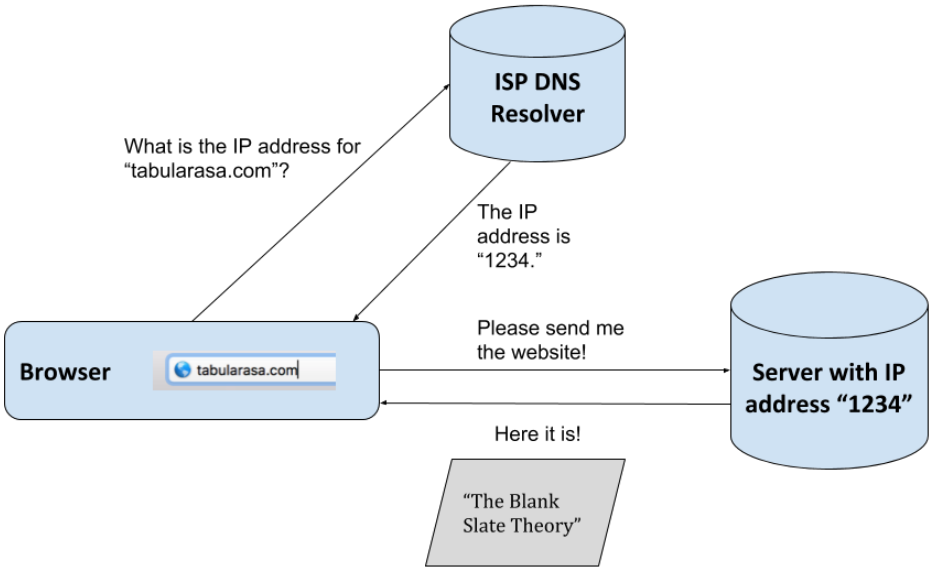
Congratulations! After purchasing a litany of services, your website is finally online. Your Google Analytics page reveals new readers every day. We now understand the basics of how a writer publishes her work online and what array of intermediaries must provide crucial services before her work can be read. To complete our understanding, we must switch sides to become a reader of *tabularasa.com*. Several key steps allow the reader to load and view the site on Chrome or Firefox.

2.2 Reading a Site

1. Make a request to a ***domain name system (DNS) resolver*** to look up the site's location. When you press "enter" on your web browser to view "tabularasa.com," the browser determines the location of the requested content, which is uniquely identified by an IP, or "Internet protocol," address. The mapping between URLs and IP addresses is stored on a DNS resolver. By default, the browser will ask your ISP to look up the DNS – for example, my web browser would automatically ask Comcast to determine the IP address

for “tabularasa.com” and send it back. Now, you should be able to access the URL with a machine-readable unique identifier.[15]

2. The browser initiates a TCP/IP connection with the ***Server/Web Host*** using the IP address. This server stores all the information for the webpage. Once the browser and server verify each other’s identities, the browser requests the blog information. The server sends it back to the browser, which displays it.[16]
3. ***Content Distribution Network.*** This is an optional layer in front of the server that allows information to be stored on multiple servers instead of one. If the site is using a CDN, the browser might ask the CDN for the site’s content instead of the server.



A writer uses several services, including a web host, domain name registrar, certificate authority, content distribution network, and others, to publish her content online. A reader requires a DNS resolver and a CDN to view the site on her browser. However, this process does

not always occur so smoothly. In fact, censorship has occurred at all levels of the stack. In the next section, we examine historical censorship controversies and the current outlook for speech at several key layers of the stack.

3. Case Studies in Censorship

3.1 Web Hosts

Web hosts are the most visible indirect intermediary. For a fee, a host stores the contents of a website on its servers. Without web hosting services, anyone creating a website would need to establish his own server, a daunting task for a non-technical Internet user. Because hosts are the most obvious enablers of Internet speech, they have often been first in line for criticism. While *The Daily Stormer* was only the most recent case, web hosts are frequently asked to censor their users on the grounds of copyright violation or hate speech.

Copyright violations are one of the most common justifications for takedown requests. Under the Digital Millennium Copyright Act, an online service provider may avoid liability for copyright infringement committed by customers if it follows a prescribed process upon notification of copyright infringement. However, not all requests are legitimate. Over half of the notices submitted to Dreamhost's Abuse team do not represent legitimate copyright violations.[17]

Often, copyright is a thinly veiled excuse for powerful institutions to silence critical rivals. Many cases involve powerful corporations accusing users of violating copyright laws. In one, the U.S. Chamber of Commerce attempted to punish the Yes Men, a group of activists, for a parody video in which they impersonated a Chamber of Commerce spokesperson. Claiming a violation of the Chamber of Commerce's trademark, they pressured the Yes Men's hosting provider to cancel its service. They lost the lawsuit.[18] In another case, ABC News sent false

copyright claims to 1&1 Internet, the hosting provider of a blogger nicknamed "Spocko," as retaliation against him posting clips from an ABC-owned radio station with critical commentary. 1&1 Internet caved to ABC's threats and Spocko was forced to switch providers.[19] These abuses of power silence speech.

Many hosting providers do not have strong policies against intimidation. Smaller hosts would prefer to avoid an expensive and protracted legal battle with more powerful companies, often choosing to give up a single customer to avoid this hassle. Cindy Cohn, president of the Electronic Frontier Foundation, claims that "the relative power of those facing censorship plays a key role in who gets censored and who does not."[20] Accordingly, many web hosts' vague Terms of Service allow them to terminate service at will. HostGator's ToS agreement claims that it "does not monitor User Content" and "exercises no control over…User Content…passing through [its] computers, network hubs, and points of presence or the Internet." However, the agreement also contains a clause allowing it to "immediately take any corrective action in HostGator's sole discretion," including termination of services.[21] Despite this, other notable hosts have publicly spoken out to defend the web host as a content-neutral intermediary. Dreamhost publicly reiterated strong support for the First Amendment, explaining that "we are a resource for publishers of all backgrounds, not a clearinghouse for thoughts and opinions (however distasteful some of them might be)."[22] Overall, however, web hosts are often the first institutions asked to remove speech. Protected by their Terms of Service, often quickly comply to avoid an expensive legal battle.

3.2 Domain Name Registrars

Domain name registrars allow sites to register unique URLs like "tabularasa.com." They associate a human-readable name with a machine-readable IP address, or unique location for

your site's content, in the global Domain Name System. Without a domain name registrar, a reader could not type your website's name into a browser to load the page, because the name would not be associated with your site's IP. Again, copyright has often been used to pressure domain name registrars into withdrawing services. When satirists created a fake version of the *New York Times* that mocked the diamond corporation De Beers in a joking advertisement, De Beers asked that Joker.com, the site's domain name registrar, remove its registration. The case was argued by the Electronic Frontier Foundation and won.[23]

An extensive study of domain name registrars found that their Terms of Service agreements often permitted termination of service for vague reasons, leaving the possibility of ideologically- or intimidation-motivated censorship.[24] For example, GoDaddy's "Domain Name Registration Agreement" allows the termination of contracts if sites are found to engage in "morally objectionable activities," which include "activities designed to encourage unlawful behavior by others." This definition can be liberally interpreted to justify termination of a wide variety of sites. In fact, the study surveyed Terms of Service agreements of all of the domain name registrars participating in the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit governing registrars. It found that 57% of domain names under ICANN's territory were owned by registrars who had morality clauses. A further 18% used registrars with a "sole discretion" or morality clause equivalent that would allow their provider to terminate their registration at their discretion. Furthermore, section 3.18 of ICANN's rules encourages registrars to quickly remove content when asked, without any governmental due process. If over half of copyright notices received by registrars, like Dreamhost's, were false, then following this policy would remove much legitimate speech! Thankfully, the market for domain name registrars is competitive, allowing consumers to switch providers. However, an ICANN-wide

content neutrality policy could ensure a precedent for content neutrality, without the additional hurdle of switching providers.

3.3 Content Distribution Networks and DDoS Protection

The Daily Stormer was only the most controversial client for Cloudflare, which has since received around seven thousand requests to terminate content distribution network services for sites around the Internet.[25] Cloudflare's CDN improves load times for sites using its services by storing their data at servers around the world. When a user requests to view a site's page in her browser, Cloudflare returns a copy of the site's data from the server geographically closest to the user, allowing the site to be loaded faster.[26] More crucially, however, Cloudflare also protects sites from distributed denial of service (DDoS) attacks. A distributed denial of service attack overwhelms a server by overwhelming it with Internet traffic. An attacker coordinates a network of Internet machines to bombard a targeted site with requests. If successful, the site's server will crash and the site will not load.[27] Since the attacker uses multiple machines which alone may send a normal number of requests, it is difficult to block attackers without cutting off legitimate users.

DDoS attacks famously downed Estonian government agencies, financial institutions, and media outlets in a 2007 attack usually attributed to Russia.[28] Other large attacks targeted GitHub and Dyn, a DNS company.[29] Many DDoS attacks originate from "booter" or "stresser" services that allow amateur users to purchase a DDOS attack and kick anyone off the Web.[30] One service, WebStresser, taken down by US and UK authorities in 2018, allowed users to purchase a DDoS attack for as little as $14.99.[31] DDoS is a cheap and easy way to silence your enemies.

Without CDNs, then, sites become slow and vulnerable to existential attack. Despite this, CDNs have not been spared by large companies complaining about copyright infringement. Recording groups such as the Recording Industry Association of America (RIAA), Motion Picture Association of America (MPAA), and PhRMA repeatedly target CDNs for protecting sites alleged to have violated copyright.[32] As we saw previously, these copyright suits are often frivolous, yet CDNs still respond by removing the site.

Until the *Stormer* case, however, outright censorship for political purposes was uncommon. But now, many feel that Internet services should not protect hate sites. Cloudflare's first termination requests for the *Daily Stormer* originated from a would-be attacker, Jester, who requested it to "get out of the way so we can DDoS this site off the Internet."[33] Later, the Southern Poverty Law Center published an angry exposé blaming Cloudflare for "optimizing 48 hate sites" across Europe.[34] Another piece explicitly listed hate sites, their hosts, and their Cloudflare protection status.[35] A *Wired* article sensationally asked "why Cloudflare let an extremist stronghold burn." A growing coalition of media now asks Cloudflare to withdraw CDN services, even if doing so could expose sites to existential DDOS attack. In a sense, then, CDNs are deciding whether these sites should exist.

4. Content Neutrality: Why and How to Enforce It

These arguments are well-intentioned, aiming to prevent hate speech from overwhelming the Internet. But evidence suggests that, rather than actively policing hate speech, a policy of content neutrality is far better for the Internet and public dialogue. A long tradition of Internet scholarship argues that intermediaries should not regulate content. Tim Wu's original "net neutrality" paper suggested that broadband operators should not restrict what individuals do with their broadband networks.[36] More broadly, however, the principle suggests that Internet

providers should treat all data on the Internet equally, as neutral intermediaries serving as public utilities.[37]

This principle is usually applied to ISPs, but it applies more obviously to indirect intermediaries than direct ones like social media platforms that actively curate content.[38] However, American Internet providers are free to apply their own standards for selecting content and clients. The First Amendment and Section 230 of the Communications Decency Act also protect Internet intermediaries' rights to regulate their own content. [39] While the controversies described in the previous section might be disturbing, they are not illegal.

Simultaneously, however, no American law forces platforms to scan and remove certain types of content. This is because intermediary liability for Internet providers in the United States today is primarily shaped by Section 230 of the 1996 Communications Decency Act. Originally intended only to address pornography, it criminalized distributing "obscene or indecent" material to those under age 18. Though the rest of the act was deemed unconstitutional by the Supreme Court in 1997, an amendment added by the House, Section 230, survived. A response to earlier lawsuits trying to hold ISPs and web hosts responsible for defamation by their users, it provided a "safe harbor" for platforms: ISPs and web hosts could not be held liable under state law for users' posts. [40]

This short amendment would shape the formation of the Internet. It enabled smaller platforms to flourish, unencumbered by extreme legal requirements which would have proved too great a burden to enforce. Additionally, it promoted a culture of free expression since platforms had no incentive to pro-actively moderate and over-remove content to avoid liability. Many commentators credit Section 230 of the CDA with enabling the United States to become an Internet leader. American law determines that content platforms are not obligated to moderate

content, but they may also freely impose their own terms of service agreements for speech on their platforms. Google and Cloudflare's denial of service to *The Daily Stormer* was a perfectly legal exercise of their right to freedom of association.

Recent controversies over CDA's application to direct hosts had the unintended effect of affirming its applications to indirect hosts. While the law was intended to apply to ISPs and web hosts, in recent years its provisions have most notably protected social media platforms like Facebook and Twitter from legal repercussions for hosting fake news and foreign-sponsored political advertising.[41] Many argue that the CDA was intended to apply to platforms that only "provided access to the Internet or conveyed information." Social media platforms that actively curate their users' feeds do not meet this criterion. Tarleton Gillespie argues that social media platforms compose a new hybrid category between traditional media platforms that published their own content and ISPs, which simply propagate content.[42]

This debate clarifies the application of the law to Internet intermediaries. Content distribution networks, web hosts, certificate authorities, and others simply enable information platforms. Their responsibilities do not include actively creating or moderating content. The legal basis for Internet infrastructure companies' intermediary liability is clear; platforms can do whatever they want. In practice, however, platforms have exercised the freedoms afforded by the CDA in different ways. One paper presents a useful framework for understanding platforms' approaches: "rule-of-law" and "discretion." Domain name registrars applying a "rule-of-law" approach only suspend customers or censor speech in response to law enforcement agencies' requests, court orders, or other legal requirements. This approach favors the consumer, since platforms accept customers by default instead of applying their own policy. Others take a discretionary approach, in which they suspend service based on their opinion of the domain they

support. More broadly, platforms taking a discretionary approach could suspend service or remove speech according to their opinion of that speech.[43]

A rule-of-law approach that allows all content unless explicitly determined to be illegal is important for the future of the Internet. First, the content of the sites does not affect the experience of other users using the services of an indirect intermediary. Social media companies like Facebook have clear "terms of service" that prohibit gory violence or pornography; without them, these sites would be unusable. If GoDaddy hosts a pornographic website, this does not degrade or interfere with the experience of other customers.

Second, indirect intermediaries have little power to granularly moderate information. Because Facebook and Twitter control every post and comment on their domains, they must employ an army of content moderators to manually review flagged posts. Their constantly-expanding content policies encompass hundreds of rules.[44] Internet intermediaries do not have this granular control. Unlike social media companies, they do not ultimately control the domain in question. Therefore, their only option is to remove the entire site. Facebook, Twitter, and others already receive ample criticism for poor content moderation without any recourse for due process. If these large, well-resourced companies already often fail in content moderation, why would indirect intermediaries, with less control and fewer resources, perform better?

One powerful argument against content neutrality is that businesses should be allowed to freely manage their risk by denying a client who would potentially repel other clients. Client outcries could be mitigated if indirect intermediaries clearly stated the limitations of their abilities to remove a site. For example, smaller platforms could emphasize their inability to moderate at scale or remove only certain pages of a site. A more powerful solution would be the imposition of stricter rules around content neutrality by large Internet governance institutions

such as ICANN, the domain name registrar organization. ICANN could add a provision to its rules preventing domain name registrars from including "morally objectionable" or "sole discretion" clauses in their contracts.[45] This would deflect blame away from single businesses and towards the more powerful governing body, mending the power imbalance that prevents smaller platforms from standing up to the powerful businesses or social media outcry.[46] If responsibility lay with a single governing body that could not be easily boycotted since it encompassed a huge portion of the market, risk management concerns could be mitigated.

Content neutrality is important because there may not be enough competition to go elsewhere. This is especially true at the ISP level: one study by *PCMag* showed that 70% of zip codes only had access to zero or one ISPs for 25MBPs Internet service.[47] Is this true, however, for other indirect intermediaries besides ISPs? Though at some layers there are many choices, one blockage at any layer will remove a site from the Internet. In one 1999 case, OneNet Communications, a parent ISP provider of a smaller ISP, Plebeian Systems, which was hosting the controversial "Nuremberg Files" listing the personal data of abortion doctors, received so much "heat and email" that it pressured Plebeian into removing the site or else lose service. One commentator stated that "these people will go after every link of the chain until one of the links breaks."[48] This was in 1999! Today when a case goes viral, social media can provoke widespread boycotts and shaming of providers. In the case of Gab, the right-wing social media platform and favored outlet for the 2018 Pittsburgh synagogue shooter, PayPal, Stripe, Microsoft Azure, GoDaddy, and Medium terminated service, removing the site from the Internet.[49] Finally Gab found a new host in Epik.com.[50] However, one could easily imagine an Internet landscape in which enough intermediaries at a given level are reluctant to host a controversial site that it is

effectively silenced. Competition is not guaranteed, and constantly jumping providers is a potentially existential obstacle for an under-resourced website.

Given the tendency of social media platforms to simplify issues and amplify emotional rhetoric, it is hard to argue that any social media mob should control who should be on the Internet. On both sides, mobs of Internet commentators insult, name-call, even dox targets. These mobs run the gamut from conservatives angry at *New York Times* columnist Sarah Jeong's controversial tweets,[51] to liberals angry at the invitation of Steve Bannon to a *New Yorker* conference.[52] Often, the loudest voice, not the most moral voice, determines the outcome.

Even if companies were to ignore the public and abide by their own impartial rules, imposing an unbiased standard and abiding by due process is logistically unlikely. Cloudflare CEO Matthew Prince emphasizes the importance not of "freedom of speech," but of "due process" online. However, an extensive content policy to adjudicate these cases and offer an appeals process seems impossible for every indirect intermediary to implement, because many are under-resourced. The problem is difficult enough for social media giants Facebook and Twitter, often punishing unintended victims. For example, Facebook shut down conversations among African-American women about the harassment they faced online,[53] and censored mothers who share breastfeeding images in private groups.[54] Facebook and Twitter often failed to provide an appeals process: 27% of appeals reported to OnlineCensorship.org were ignored.[55] If Facebook, with all of its resources, struggles with content enforcement, why would smaller intermediaries succeed in imposing a clear content policy and enforcing it with due process? A more practical solution is the "rule-of-law" approach favored by some of ICANN's domain name registrars, which only removes website when required by law enforcement. The Manila

Principles on Intermediary Liability could provide helpful, minimal guidelines for implementation.[56]

Even if a perfectly impartial standard could be imagined and adjudicated, there is no conclusive evidence that censorship would reduce the hold of these sentiments in the real world. Hateful speakers will likely exist on the Internet regardless of censorship. In fact, widespread bans could push radical speakers, galvanized by their "victim" status, to fringe corners of the Internet. Even temporarily de-platforming a site can swiftly spur the creation of more concentrated forums. After Gab's banning, many former members joined a site called "FreeZoxees," specifically marketed towards "Gabfugees."[57] One paper found through a simulation that filtering social media in times of political unrest ultimately results in higher levels of violence.[58] To the contrary, another paper found that banning offensive subreddits on Reddit did reduce the overall level of hate speech on the site. It is difficult to determine whether members of r/incels simply migrated to other corners of the Internet and radicalized further, worsening dialogue overall.[59] Until more evidence exists, it would be dangerous to censor widely.

5. Conclusion

A diverse array of actors mediate an idea's journey from a writer to a reader. Without web hosts, certificate authorities, domain name registrars, and others, Internet speech would not be possible. The power of these indirect intermediaries to block online speech is often overshadowed by more public controversies over direct intermediaries like Twitter and Facebook. However, recent controversies like that over *The Daily Stormer* demonstrated the censorship abilities of these private actors. While private platform censorship is legal - First Amendment and the

Communications Decency Act allow businesses to freely associate and moderate their own platforms - a policy of content neutrality at all levels would improve online dialogue. An impartial standard adjudicated through due process is nearly impossible for direct hosts to implement; let alone indirect intermediaries, often under-resourced and by definition farther removed from content. Instead, indirect intermediaries should only remove content when required by law enforcement, after rigorous due process. Only a strong policy of net neutrality at every level of the stack can safeguard the rich American tradition of free expression online.

---

[1] Johnson, Steven. "Inside Cloudflare's Decision to Let an Extremist Stronghold Burn." *Wired*, Conde Nast, 15 Feb. 2018, www.wired.com/story/free-speech-issue-cloudflare/.

[2] Anglin, Andrew. "Mystery on Fat Mountain: Heather Heyer's Autopsy Nowhere to Be Seen – Did She Have a Heart Attack?" *The Daily Stormer*, The Daily Stormer, 31 Aug. 2017, dailystormer.name/mystery-on-fat-mountain-heather-heyers-autopsy-nowhere-to-be-seen-did-she-have-a-heart-attack/.

[3] Amy Siskind. ".@GoDaddy You Host The Daily Stormer - They Posted This on Their Site. Please Retweet If You Think This Hate Should Be Taken down & Banned. Pic.twitter.com/FqTtGoTbmn." *Twitter*, Twitter, 14 Aug. 2017, twitter.com/amy_siskind/status/896908664900009984.

[4] Hatmaker, Taylor. "Google Drops Domain Hosting for Infamous Neo-Nazi Site the Daily Stormer." *TechCrunch*, TechCrunch, 14 Aug. 2017, techcrunch.com/2017/08/14/google-daily-stormer-domain/.

[5] Matsakis, Louise. "Following GoDaddy, the Daily Stormer's Email Provider Drops It as a Customer." *Motherboard*, VICE, 14 Aug. 2017, motherboard.vice.com/en_us/article/7xxvng/following-godaddy-the-daily-stormers-email-provider-drops-it-as-a-customer.

[6] Guynn, Jessica. "Twitter Boots The Daily Stormer in Latest Eviction for Neo-Nazi Site." *USA Today*, Gannett Satellite Information Network, 16 Aug. 2017, www.usatoday.com/story/tech/news/2017/08/16/twitter-boots-daily-stormer-latest-eviction-neo-nazi-site/573428001/.

[7] Johnson.

[8] Prince, Matthew. "Why We Terminated Daily Stormer." *The Cloudflare Blog*, The Cloudflare Blog, 29 Aug. 2018, blog.cloudflare.com/why-we-terminated-daily-stormer/.

[9] "What Is Web Hosting? ." *Website.com Website Builder*, www.website.com/beginnerguide/webhosting/6/1/what-is-web-hosting?.ws.

[10] Gewirtz, David. "Best Web Hosting Providers: InMotion, Hostgator, Bluehost and More." *CNET*, CNET, 14 May 2018, www.cnet.com/web-hosting/.

[11] Darwin, E.V., et al. "The Best Domain Registrars - the Good, the Bad and the Ugly - 2018 Guide." *Make A Website Hub*, Make a Website Hub, 23 Nov. 2018, makeawebsitehub.com/reviews/domain-registrars/.

[12] Kloepfer, Daniel, et al. "What Are Certificate Authorities?" *GlobalSign*, GlobalSign, www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies/.

[13] "The Top 5 Most Popular SSL Certificate Authorities Reviewed." *WPMU Dev*, Incsub, premium.wpmudev.org/blog/ssl-certificate-authorities-reviewed/.

[14] "What Is a CDN? How Does a CDN Work?" *Cloudflare*, Cloudflare, www.cloudflare.com/learning/cdn/what-is-a-cdn/.

[15] "What Is a DNS Resolver? - Definition from Techopedia." *Techopedia.com*, Techopedia Inc. , www.techopedia.com/definition/9176/dns-resolver.

[16] "How the Web Works." *MDN Web Docs*, Mozilla, developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works.

[17] "DreamHost's Guide to the DMCA - DreamHost.blog." *DreamHost*, DreamHost, 28 Aug. 2018, www.dreamhost.com/blog/dmca-guide/.

[18] "Diamond Conglomerate Attempts to Silence Critical Parody." *Electronic Frontier Foundation*, Electronic Frontier Foundation, 18 Nov. 2011, www.eff.org/takedowns/diamond-conglomerate-attempts-silence-critical-parody.

[19] "Spocko and ABC/KSFO." *Electronic Frontier Foundation*, Electronic Frontier Foundation, 5 Oct. 2011, www.eff.org/cases/spocko-and-abc-ksfo.

[20] Cohn, Cindy L. "Bad Facts Make Bad Law: How Platform Censorship Has Failed So Far And How To Ensure that the Response to Neo-Nazis Doesn't Make It Worse." 2 GEO. L. TECH. Rev. 432 (2018). https://georgetownlawtechreview.org/bad-facts-make-bad-law-how-platform-censorship-has-failed-so-far-and-how-to-ensure-that-the-response-to-neo-nazis-doesnt-make-it-worse/GLTR-07-2018/

[21] "Web Hosting." *HostGator Blog*, HostGator, www.hostgator.com/tos.

[22] Farivar, Cyrus. "Web Hosting, CDN Companies Torn as to How to Respond to Racist Websites." *Ars Technica*, Ars Technica, 17 Aug. 2017, arstechnica.com/tech-policy/2017/08/squarespace-set-to-kick-out-white-nationalist-websites/.

[23] "Diamond Conglomerate Attempts to Silence Critical Parody." *Electronic Frontier Foundation*, Electronic Frontier Foundation, 18 Nov. 2011, www.eff.org/takedowns/diamond-conglomerate-attempts-silence-critical-parody.

[24] Kuerbis, B., Mehta, I., & Mueller, M. (2017). In Search of Amoral Registrars: Content Regulation and Domain Name Policy. Atlanta, GA: Internet Governance Project, Georgia Institute of Technology. https://www.internetgovernance.org/wp-content/uploads/AmoralReg-PAPER-final.pdf

[25] Johnson.

[26] "What Is a CDN? How Does a CDN Work?" *Cloudflare*, Cloudflare, www.cloudflare.com/learning/cdn/what-is-a-cdn/.

[27] "What Is a Distributed Denial-of-Service (DDoS) Attack?" *Cloudflare*, www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

[28] "Famous DDoS Attacks." *Cloudflare*, www.cloudflare.com/learning/ddos/famous-ddos-attacks/.

[29] Newman, Lily Hay. "How Creative DDOS Attacks Still Slip Past Defenses." *Wired*, Conde Nast, 12 Mar. 2018, www.wired.com/story/creative-ddos-attacks-still-slip-past-defenses/.

[30] Krebs, Brian. "Who Is Anna-Senpai, the Mirai Worm? ." *Krebs on Security*, Krebs on Security, 17 Jan. 2018, krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/.

[31] Krebs, Brian. "DDoS-for-Hire Service Webstresser Dismantled." *Krebs on Security*, Krebs on Security, 25 Apr. 2018, krebsonsecurity.com/2018/04/ddos-for-hire-service-webstresser-dismantled/.

[32] "Content Delivery Networks (CDNs)." *Electronic Frontier Foundation*, 18 Aug. 2017, www.eff.org/free-speech-weak-link/cdn.

[33] Johnson.

[34] Hankes, Keegan. "Cloudflare Optimizing Content Delivery For At Least 48 Hate Sites Across Europe." *Southern Poverty Law Center*, Southern Poverty Law Center, 7 Mar. 2017, www.splcenter.org/hatewatch/2017/03/07/cloudflare-optimizing-content-delivery-least-48-hate-sites-across-europe.

[35] "How Tech Supports Hate." *Southern Poverty Law Center*, www.splcenter.org/hate-and-tech.

[36] Wu, Tim, Network Neutrality, Broadband Discrimination. Journal of Telecommunications and High Technology Law, Vol. 2, p. 141, 2003. Available at SSRN: https://ssrn.com/abstract=388863 or http://dx.doi.org/10.2139/ssrn.388863

[37] Doren, Peter Van, and Thomas A. Firey. "Understanding 'Net Neutrality'." *Cato.org*, Cato Institute, 14 Dec. 2017, www.cato.org/publications/commentary/understanding-net-neutrality.

[38] Keller, Daphne. "Toward a Clearer Conversation About Platform Liability." *Knight First Amendment Institute*, Knight First Amendment Institute at Columbia University, 2018, knightcolumbia.org/content/toward-clearer-conversation-about-platform-liability.

[39] "Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston, Inc." *Oyez,* 16 Dec. 2018, www.oyez.org/cases/1994/94-749

[40] Gillespie, Tarleton. "Platforms Are Not Intermediaries." 2 Geo. L. Tech. Rev. 198 (2018)

[41] Hwang, Tim, Dealing with Disinformation: Evaluating the Case for CDA 230 Amendment (December 17, 2017). Available at SSRN: https://ssrn.com/abstract=3089442 or http://dx.doi.org/10.2139/ssrn.3089442

[42] Gillespie.

[43] Kuerbis.

[44] Koebler, Jason, and Joseph Cox. "Here's How Facebook Is Trying to Moderate Its Two Billion Users." *Motherboard*, VICE, 23 Aug. 2018, motherboard.vice.com/en_us/article/xwk9zd/how-facebook-content-moderation-works.

[45] Kuerbis.

[46] Cohn.

[47] Segan, Sascha. "Exclusive: Check Out the Terrible State of US ISP Competition." *PCMAG*, PCMAG.COM, 15 Dec. 2017, www.pcmag.com/news/357972/exclusive-data-shows-the-terrible-state-of-us-isp-competition.

[48] "ISP Censorship." *Extremism and Censorship*, Stanford Computer Science, 1999, cs.stanford.edu/people/eroberts/cs181/projects/1998-99/nuremberg-files/censorship.html.

[49] Lieu, Johnny. "'Free Speech' Social Platform Gab Goes Offline after Fatal Pittsburgh Shooting." *Mashable*, Mashable, 29 Oct. 2018, mashable.com/article/gab-goes-offline-hosting/#jwkQ1aHvGOqf.

[50] Monster, Rob. "Why Epik Welcomed Gab.com." *Epik Blog*, Epik, 3 Nov. 2018, epik.com/blog/why-epik-welcomed-gab-com.html.

[51] Stephens, Bret. "The Outrage Over Sarah Jeong." *The New York Times*, The New York Times, 9 Aug. 2018, www.nytimes.com/2018/08/09/opinion/sarah-jeong-tweets-opinion-section.html.

[52] Sopan, Deb, and Peters W. Jeremy. "New Yorker Festival Pulls Steve Bannon as Headliner Following High-Profile Dropouts." *The New York Times*, The New York Times, 3 Sept. 2018, www.nytimes.com/2018/09/03/arts/bannon-new-yorker-festival-remnick.html.

[53] Oluo, Ijeoma. "Facebook's Complicity in the Silencing of Black Women." *Medium.com*, Medium, 2 Aug. 2017, medium.com/@IjeomaOluo/facebooks-complicity-in-the-silencing-of-black-women-e60c34434181.

[54] Dewey, Caitlin. "Facebook Is Embroiled in Yet Another Breastfeeding Photo Controversy." *The Washington Post*, WP Company, 26 Feb. 2015, www.washingtonpost.com/news/the-intersect/wp/2015/02/26/facebook-is-embroiled-in-yet-another-breastfeeding-photo-controversy/?noredirect=on&utm_term=.5b0adb6e5997.

[55] Anderson, Jessica, et al. *Censorship In Context: Insights From Crowdsourced Social Media Data*. Electronic Frontier Foundation, 2016, pp. 17–20, *Censorship In Context: Insights From Crowdsourced Social Media Data*.

[56] "Manila Principles on Intermediary Liability." *Manila Principles | Manila Principles*, www.manilaprinciples.org/.

[57] Owen, Tess, and Carter Sherman. "Kicking Gab off the Internet Won't Kill Online Extremism. It May Make It Worse." *VICE News*, VICE News, 31 Oct. 2018, news.vice.com/en_us/article/3kmxdv/kicking-gab-off-the-internet-wont-kill-online-extremism-it-may-make-it-worse.

[58] Antonio Casilli, Paola Tubaro. Social Media Censorship in Times of Political Unrest - A Social Simulation Experiment with the UK Riots. Bulletin de Méthodologie Sociologique / Bulletin of Sociological Methodology, SAGE Publications, 2012, 115 (1), pp.5-20.

[59] Eshwar Chandrasekharan, Umashanthi Pavalanathan, Anirudh Srinivasan, Adam Glynn, Jacob Eisenstein, and Eric Gilbert. 2017. You Can't Stay Here: The Efficacy of Reddit's 2015 Ban Examined Through Hate Speech. Proc. ACM Hum.-Comput. Interact. 1, 2, Article 31 (November 2017), 22 pages. https://doi.org/10.1145/3134666

Bibliography

Anderson, Jessica, et al. *Censorship In Context: Insights From Crowdsourced Social Media Data*. Electronic Frontier Foundation, 2016.

Anglin, Andrew. "Mystery on Fat Mountain: Heather Heyer's Autopsy Nowhere to Be Seen – Did She Have a Heart Attack?" *The Daily Stormer*, The Daily Stormer, 31 Aug. 2017, dailystormer.name/mystery-on-fat-mountain-heather-heyers-autopsy-nowhere-to-be-seen-did-she-have-a-heart-attack/.

Antonio Casilli, Paola Tubaro. Social Media Censorship in Times of Political Unrest - A Social Simulation Experiment with the UK Riots. Bulletin de Méthodologie Sociologique / Bulletin of Sociological Methodology, SAGE Publications, 2012, 115 (1), pp.5-20.

Cohn, Cindy L. "Bad Facts Make Bad Law: How Platform Censorship Has Failed So Far And How To Ensure that the Response to Neo-Nazis Doesn't Make It Worse." 2 GEO. L. TECH. Rev. 432 (2018). https://georgetownlawtechreview.org/bad-facts-make-bad-law-how-platform-censorship-has-failed-so-far-and-how-to-ensure-that-the-response-to-neo-nazis-doesnt-make-it-worse/GLTR-07-2018/

"Content Delivery Networks (CDNs)." *Electronic Frontier Foundation*, 18 Aug. 2017, www.eff.org/free-speech-weak-link/cdn.

Darwin, E.V., et al. "The Best Domain Registrars - the Good, the Bad and the Ugly - 2018 Guide." *Make A Website Hub*, Make a Website Hub, 23 Nov. 2018, makeawebsitehub.com/reviews/domain-registrars/.

Dewey, Caitlin. "Facebook Is Embroiled in Yet Another Breastfeeding Photo Controversy." *The Washington Post*, WP Company, 26 Feb. 2015, www.washingtonpost.com/news/the-intersect/wp/2015/02/26/facebook-is-embroiled-in-yet-another-breastfeeding-photo-controversy/?noredirect=on&utm_term=.5b0adb6e5997.

"Diamond Conglomerate Attempts to Silence Critical Parody." *Electronic Frontier Foundation*, Electronic Frontier Foundation, 18 Nov. 2011, www.eff.org/takedowns/diamond-conglomerate-attempts-silence-critical-parody.

Doren, Peter Van, and Thomas A. Firey. "Understanding 'Net Neutrality'." *Cato.org*, Cato Institute, 14 Dec. 2017, www.cato.org/publications/commentary/understanding-net-neutrality.

"DreamHost's Guide to the DMCA - DreamHost.blog." *DreamHost*, DreamHost, 28 Aug. 2018, www.dreamhost.com/blog/dmca-guide/.

Eshwar Chandrasekharan, Umashanthi Pavalanathan, Anirudh Srinivasan, Adam Glynn, Jacob Eisenstein, and Eric Gilbert. 2017. You Can't Stay Here: The Efficacy of Reddit's

2015 Ban Examined Through Hate Speech. Proc. ACM Hum.-Comput. Interact. 1, 2, Article 31 (November 2017), 22 pages. https://doi.org/10.1145/3134666

"Famous DDoS Attacks." *Cloudflare*, www.cloudflare.com/learning/ddos/famous-ddos-attacks/.

Farivar, Cyrus. "Web Hosting, CDN Companies Torn as to How to Respond to Racist Websites." *Ars Technica*, Ars Technica, 17 Aug. 2017, arstechnica.com/tech-policy/2017/08/squarespace-set-to-kick-out-white-nationalist-websites/.

Gewirtz, David. "Best Web Hosting Providers: InMotion, Hostgator, Bluehost and More."

CNET, CNET, 14 May 2018, www.cnet.com/web-hosting/.

Gillespie, Tarleton. "Platforms Are Not Intermediaries." 2 Geo. L. Tech. Rev. 198 (2018)

Guynn, Jessica. "Twitter Boots The Daily Stormer in Latest Eviction for Neo-Nazi Site." *USA Today*, Gannett Satellite Information Network, 16 Aug. 2017, www.usatoday.com/story/tech/news/2017/08/16/twitter-boots-daily-stormer-latest-eviction-neo-nazi-site/573428001/.

Hankes, Keegan. "Cloudflare Optimizing Content Delivery For At Least 48 Hate Sites Across Europe." *Southern Poverty Law Center*, Southern Poverty Law Center, 7 Mar. 2017, www.splcenter.org/hatewatch/2017/03/07/cloudflare-optimizing-content-delivery-least-48-hate-sites-across-europe.

Hatmaker, Taylor. "Google Drops Domain Hosting for Infamous Neo-Nazi Site the Daily Stormer." *TechCrunch*, TechCrunch, 14 Aug. 2017, techcrunch.com/2017/08/14/google-daily-stormer-domain/.

"How the Web Works." *MDN Web Docs*, Mozilla, developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works.

"How Tech Supports Hate." *Southern Poverty Law Center*, www.splcenter.org/hate-and-tech.

"ISP Censorship." *Extremism and Censorship*, Stanford Computer Science, 1999, cs.stanford.edu/people/eroberts/cs181/projects/1998-99/nuremberg-files/censorship.html.

Johnson, Steven. "Inside Cloudflare's Decision to Let an Extremist Stronghold Burn." *Wired*, Conde Nast, 15 Feb. 2018, www.wired.com/story/free-speech-issue-cloudflare/.

Keller, Daphne. "Toward a Clearer Conversation About Platform Liability." *Knight First Amendment Institute*, Knight First Amendment Institute at Columbia University, 2018, knightcolumbia.org/content/toward-clearer-conversation-about-platform-liability.

Kloepfer, Daniel, et al. “What Are Certificate Authorities?” *GlobalSign*, GlobalSign, www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies/.

Koebler, Jason, and Joseph Cox. “Here's How Facebook Is Trying to Moderate Its Two Billion Users.” *Motherboard*, VICE, 23 Aug. 2018, motherboard.vice.com/en_us/article/xwk9zd/how-facebook-content-moderation-works.

Krebs, Brian. “DDoS-for-Hire Service Webstresser Dismantled.” *Krebs on Security*, Krebs on Security, 25 Apr. 2018, krebsonsecurity.com/2018/04/ddos-for-hire-service-webstresser-dismantled/.

Krebs, Brian. “Who Is Anna-Senpai, the Mirai Worm? .” *Krebs on Security*, Krebs on Security, 17 Jan. 2018, krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/.

Kuerbis, B., Mehta, I., & Mueller, M. (2017). In Search of Amoral Registrars: Content Regulation and Domain Name Policy. Atlanta, GA: Internet Governance Project, Georgia Institute of Technology. https://www.internetgovernance.org/wp-content/uploads/AmoralReg-PAPER-final.pdf

Lieu, Johnny. “'Free Speech' Social Platform Gab Goes Offline after Fatal Pittsburgh Shooting.” *Mashable*, Mashable, 29 Oct. 2018, mashable.com/article/gab-goes-offline-hosting/#jwkQ1aHvGOqf.

Matsakis, Louise. “Following GoDaddy, the Daily Stormer's Email Provider Drops It as a Customer.” *Motherboard*, VICE, 14 Aug. 2017, motherboard.vice.com/en_us/article/7xxvng/following-godaddy-the-daily-stormers-email-provider-drops-it-as-a-customer.

Newman, Lily Hay. “How Creative DDOS Attacks Still Slip Past Defenses.” *Wired*, Conde Nast, 12 Mar. 2018, www.wired.com/story/creative-ddos-attacks-still-slip-past-defenses/.

"Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston, Inc." *Oyez,* 16 Dec. 2018, www.oyez.org/cases/1994/94-749

Hwang, Tim, Dealing with Disinformation: Evaluating the Case for CDA 230 Amendment (December 17, 2017). Available at SSRN: https://ssrn.com/abstract=3089442 or http://dx.doi.org/10.2139/ssrn.3089442

“Manila Principles on Intermediary Liability.” *Manila Principles | Manila Principles*, www.manilaprinciples.org/.

Monster, Rob. “Why Epik Welcomed Gab.com.” *Epik Blog*, Epik, 3 Nov. 2018, epik.com/blog/why-epik-welcomed-gab-com.html.

Oluo, Ijeoma. "Facebook's Complicity in the Silencing of Black Women." *Medium.com*, Medium, 2 Aug. 2017, medium.com/@IjeomaOluo/facebooks-complicity-in-the-silencing-of-black-women-e60c34434181.

Owen, Tess, and Carter Sherman. "Kicking Gab off the Internet Won't Kill Online Extremism. It May Make It Worse." *VICE News*, VICE News, 31 Oct. 2018, news.vice.com/en_us/article/3kmxdv/kicking-gab-off-the-internet-wont-kill-online-extremism-it-may-make-it-worse.

Prince, Matthew. "Why We Terminated Daily Stormer." *The Cloudflare Blog*, The Cloudflare Blog, 29 Aug. 2018, blog.cloudflare.com/why-we-terminated-daily-stormer/.

Segan, Sascha. "Exclusive: Check Out the Terrible State of US ISP Competition." *PCMAG*, PCMAG.COM, 15 Dec. 2017, www.pcmag.com/news/357972/exclusive-data-shows-the-terrible-state-of-us-isp-competition.

Siskind, Amy. ".@GoDaddy You Host The Daily Stormer - They Posted This on Their Site. Please Retweet If You Think This Hate Should Be Taken down & Banned. Pic.twitter.com/FqTtGoTbmn." *Twitter*, Twitter, 14 Aug. 2017, twitter.com/amy_siskind/status/896908664900009984.

Sopan, Deb, and Peters W. Jeremy. "New Yorker Festival Pulls Steve Bannon as Headliner Following High-Profile Dropouts." *The New York Times*, The New York Times, 3 Sept. 2018, www.nytimes.com/2018/09/03/arts/bannon-new-yorker-festival-remnick.html.

"Spocko and ABC/KSFO." *Electronic Frontier Foundation*, Electronic Frontier Foundation, 5 Oct. 2011, www.eff.org/cases/spocko-and-abc-ksfo.

Stephens, Bret. "The Outrage Over Sarah Jeong." *The New York Times*, The New York Times, 9 Aug. 2018, www.nytimes.com/2018/08/09/opinion/sarah-jeong-tweets-opinion-section.html.

"The Top 5 Most Popular SSL Certificate Authorities Reviewed." *WPMU Dev*, Incsub, premium.wpmudev.org/blog/ssl-certificate-authorities-reviewed/.

"Web Hosting." *HostGator Blog*, HostGator, www.hostgator.com/tos.

"What Is a CDN? How Does a CDN Work?" *Cloudflare*, Cloudflare, www.cloudflare.com/learning/cdn/what-is-a-cdn/.

"What Is a Distributed Denial-of-Service (DDoS) Attack?" *Cloudflare*, www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

"What Is a DNS Resolver? - Definition from Techopedia." *Techopedia.com*, Techopedia Inc. , www.techopedia.com/definition/9176/dns-resolver.

"What Is Web Hosting? ." *Website.com Website Builder*, www.website.com/beginnerguide/webhosting/6/1/what-is-web-hosting?.ws.

Wu, Tim, Network Neutrality, Broadband Discrimination. Journal of Telecommunications and High Technology Law, Vol. 2, p. 141, 2003. Available at SSRN: https://ssrn.com/abstract=388863 or http://dx.doi.org/10.2139/ssrn.388863