7-2021

Widening the Lens on Content Moderation

Jenna Ruddock

Justin Sherman

AMERICAN UNIVERSITY
WASHINGTON COLLEGE OF LAW

TECH, LAW & SECURITY PROGRAM

Widening the Lens on Content Moderation

Mapping the Ecosystem of Online Content Dissemination

July 2021

AUTHORS:
Jenna Ruddock, Senior Researcher
Justin Sherman, Research Fellow

PROJECT DIRECTOR:
Gary Corn

Tech, Law & Security Program
American University Washington College of Law

Executive Summary

The Internet has enabled global communication and collaboration on an unprecedented scale. It has also become an incredibly effective means for distributing harmful content, engaging in harmful behaviors, and coordinating harmful acts. Some of these online harms exacerbate preexisting offline harms—like the distribution of child sexual abuse material—while others are relatively unique to the internet, like the ability to launch mass anonymous harassment campaigns, which disproportionately target women and people of color.[1]

In the United States, targeted online disinformation campaigns during recent election cycles have super-charged calls for a comprehensive approach to addressing harms online.[2] The focus of these conversations has largely fallen on the small group of companies operating the most-visible content distribution platforms, namely Facebook, Twitter, and Google (primarily in its role as YouTube's parent company).[3] But Facebook is not the internet, and focusing almost exclusively on the companies behind these high-profile social media platforms means that the majority of the internet is often left out of the conversation about how to effectively combat harmful content online while also protecting fundamental rights and civil liberties.

This report engages in that larger conversation by discussing the full internet ecosystem's role in generating, curating, and disseminating online content. We begin by introducing several case studies that illustrate the ways in which companies *throughout* the internet have taken action to deny services to specific actors or stem the tide of particular content, with varying degrees of success. We then propose a mapping of what we call the **online information ecosystem**: the full range of functions and services collectively enabling users to disseminate and consume content online. Finally, using this mapping as a framework, we examine the primary technical and contractual mechanisms available throughout the ecosystem to moderate online content.

Importantly, the goal of this paper is descriptive, not prescriptive. In order to have a nuanced and robust conversation about the roles, responsibilities, and decision-making of actors throughout the internet ecosystem in addressing harmful content online, it is necessary to first reach a common understanding about what is possible. This report is intended to provide a diverse range of audiences with a working understanding of the online information ecosystem's collective role in the generation and dissemination of content online.

Acknowledgments: *The authors would like to first and foremost thank Jennifer Daskal, without whom this project never would have been possible—during her time as faculty director of the Tech, Law & Security Program, she not only conceptualized this project but was the driving force behind it—as well as TLS*

program director Gary Corn, whose support, insight, and guidance has been essential to its continuation. The authors would also like to thank the many individuals, who shall remain anonymous, who participated in multiple private roundtables on this issue set. Finally, the authors would like to thank Gary Corn, Corin Stone, Paul Rosenzweig, Bill Woodcock, Laura Draper, and Blake Reid for their comments on an earlier draft of this paper. Any errors are solely attributable to the authors.

Contents

Introduction

On January 6, 2021, the United States witnessed an unprecedented attack on the U.S. Capitol building during a joint session of Congress, resulting in several deaths.[4] Parler—a social media platform where scores of participants in the Capitol riot had connected, organized, and posted live video footage of the attack—soon became the subject of intense public scrutiny.[5] Within the following forty-eight hours, Google Play and the Apple App Store had both announced that they would be suspending downloads of the Parler mobile application.[6] One day later, Amazon Web Services similarly confirmed that it would stop providing cloud hosting to Parler, temporarily forcing the platform's operational back-end offline.[7]

This was not the first—nor will it be the last—time that internet companies beyond the major social media platforms have taken voluntary action to limit the accessibility of specific content online. In October 2020, a website hosting service stopped providing services to the all-male, self-styled "Western chauvinists" known as Proud Boys, following pressure from Google.[8] Just one year earlier, on August 3, 2019, a user posted "a manifesto decrying a 'Hispanic invasion of Texas'" on 8chan, a website and messaging service widely known as a place where white extremists congregate online.[9] Hours later, a gunman presumed to be the author of the manifesto[10] opened fire in a crowded shopping mall in El Paso, killing 22 unarmed men, women, and children, and injuring another 24.[11] 8chan had already been tied to other hate-motivated killings, including the March 2019 Christchurch massacre targeting two New Zealand mosques and the fatal San Diego synagogue attack that same spring.[12] Still, it wasn't until the aftermath of the El Paso shooting that Cloudflare, a company that sells content delivery services, terminated its services to 8chan.[13] Four years prior, Cloudflare—along with content hosting company Digital Ocean, Google, and GoDaddy, one of the web's largest domain name registrars—had also stopped providing services to the Daily Stormer, one of the then-most popular neo-Nazi websites on the internet, following intense public pressure.[14] Like 8chan, the Daily Stormer struggled to find and retain new online service providers, bouncing between the dark and clear web—described by journalist Talia Lavin as "wander[ing] the digital wilderness."[15] In 2010, a similar series of termination decisions by web hosting providers and payment processors temporarily forced WikiLeaks offline in the wake of U.S. government pressure over WikiLeaks' publication of classified documents, courtesy of U.S. Army Specialist Chelsea Manning.[16]

These actions highlight the under-discussed roles that companies across the internet ecosystem play in delivering content to users and, by extension, their ability to moderate that process. While debates rage about the roles and responsibilities of the major social media platforms in addressing the distribution of harmful content online, there is far less attention paid to the roles

and responsibilities of other companies across the internet ecosystem that are also essential to the generation and distribution of online content.[17]

We seek to widen the lens beyond the content dissemination functions that have thus far dominated these discussions. Who is responsible for addressing concerns arising from the vast universe of content that exists online beyond the social media platforms—the proverbial last mile of the content distribution ecosystem? What happens when social media companies fail to respond to—or themselves explicitly promulgate—violence, fraud, and a range of other harms? At what point is it the responsibility of the numerous other companies that comprise the online information ecosystem to take action? Using what methods? According to what substantive and procedural standards? And what are the potential collateral costs—to freedom of speech, to security, and to privacy—of doing so?

This report is part one of a larger project seeking to answer these questions—issues that are critical to the ongoing efforts to respond to an array of harms being perpetuated online. What types of content and harms merit a response is, of course, a source of constant debate.[18] For the purposes of this particular paper, we are leaving that debate to the side. Our focus here is on describing the mechanisms used by companies across the online information ecosystem to address whatever falls into the bucket of agreed-upon, need-to-be addressed harms.

Examining the full range of companies that comprise the internet's content generation, storage, and delivery ecosystem—and the various ways they engage with and manage that content—is necessary to ensure truly robust public debate on a diverse set of urgent issues. As noted above, this report is intended to provide a range of audiences with a working understanding of the online information ecosystem's collective role in the generation and dissemination of content online. By necessity, we do not capture every nuance of internet architecture here, though we have done our best to not sacrifice accuracy for accessibility. We also hope our endnotes highlight ample additional resources.

Moderation Beyond Platforms: 8chan

From 2013 to 2019, 8chan gained popularity as an online gathering place for white supremacists, conspiracy theorists, and self-styled trolls.[19] While 8chan's terms of use nominally restricted posting, requesting, or linking to "any content that is illegal in the United States of America," violent and extremist content went largely unmoderated.[20] Like most websites, 8chan relies upon a web of online service providers to remain accessible to users.

In March 2019, a mass shooting at two mosques in Christchurch, New Zealand, was livestreamed on Facebook.[21] Facebook did not remove the livestream until after it had ended, at which point the footage at already made the jump over to independently hosted platforms, including 8chan.[22] In response, major **Internet Service Providers (ISPs)** in New Zealand and Australia took the dramatic step of blocking country-wide access to 8chan, as well as to several other sites that were hosting the footage.[23]

In August 2019, yet another mass shooter took to 8chan[24] – this time posting a racist manifesto before opening fire in a Walmart in El Paso, Texas, killing 22 people.[25] The next day, **content distribution network** provider Cloudflare ceased providing services to 8chan.[26] The site temporarily found a new CDN provider, until that service provider's parent company pulled its support as well.[27] Tucows, the world's second-largest **domain registrar**, also cut ties with 8chan, disrupting traffic to the 8chan.com domain.[28] 8chan ultimately survived, rebranding as 8kun.top, though the reach of its content and its accessibility to potential new users have been severely restricted by mainstream service providers' refusal to associate with the site.[29]

The lifecycle of 8chan illustrates not only the potential impact that companies throughout the internet ecosystem can have on the accessibility of harmful content—it also highlights the overwhelmingly ad-hoc and reactionary bases upon which these decisions have largely been made. While ISPs took action against 8chan in New Zealand and Australia, those same companies took no action against much larger platforms like Facebook, where hundreds of thousands of duplicate or slightly-altered versions of the footage were uploaded in the hours following the attack.[30] ISPs cited the large platforms' ongoing removal efforts as justification, yet blocked several smaller websites found to be hosting the footage that were *also* actively working to remove the content.[31] And although Cloudflare and Tucows ultimately also took action against 8chan, both companies expressed extreme reluctance both before and after doing so, with Cloudflare in particular citing the lack of clear independent standards to guide their decision-making as a cause for concern.[32]

Moderation Beyond Platforms: Covid-19

False information about coronavirus treatments has been a persistent problem during the Covid-19 pandemic. Authoritarian governments have used the pandemic as a reason—in many cases illegitimately—to crack down on the spread of "false information" within their borders.[33] Another key issue has been the spread of false coronavirus treatment information through traditional media, such as then-U.S. President Donald Trump's dangerous suggestion in an April 2020 press briefing that individuals inject disinfectants to treat the virus.[34] Yet the spread of false information about Covid-19 treatments online has been a persistent problem far beyond traditional media and high-profile social media platforms, and companies across the online information ecosystem have taken action to limit its dissemination—including within the Domain Name System (DNS).

In April 2020, the United Kingdom's **domain name registry** Nominet (the official registry for .uk domain names) began screening coronavirus-related websites by default when they were registered with the company; only once the website was deemed legitimate would the domain name be usable. Nominet said in April 2020 that this had already led to the suspension of over 600 coronavirus-related domain names under its umbrella. "We don't want to prevent legitimate registration from getting through, but I think the current situation warrants further checks at the point of registration," Nominet's managing director of registry services told *ZDNet*.[35]

Also in April 2020, the U.S. Department of Justice (DOJ) announced a disruption of hundreds of online scams related to the coronavirus "without requiring legal processes."[36] The DOJ said it worked directly with **domain registries and registrars**, passing along complaints about domains that hosted false information or were even selling fake vaccines and fake cures. It also passed along the names of domains that were hosting malware or that operated fraudulent charities purporting to help address the coronavirus. Many of these domain registries and registrars, the DOJ said, then reviewed the domains, found them to be in violation of their policies, and took down the domains voluntarily.[37] The DOJ itself received these leads from industry and was also using new industry tools to detect new domains that hosted false Covid-19 information and other scams.[38] It did not specify how the takedowns were technically carried out, and it did not name any specific domain registrars or registries involved.[39] Quad9, a public recursive DNS resolver, independently monitored malicious Covid-specific domain sets and blocked access attempts.

Companies across the DNS have a variety of levers at their disposal to limit access to online content, described in greater detail below. These actions taken to limit the spread of Covid-19 false information help illustrate how these levers

can be deployed relatively selectively, or relatively broadly, to limit the accessibility of online content and services to internet users globally.[40]

Mapping the Ecosystem: How Content Moves Online

When using the internet in our daily lives, we rarely think about all of the steps that it takes for content to travel from another device to our own screens, and all of the parties involved in making that exchange of information possible. When we post on Facebook, for example, the only obvious parties to that transaction are our own devices (and by extension, the companies that produce them), the company providing our internet connection, and Facebook itself. But even sharing such a simple piece of content online requires a number of other critical actors whose role in the distribution of content throughout the internet ecosystem is oftentimes overlooked. Without these many parties—and in the age of a privatized internet, these organizations are in large part private companies—the poster would never make it online, the post would not get to the right place, and it certainly would not be accessible to others, whether half a mile away or halfway around the world.

Echoing but diverging slightly from traditional, more abstracted models of the internet protocol "stack",[41] the mapping we propose is intended to provide a framework for discussing how content is distributed throughout the internet ecosystem by identifiably involved actors. As with any modeling exercise, this mapping seeks to provide workable categories, thus eliding the full set of complexities. It is not, as a result, exhaustive. It also is not the only way to categorize or describe the practical functions carried out,[42] and it is critical to note that:

- certain functions often overlap;
- certain companies fall into multiple service provider categories; and,
- increasingly, related functions are often bundled together and presented as a single service.

What this mapping offers is a model that sheds light on the broad spectrum of functional roles played by companies throughout the online information ecosystem, all of which, to varying degrees, enable users to share or access content on their devices:

> ***Accessing:*** This is the part of the online information ecosystem that connects devices (like computers and phones) to the online world, via a combination of wires, cables, servers, routers, and more. **Internet service providers** (ISPs) like AT&T, Comcast, Verizon, and Vodaphone all operate in this space. It also includes **Virtual Private Networks** (VPNs) like Tor, which enable users to access the internet in ways that mask location and are thus often utilized to evade local content

controls.

Delivering: This part of the ecosystem routes internet traffic from users to sought-after content (such as websites, streaming videos, and apps) and back again. It includes the **registries, registrars**, and **Domain Name System operators** that effectively create and operate a phone book for the internet, the range of **content delivery networks** like Cloudflare and Akamai that allow content publishers to scale to meet user demand, and an array of other private and quasi-governmental actors that help deliver traffic along routes from point A to point B.

Hosting and securing: Hosting services provide a place for content to sit and business logic to be executed. This includes **cloud providers** like Microsoft, Google, and Amazon and **website hosting platforms** like Bluehost. **DDoS mitigation services** protect hosting services, and the servers that such hosting services use, by filtering attacks on the system. Cloudflare, Verisign, and Amazon (AWS Shield) are among the companies providing these services. Increasingly, hosting and DDoS mitigation services are offered by the same providers, though key companies operating in this part of the ecosystem, such as Cloudflare, do not offer web hosting services.[43]

Browsing: **Web browsers**, like Google Chrome, Safari, and Firefox, provide the digital gateway to accessing public-facing content on the public internet as well as on the "dark web."

Content-curating: Content curation is the user-interfacing part of the ecosystem that has as its core the aggregation and curation of content online. We use the term "curation" here broadly to include both algorithmic and human curation that ranks, sorts, prioritizes, suggests, or otherwise filters content. This comes in a variety of forms, including platforms, search engines, app stores, and a range of other entities that enable or support user-generated content.

> ***Platforms*** — **Social platforms** including Facebook, Twitter, YouTube, Instagram, Reddit, and TikTok and **online marketplaces** like Amazon, Airbnb, and Alibaba both directly curate content and also enable user curation.
>
> ***Search*** — **Search engines** are a unique and critically distinct part of the online ecosystem, influencing the ways in which their users encounter content by algorithmically curating search results for specific queries.

App stores – **App stores**, like the Apple iOS App Store and the Google Play Store, serve as both gateways to communities of internet users as well as content-curators in their own right. In addition to operating as file-hosting services that store mobile application software files, which users download onto their devices to then access content hosted elsewhere, app stores create both technical and content-oriented rules that govern how applications are posted to, maintained through, and removed from their platforms.

Financially Facilitating: These are the plugins and services that enable the processing of payments, an essential component of e-commerce and other fee-for-service interactions online. Well-known examples include Alipay, M-Pesa, PayPal, Amazon Pay, Stripe, Square, Visa, and MasterCard.

How these various subcomponents of the online information ecosystem interact at any given time to produce and disseminate content is not static, and importantly, these categories are not discrete. Single companies often act in a variety of functional roles and thus have potential control over a variety of these functions. Google, for example, operates across each of these areas. It builds fiber-optic internet cables (access role); operates a registry, a registrar, and a recursive resolver (delivery role); provides scaled cloud services (hosting and securing role); runs a digital wallet and online payment system (financially facilitating role); offers an internet browser (browsing role); manages an app store (app store role); and runs the dominant search engine across the United States and Europe (content-curating role); all in addition to its core business functions of advertising and data monetization.

A Deeper Dive: Levers of Control

Building on the basic mapping and case studies introduced above, the following section explores in greater detail the functionality provided by each part of the ecosystem, the corresponding mechanisms of content mediation available, and further illustration of how these levers can be—and have been—utilized.

Accessing

The precursor to communicating online is **accessing** the internet. This requires access to both the infrastructure layer—the actual cables, cellular system, routers, switches, and other hardware via which the 0s and 1s that make up our digital communications travel—and the logical layer—meaning the internet protocols that computers use to route information in the digital world.[44] As a practical matter, this access is generally provided by Internet Service Providers (or "ISPs"). ISPs connect individual users to the internet, enabling them to access and share content.[45]

Just as ISPs can provide access, they can also turn off access—something that typically happens in response to government mandates,[46] though ISPs can act independently as well, as they did in the 8chan case.[47] These actions can be regional, or platform- and service-specific.[48] ISPs can cut access to services altogether, cut access to services for a particular geographic area, or block particular content through techniques like deep packet inspection (a form of opening up traffic and filtering for certain key words or images) or blocking ranges of IP addresses. These firms can also take steps to "throttle" access to content, or slow down its speed of transmission, which raises the costs (temporally, sometimes also financially) for users to access internet content. Virtual private networks (VPNs) can provide an alternative way for users to connect—enabling users to mask their location and access internet content blocked by local content controls imposed on their local ISPs through laws and regulations, particularly intellectual property regimes. However, VPN companies can themselves make decisions about what kinds of traffic to allow or disallow through their encrypted connections—even if most allow users to access whatever content they choose—and they can also be regulated by governments to prevent access to certain kinds of content.

Browsing

Once users are connected to the internet on a technical level—with the requisite hardware installed, and electronic signals flowing—users need to navigate the internet in words and languages that they understand. Browsers are software applications, installed on a user's device, that enable users to initiate the process of requesting and retrieving web content by typing a user-friendly domain name (URL) into an address field—for example, www.american.edu. Certain devices might have specific browsers pre-installed (e.g., Safari on Apple devices), but users are generally able to install and use a variety of browsers to navigate to content.

Though often overlooked, browsers can and do determine what information is made available to users online. Browsers can block access to particular webpages or websites, both for technical reasons (such as the destination site not having HTTPS enabled) as well as content-oriented ones. They can redirect users to different websites, and they can also issue interstitial notices that appear before access is granted. For example, when a user on Google Chrome attempts to visit a site known to host malware, a warning is typically delivered while the browser intercepts and stops the webpage from loading.[49] These kinds of interstitial notices can operate as warning signals that users have to click through; they can require entry and certification of particular information, such as self-verification of age or parental approval; or they can block access to the website altogether.

Delivering

For online traffic to get routed from one point to another, it needs to have a digital address and a means of finding that address—a function the Domain Name System

(DNS) performs. This is a multi-step process: First, the plain language web address (e.g., facebook.com, worldwildlife.org, or whitehouse.gov) is translated into a unique digital address (known as an IP address) by a recursive DNS nameserver, which retrieves the relevant information and then sends it back to the initial requester.[50] Notably, the **DNS nameservers** do not create or maintain this digital directory—they merely serve as publishers, distributing it to the public. A range of private- and public-sector actors perform the role of creating and maintaining the directory. **Registry** operators like Verisign (.COM and .NET), Nominet (UK), and Afnic (France) maintain the top-level domains—the last part of the website address. **Registrars** like GoDaddy, Squarespace, Bluehost, and Google Domains sell subsidiary domain names—what goes to the left of the .com, .org, or .edu.[51] There are also country-specific top level domain names, called "ccTLDs," such as .cn for Chinese websites, .de for German websites, and .ir for Iranian websites.

The DNS is fertile ground for controlling what is and is not accessible online.[52] As discussed above, Tucows, one of the world's biggest domain registrars, suspended its agreement with the parent company of 8chan in the wake of the 2019 El Paso shooting.[53] Without a registrar servicing a domain (in that case, 8chan.com), content retrieval requests from users go unanswered, making the website inaccessible. Similarly, GoDaddy and then Google stopped servicing the domain for the Daily Stormer in the wake of its support for and disturbing commentary on the 2017 Charlottesville Unite the Right rally and terrorist attack.[54] This past year, in an effort to combat harmful content relating to the Covid-19 pandemic, a stakeholder group representing major registrars around the world published a guide for "Registrar approaches to the Covid-19 Crisis."[55]

Content delivery network (CDN) services also play a critical role in scaling the **delivery** of websites and other content to users. Generally speaking, CDNs consist of a geographically distributed set of servers that accelerate the delivery of internet content by holding cached content of a website (content stored locally so that new requests can be filled faster). This protects against long delays in accessing requested content; regionally staged CDNs can respond to local requests with relative speed.

CDNs can be a source of control independent of the security services that CDNs also provide (described below). Before the Chinese government banned Google from operating in China, the government blocked the Google cache.[56] In 2020, Vietnam's state-owned telecommunications companies forced Facebook's local Vietnamese cache servers offline for a period of seven weeks.[57] The connection was so slow as to make Facebook effectively unavailable to many users. It was only after Facebook negotiated with the government and agreed to a range of content take-down requests that the domestic cache servers were allowed back online.[58]

Hosting and securing

Content needs a home, because otherwise there will be nothing to route and deliver upon request. This is where **hosting** services come in. Web hosting is enabled by servers, or computers running programs designed to listen for and process incoming internet requests.[59] The most familiar website hosting is public. Subscribers pay for website hosting via companies like DigitalOcean or one of the many cloud providers like Amazon Web Services, Google Cloud, or Microsoft Azure that publish websites publicly for any internet user to access (though full access may then be conditioned on subscriptions, membership, etc.).[60]

While not a distinct part of the technical architecture, **DDoS mitigation** services play a key functional role in this part of the ecosystem by supporting hosting and delivery functions. They ensure availability in the face of distributed denial of service (DDoS) attacks on target servers, thereby ensuring the continued operation of websites, messaging services, and digitally connected devices, among other parts of the internet.[61] Related service providers—like web hosts or CDNs—often bundle DDoS mitigation services with their core services.

Content controls in this part of the internet ecosystem can take several forms. Website hosts can block requesting IP addresses (or support plugins that do the same). Hosts can also modify the content displayed to users depending on their geographic location. For instance, a user could go to a federal website to learn about a policy and then have the same website load state-specific information, tied to the user's location, as determined by the user's IP address. Similarly, the host of a streaming website, such as Amazon Web Services (which hosts Netflix), can ensure that only regionally licensed videos are available, or otherwise geographically segmented services are provided.[62]

DDoS mitigation services are equally critical to determining what is and is not available online. The same fundamental infrastructure that enables content to be hosted, routed, and delivered to users in response to legitimate requests for access is vulnerable to exploitation by malicious actors looking to deny users access to content. This is what DDoS attacks do—flood a target device with traffic in order to overwhelm that device and render it inaccessible by other users. Protections against such attacks, therefore, also enable content availability on the internet. 8chan, for example, was forced offline once Cloudflare stopped providing DDoS protections.[63] Absent DDoS mitigation services, website hosts and others are at risk of being flooded by attackers, or by normal use (the "slashdot effect"), ultimately rendering them inaccessible or forcing them to shut down.

Content-curating

At the edge of this ecosystem are the open web and—likely the most discussed and analyzed part of the ecosystem—the content curators. Content curators include

search engine operators like Google and Microsoft (Bing); **social platforms** like Facebook, Twitter, YouTube, Instagram, Reddit, and TikTok; **mobile app stores**, such as the Apple iOS App Store and Google's Play Store; and a range of other entities that support, rank, sort, and otherwise filter user-generated content. Some companies in this space—such as Airbnb, Alibaba, Uber, and ebay!—curate content to connect people in order to provide an offline service. Still others, such as online dating apps and Eventbrite, connect people to people. A range of content disseminators serve closed ecosystems of users; think, for example, of Dropbox. All of these actors are user-interfacing, in that they directly interact with users online, employing different models to aggregate or curate content for users to consume. They each play, as a result, a key role in determining what content is and is not available to users online.

The tools available within this part of the online ecosystem are diverse, though there are several key methods of moderation. **Platforms** that host user-generated content—for example, social media platforms or online newspaper comment sections—are typically able to target individual pieces of content for removal. These removals are largely informed by "community standards" or similar terms of service.

More discreetly, many content curators regulate the degree of visibility of content rather than removing it from a platform (or in the case of search engines, from the internet). Google's **search** algorithm, for example, exercises a significant amount of control over which websites and thus which information each user sees in response to a particular query.[64] Similarly, platforms like Facebook and YouTube use algorithmic curation to suggest content that users might not otherwise encounter.[65] Twitter's introduction of flags and filters for misinformation relating to U.S. election integrity and the Covid-19 pandemic previewed another set of tools that stop short of actually removing potentially harmful content.[66]

Mobile app stores, such as the Apple iOS App Store and Google's Play Store, play a unique role in the ecosystem due to the widespread use of mobile applications, the dominance of the two major app stores, and the fact that users' choice of app store is largely predetermined by their choice of mobile device. App stores serve as gateways to online communities of users (e.g., of iPhones or Android devices) that rely on those app store platforms to download approved applications to their devices. Once the software files are downloaded from an app store, users run the applications on their device to access content hosted (in most cases) by parties other than the app store (e.g., the TikTok app connects to servers for tiktok.com which are hosted on cloud services separate from Apple and Google).

App stores have levers of control over which applications are posted on their stores, how applications are maintained through their stores (e.g., content policies, security updates), and how applications are removed from their stores. These controls are both technical and content-oriented; for example, while Parler's return to Apple's App Store following its takedown in the wake of the January 6th attack on the Capitol

seems to be contingent upon stricter moderation of hate speech, Parler will not filter the same content for users accessing the platform by other means, such as browsers.[67]

Financially Facilitating

Underpinning many websites, mobile applications, and other key internet services are financial services plugins that enable **payment processing**. These payment plugins add features to websites and can be used across multiple different services. They either manage payments directly within a website or redirect purchasers to their respective third-party website (e.g., logging into PayPal in a second browser window in order to pay for something in the first). Apple, Alipay, PayPal, Amazon (Amazon Pay), Stripe, Square, Visa, and MasterCard all provide these payment services. They protect website owners from having to worry about the technical and regulatory difficulties of creating a secure online monetary transaction system.

Just as financial interactions are often required to access, publish or distribute information in hard copy, financial interactions online can govern access to information—as with subscription-based platforms—as well as facilitate or prevent content consumers from supporting content creators on- or offline. Payment processors can refuse—and at various times have refused—to support sellers that are deemed objectionable. In 2010, for example, WikiLeaks was effectively "starved" of 95% of its revenue after the U.S. government threatened reprisal against Julian Assange and his website and pressured both U.S. and U.K. payment processors, including Visa, MasterCard, and Moneybookers, to stop providing their services to WikiLeaks.[68] Similarly, copyright owners have long turned to payment processors to "choke the flow of money to 'pirate sites,'" eventually forcing the websites to shut down.[69] In 2015, an ambitious sheriff in Cook County, Illinois, sought to choke Backpage.com—an online classified ad forum that was widely known as a place to hire sex workers—by demanding that credit card companies refuse payment for ads on Backpage.[70] Sex workers are frequently targeted in this way, having their accounts suspended and funds frozen.[71]

Conclusion: A Wider Lens

From screen to screen, every piece of online content relies on the majority of the internet ecosystem mapped above—a diverse network of companies providing related, but distinct, functions that enable us to tweet, to blog, to comment on the news, to view others' content or to share our own. This same ecosystem also empowers harmful actors to launch harassment campaigns, spread disinformation, and exchange illegal and abusive material.

Each of the functions described above presents unique opportunities to regulate this content as it moves through the online information ecosystem. Companies exercising these various functions not only can but also, as illustrated, already *do* take action to target specific content. These actions are not cost free. They often involve attendant

risks of collateral and disproportionate impacts. The consequences of allowing—or even requiring—companies controlling core internet infrastructure (such as Internet Service Providers) to moderate certain online content are vastly different from allowing or requiring those on the edge of the ecosystem, such as content curators, to do the same.

However, due at least in part to the lack of widespread attention paid to the functional roles these companies play in disseminating content online, when these companies have acted there have been few guiding norms or standards to reference. Content, users, and even entire platforms have been denied services on a largely ad-hoc basis, presenting significant speech- and security-related concerns while simultaneously reducing the likelihood that these actions will have a meaningful long-term impact in terms of effectively disrupting the dissemination of harmful content online. Widening the lens of content moderation conversations to account for the full online information ecosystem allows us to engage in more nuanced, comprehensive, and thus hopefully more effective conversations about when, where, and how to most effectively address the dissemination of harmful content online given the potential collateral costs. We look forward to continuing these conversations in follow-on reports.

The Technology, Law & Security Program (TLS) is a new initiative at American University Washington College of Law that tackles the challenges and opportunities posed by emerging technology—offering innovative solutions, engaging our students, and training the leaders of tomorrow.

Endnotes

[1] Viktorya Vilk, *What to Do if You're the Target of Online Harassment,* Slate (June 3, 2020), https://slate.com/technology/2020/06/what-to-do-online-harassment.html (noting that "[p]eople of color and LGBTQ+ people are disproportionately targeted, and women are twice as likely as men to experience sexual harassment online.").
[2] Musadiq Bidar, *Lawmakers vow stricter regulations on social media platforms to combat misinformation*, CBS News (March 25, 2021), https://www.cbsnews.com/news/misinformation-extremism-hearing-google-facebook-twitter-watch-live-stream-today-2021-03-25.
[3] Gerrit De Vynck et al., *Big tech CEOs face lawmakers in House hearing on social media's role in extremism, misinformation*, Washington Post (March 25, 2021), https://www.msn.com/en-us/news/politics/big-tech-ceos-faced-congress-in-house-hearing-on-social-media-s-role-in-extremism-misinformation/ar-BB1eXHCY.
[4] Kimberly Dozier & Vera Bergengruen, *Incited by the President, Pro-Trump Rioters Violently Storm the Capitol,* TIME (Jan. 7, 2021), https://www.businessinsider.com/photos-show-the-aftermath-of-a-siege-on-capitol-building-2021-1?IR=T.
[5] Brian Fung, *Parler has now been booted by Amazon, Apple and Google,* CNN Business (Jan. 11, 2021), https://www.cnn.com/2021/01/09/tech/parler-suspended-apple-app-store/index.html.
[6] *Id.*
[7] *Id.* ("The decision, which went into force on Sunday at 11:59 p.m. Pacific time, will shut down Parler's website and app until it can find a new hosting provider."). Parler finally secured a new hosting provider, a Los Angeles-based company named SkySilk, though early reports indicated that users were having trouble connecting to and browsing the site. *See* Bobby Allyn & Rachel Treisman, *After Weeks Of Being Offline, Parler Finds A New Web Host,* NPR (Feb. 15, 2021), https://www.npr.org/2021/02/15/968116346/after-weeks-of-being-off-line-parler-finds-a-new-web-host.
[8] Catalin Cimpanu, *Proud Boys website kicked off web host, Google Cloud*, ZDNet (Oct. 10, 2020), https://www.zdnet.com/article/proud-boys-websites-kicked-off-google-cloud. Google did not provide services directly to the websites in question but provided services to a hosting provider that in turn provided services to the Proud Boys. Proud Boys was, however, able to find a new hosting provider within days. *Id*.
[9] Tim Elfrink, *"'A cesspool of hate': U.S. web firm drops 8chan after El Paso shooting*," The Washington Post (Aug. 5, 2019), https://www.washingtonpost.com/nation/2019/08/05/chan-dropped-cloudflare-el-paso-shooting-manifesto.
[10] Lois Beckett & Sam Levin, *El Paso shooting: 21-year-old suspect 'posted anti-immigrant manifesto',* The Guardian (Aug. 4, 2019), https://www.theguardian.com/us-news/2019/aug/03/el-paso-shooting-21-year-old-suspect-in-custody-as-officials-investigate-possible-hate.
[11] Chas Danner, *Everything We Know About the El Paso Walmart Massacre*, New York Mag. (Aug. 7, 2019), https://nymag.com/intelligencer/2019/08/everything-we-know-about-the-el-paso-walmart-shooting.html.
[12] Timothy McLaughlin, *The Weird, Dark History of 8chan*, WIRED (Aug. 6, 2019), https://www.wired.com/story/the-weird-dark-history-8chan; Damien Cave, *Man Pleads Guilty to New Zealand Mosque Massacre*, N.Y. Times, (Mar. 25, 2020), https://www.nytimes.com/2020/03/25/world/australia/new-zealand-mosque-shooting-guilty-plea.html; Jennifer Medina, Christopher Mele & Heather Murphy, *One Dead in Synagogue Shooting Near San Diego; Officials Call It Hate Crime*, N. Y. Times (Apr. 27, 2019), https://www.nytimes.com/2019/04/27/us/poway-synagogue-shooting.html.
[13] Matthew Prince, *Terminating Service for 8Chan*, Cloudflare (Aug. 4, 2019), https://blog.cloudflare.com/terminating-service-for-8chan; *see also* McLaughlin, *supra* note 11.
[14] Natasha Lomas, *Digital Ocean and Cloudflare ditch neo-Nazi client, The Daily Stormer,* TechCrunch (Aug. 16, 2017), https://techcrunch.com/2017/08/16/digital-ocean-and-cloudflare-ditch-neo-nazi-client-the-daily-stormer; *see also* Matthew Prince, *Why We Terminated Daily Stormer*, Cloudflare (Aug.

16, 2017), https://blog.cloudflare.com/why-we-terminated-daily-stormer; *see also* Taylor Hatmaker, *Google drops domain hosting for infamous neo-Nazi site the Daily Stormer*, TechCrunch (Aug. 14, 2017), https://techcrunch.com/2017/08/14/google-daily-stormer-domain.

[15] Talia Levin, *The Neo-Nazis of the Daily Stormer Wander the Digital Wilderness,* The New Yorker (Jan. 7, 2018), https://www.newyorker.com/tech/annals-of-technology/the-neo-nazis-of-the-daily-stormer-wander-the-digital-wilderness.

[16] Kevin Poulsen, *PayPal Freezes WikiLeaks Account*, WIRED (Dec. 4, 2010), https://www.wired.com/2010/12/paypal-wikileaks; Charles Arthur, *WikiLeaks under attack: the definitive timeline*, The Guardian (Jan. 8, 2010), https://www.theguardian.com/media/2010/dec/07/wikileaks-under-attack-definitive-timeline.

[17] Important exceptions include Suzanne van Geuns & Corinne Cath-Speth, *How hate speech reveals the invisible politics of internet infrastructure*, Brookings Tech Stream (2020), https://www.brookings.edu/techstream/how-hate-speech-reveals-the-invisible-politics-of-internet-infrastructure; Joan Donovan, *Navigating the Tech Stack: When, Where and How Should We Moderate Content?,* Centre for Int'l Gov. Innovation (2019), https://www.cigionline.org/articles/navigating-tech-stack-when-where-and-how-should-we-moderate-content; Jack M. Balkin, *Free Speech is a Triangle*, 118 Columbia L. Rev. 2011, 2015 (2018); Cindy Cohn, *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); Annemarie Bridy, *Notice and Takedown in the Domain Name System*, 74 Wash. & Lee L. Rev. 1345 (2016). For additional thoughtful discussions of the multiplicity of players and their effect on communications online, see LAURA DENARDIS, GLOBAL WAR FOR INTERNET GOVERNANCE 2 (Yale University Press 2014); Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 Harv. L. Rev. 2296, 2298 (2014).

[18] As Annemarie Bridy, referencing scholarship by Danielle Citron, writes: "clarity in definitions of terms like 'hate speech '[sic] and 'terrorist material' is critical to prevent censorship creep – the expansion of speech policies beyond their original goals. Definitional clarity has other benefits, too. These include notice to users about the kind of speech culture a platform is trying to foster and facilitation of consistent enforcement by the platform." Annemarie Bridy, *Remediating Social Media: A Layer-Conscious Approach*, 24 B.U. J. Sci. & Tech. L. 193, 220 (2018). *See also* Jack M. Balkin, *Old-School/New-School Speech Regulation*, 27 Harv. L. Rev. 2296 (2014); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech,* 131 Harv. L. Rev. 1598 (2018).

[19] McLaughlin, *supra* note 12*; see also* Morning Edition, *The Website Where Violent White Supremacists State Their Case,* NPR (Aug. 5, 2019), https://www.npr.org/2019/08/05/748166877/the-website-where-violent-white-supremacists-state-their-case.

[20] McLaughlin, *supra* note 12*; see also* Jim Salter, *8chan resurfaces, along with the Daily Stormer and another Nazi site,* Ars Technica (Aug. 7, 2019), https://arstechnica.com/tech-policy/2019/08/8chan-resurfaces-along-with-the-daily-stormer-and-a-nazi-site.

[21] *New Zealand mosque shooting: What is known about the suspect?*, BBC (Mar. 18, 2019), https://www.bbc.co.uk/news/world-asia-47579243.

[22] Jon Porter, *Facebook says the Christchurch attack live stream was viewed by fewer than 200 people,* The Verge (Mar. 19, 2019), https://www.theverge.com/2019/3/19/18272342/facebook-christchurch-terrorist-attack-views-report-takedown; Jon Brodkin, *4chan, 8chan blocked by Australian and NZ ISPs for hosting shooting video,* ArsTechnica (Mar. 20, 2019), https://arstechnica.com/tech-policy/2019/03/australian-and-nz-isps-blocked-dozens-of-sites-that-host-nz-shooting-video.

[23] *Id.*

[24] 8chan was also connected to the tragic Poway synagogue shooting in April 2019, during which a gunman opened fire in a synagogue on the last day of Passover, wounding three and killing Lori Gilbert-Kaye as she protected the congregation's rabbi. A racist and antisemitic manifesto purportedly authored by the shooter was posted to 8chan shortly before the attack. However, none of 8chan's online service providers took action following this shooting. *See* EJ Dickson, *After*

California Synagogue Shooting, 8Chan Is Back In the Spotlight, Rolling Stone (Apr. 29, 2019), *https*://www.rollingstone.com/culture/culture-features/poway-synagogue-shooting-8chan-white-supremacist-828647.
[25] Danner, *supra* note 11.
[26] Prince, *supra* note 13.
[27] C. Fisher, *The internet is racing to cut ties with 8chan after another deadly shooting,* Engadget (Aug. 5, 2019), https://www.engadget.com/2019-08-05-8chan-cloudflare-internet-services-pull-support.html.
[28] Isabel Togoh, *Tucows Drops 8chan Domain Registration After El Paso Shooting,* Forbes (Aug. 5 2019), https://www.forbes.com/sites/isabeltogoh/2019/08/05/tucows-drops-8chan-domain-registration-after-el-paso-shooting/?sh=72a39af0ffbf.
[29] Sarah E. Needleman & Parmy Olson, *8chan Faces Roadblock in Efforts to Return to Service,* Wall St. J. (Aug. 5, 2019), https://www.wsj.com/articles/fringe-message-forum-8chan-goes-offline-after-el-paso-shooting-11564990191.
[30] Jon Brodkin, *Facebook: No one reported NZ shooting video during 17-minute livestream,* ArsTechnica (Mar. 19, 2019), https://arstechnica.com/tech-policy/2019/03/facebook-no-one-reported-nz-shooting-video-during-17-minute-livestream; *see also* Facebook, *Update on New Zealand* (Mar. 18, 2019), https://about.fb.com/news/2019/03/update-on-new-zealand.
[31] Paul Smith, *Telecos caught in social media crackdown,* Australian Financial Review (Mar. 20, 2019), https://www.afr.com/companies/telecommunications/pm-drags-isps-into-postchristchurch-content-control-meeting-as-sites-get-blocked-20190320-h1cl2q (noting that "[o]n Wednesday afternoon a Telstra spokesman said it had started to unblock sites that reached out to it and were proactively removing related content from their websites. He conceded some websites had been blocked despite the fact they had already been removing the footage, and said those sites had been unblocked.").
[32] *See* Prince, *supra* note 24.
[33] Justin Sherman, *Censorship in Crisis: Government Information Crackdowns in the Covid-19 Pandemic* (Washington, D.C.: American University Washington College of Law, August 25, 2020), https://digitalcommons.wcl.american.edu/research/57.
[34] Dartunorro Clark, *Trump suggests 'injection' of disinfectant to beat coronavirus and 'clean' the lungs*, NBC News (Apr. 23, 2020), https://www.nbcnews.com/politics/donald-trump/trump-suggests-injection-disinfectant-beat-coronavirus-clean-lungs-n1191216.
[35] Daphne Leprince-Ringuet, *Domain name registry suspends 600 suspicious coronavirus websites*, ZDNet (Apr. 7, 2020), https://www.zdnet.com/article/domain-name-registrar-suspends-600-suspicious-coronavirus-websites.
[36] "Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams," U.S. Department of Justice (Apr. 22, 2020), https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams.
[37] *Id*.
[38] *See* Derek B. Johnson, *Feds disrupt hundreds of COVID-19 scammer domains*, Federal Computer Week (Apr. 22, 2020), https://fcw.com/articles/2020/04/22/doj-domain-takedowns-johnson.aspx.
[39] It is also unknown if the individual domain registrars and registries that voluntarily took action disclosed their decisions to the affected individuals—e.g., the domain owners—but it is reasonably safe to assume that some form of notification was given.
[40] In March 2020, the U.S. Department of Justice also took legal action against a website engaging in a Covid-19-related wire fraud scheme. After the Department became aware of the website, it requested an injunction from a U.S. district judge. The judge granted the request and issued a temporary restraining order requiring the domain's registrar to immediately take down the website while a DOJ investigation continued. In this case, the DOJ publicly disclosed the details of the takedown action after it occurred, and it even provided the name of the specific domain in its press release, "coronavirusmedicalkit.com." The DOJ release did not name the specific registrar, but it was discoverable through public sources using the domain name; TechCrunch subsequently reported that

the domain registrar was NameCheap, and one of its spokespeople confirmed to the publication that it had responded to the injunction and suspended the website, rendering it inaccessible. *See* Zack Whittaker, *Justice Dept. files its first coronavirus takedown: a bogus vaccine website*, TechCrunch, March 22, 2020, https://techcrunch.com/2020/03/22/justice-department-coronavirus.

[41] While our mapping does not use the terminology of "layers" or the "stack," this is primarily to accommodate categories of actors—such as financial facilitators—that do not neatly fit into a more technical hierarchy of infrastructure service providers. The principles articulated by scholarship on layer-conscious Internet regulation, however, remain highly relevant to this discussion. *See e.g.* Bridy, *supra* note 18 (noting that "different layers of modern digital networks have very different economic and technological attributes" and citing to Blevins' *The New Scarcity*); John Blevins, *The New Scarcity: A First Amendment Framework for Regulating Access to Digital Media Platforms*, 79 Tenn. L. Rev. 353, 359 (2012) (detailing the distinctions between "network-layer platform regulations and application-layer platform regulations"). *See also* Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era,* 48 UCLA L. Rev. 925, 930.

[42] Donovan, *supra* note 17.

[43] *How Does Cloudflare Work?*, Cloudflare (Last accessed May 21, 2021), https://support.cloudflare.com/hc/en-us/articles/205177068-How-does-Cloudflare-work- ("Cloudflare is not a hosting provider.").

[44] *See* Centre for International Governance Innovation & Chatham House, The Royal Institute of International Affairs, Global Commission on Internet Governance 3-4 (2016).

[45] As recently as 2019, nearly a quarter of U.S. adults did not have high-speed broadband service at home, and nearly one-in-five U.S. adults relied on a smartphone for Internet connectivity rather than home broadband service. *See Internet/Broadband Fact Sheet,* Pew Research Center (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/internet-broadband.

[46] *See e.g.*, Samuel Woodhams and Simon Migliano, *The Global Cost of Internet Shutdowns in 2019* (London: PrivacyCo Ltd., January 2020), https://www.top10vpn.com/cost-of-internet-shutdowns/; *Policy Brief: Internet Shutdowns* (Reston: Internet Society, December 2019), https://www.internetsociety.org/policybriefs/internet-shutdowns.

[47] Brodkin, *supra* note 23.

[48] In 2019 alone, some 122 "major" blackouts – defined as blackouts that were either regional or country-wide – were recorded in a range of different countries including Chad, Iran, Myanmar, Sudan; the longest and most wide-spread shutdowns were ordered by India. Samuel Woodhams & Simon Migliano, *Top10VPN* (Jan. 3, 2021), https://www.top10vpn.com/cost-of-internet-shutdowns (noting that "India imposes internet restrictions more often than any other country"); Feliz Solomon, *Internet Shutdowns Become a Favorite Tool of Governments: 'It's Like We Suddenly Went Blind'*, Wall Street Journal (Feb. 25, 2020), https://www.wsj.com/articles/internet-shutdowns-become-a-favorite-tool-of-governments-its-like-we-suddenly-went-blind-11582648765. ISPs can also restrict certain kinds of services and platforms. As just some examples of many, ISPs have been ordered to cut off streaming services in the precursor to the 2018 Bangladeshi elections to prevent the exchange of pictures and videos. *See* Reuters Staff, *Bangladesh slows down mobile internet speeds ahead of election: Daily Star*, Reuters (Dec. 27, 2018), https://www.reuters.com/article/us-bangladesh-election-internet-idUSKCN1OR06E.

[49] "Manage warnings about unsafe sites," Google Chrome Help, n.d. (accessed September 30, 2020), https://support.google.com/chrome/answer/99020?co=GENIE.Platform%3DDesktop&hl=en.

[50] Chris Frost, *What Is the Difference Between Authoritative and Recursive DNS Nameservers?*, Cisco (July 16, 2014), https://umbrella.cisco.com/blog/2014/07/16/difference-authoritative-recursive-dns-nameservers. There are four categories of domain nameservers. The root servers operate as telephone books for their respective roots (such as .com, .org, and .gov) of which there are 13. Each is managed by its own TLD nameserver, which manages information for each domain name with the same root—in turn backed up by an authoritative nameserver.

[51] "What is the difference between a registry, registrar and registrant?" GoDaddy, n.d. (accessed October 1, 2020), https://www.godaddy.com/help/what-is-the-difference-between-a-registry-registrar-and-registrant-8039.
[52] In China, for example, a government body operates and administers the registry for China's top-level domain .cn. and thus allows the government a lever of control over who is able to register domains to host content. *See* "Domain name registration in China," Government of Canada, n.d. (Last accessed November 23, 2020), https://www.tradecommissioner.gc.ca/china-chine/market-facts-faits-sur-le-marche/76359.aspx?lang=eng.
[53] Sean Keane & Oscar Gonzalez, "8chan's Rebranded 8Kun Site Goes Offline Days After Launch," CNET, November 25, 2019, https://www.cnet.com/news/8chan-rebranded-8kun-site-taken-offline-days-after-launch.
[54] Taylor Hatmaker, *Google Drops Domain Hosting for Infamous Neo-Nazi Site the Daily Stormer*, *TechCrunch* (Aug. 14, 2017), https://techcrunch.com/2017/08/14/google-daily-stormer-domain; Catherine Shu, *GoDaddy Tells White Supremacist Site Daily Stormer to Find a New Domain Provider*, *TechCrunch*, (Aug. 14, 2017), https://techcrunch.com/2017/08/13/godaddy-tells-white-supremacist-site-daily-stormer-to-find-a-new-domain-provider; Russell Brandom, *Google Says It Will Ban Neo-Nazi Site After Domain Name Switch*, The Verge (Aug. 14, 2017), https://www.theverge.com/2017/8/14/16145064/google-daily-stormer-ban-neo-nazi-registrar-godaddy; Katie Mettler and Avi Selk, *GoDaddy – then Google – ban neo-Nazi site Daily Stormer for disparaging Charlottesville victim*, The Washington Post (Aug. 14, 2017), https://www.washingtonpost.com/news/morning-mix/wp/2017/08/14/godaddy-bans-neo-nazi-site-daily-stormer-for-disparaging-woman-killed-at-charlottesville-rally.
[55] Göran Marby, *Keeping the DNS Secure During the Coronavirus Pandemic*, ICANN (Apr. 7, 2020), https://www.icann.org/en/blogs/details/keeping-the-dns-secure-during-the-coronavirus-pandemic-7-4-2020-en.
[56] OPENNET INITIATIVE, INTERNET FILTERING IN CHINA 2004-2005: A COUNTRY STUDY 48-49 (2005), https://opennet.net/sites/opennet.net/files/ONI_China_Country_Study.pdf.
[57] James Pearson, *Facebook agreed to censor posts after Vietnam slowed traffic – sources*, Reuters (Apr. 21, 2020), https://www.reuters.com/article/us-vietnam-facebook-exclusive-idUSKCN2232JX.
[58] *Id*.
[59] "What is an origin server?" Cloudflare, n.d. (accessed October 1, 2020), https://www.cloudflare.com/learning/cdn/glossary/origin-server.
[60] Hosting can also be private, rendering websites accessible only to authorized personnel connected to an internal network; for example, a university may provide a database accessible only to certain researchers logged into the university network system, while a business might provide an internal website for Human Resources accessible only by employees using company workstations.
[61] Cloudflare, Verisign, and Amazon (AWS Shield) are among the companies providing this suite of services.
[62] "Netflix Case Study," Amazon Web Services, n.d. (last accessed November 12, 2020), https://aws.amazon.com/solutions/case-studies/netflix-case-study.
[63] Josh Taylor & Julia Carrie Wong, *Cloudflare cuts off far-right message board 8chan after El Paso shooting,* The Guardian (Aug. 4, 2019), https://www.theguardian.com/us-news/2019/aug/05/cloudflare-8chan-matthew-prince-terminate-service-cuts-off-far-right-message-board-el-paso-shooting.
[64] Jeff Desjardins, *How Google retains more than 90% of market share,* Business Insider (Apr. 23, 2018), https://www.businessinsider.com/how-google-retains-more-than-90-of-market-share-2018-4; Daisuke Wakabayashi & Jack Nicas, *Apple, Google and a Deal That Controls the Internet,* N.Y. Times (Oct. 25, 2020).
[65] Cecilia D'Anastasio, *The Christchurch Shooter and YouTube's Radicalization Trap,* Wired (Dec. 8, 2020), https://www.wired.com/story/christchurch-shooter-youtube-radicalization-extremism.

[66] Yoel Roth and Nick Pickles, *Updating our approach to misleading information*, Twitter Blog (May 11, 2020), https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information.html.
[67] Kevin Randall, *Social app Parler is cracking down on hate speech – but only on iPhones*, Washington Post (May 17, 2021), https://www.washingtonpost.com/technology/2021/05/17/parler-apple-app-store.
[68] Annemarie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1523, 1524-25 (2015) (clarifying that the payment processors terminated their services based on their own respective business judgments, not pursuant to any court order).
[69] Annemarie Bridy, *Copyright's Digital Deputies: DMCA-Plus Enforcement by Internet Intermediaries*, in RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW 185, 201 (John A. Rothchild ed., 2016); *see also* Bridy, supra note 68 (describing how, after SOPA and PIPA failed in 2012, corporate IP owners entered into an agreement with payment processors, pursuant to which IP owners notify the payment processors of infringing sales and then they payment processors in turn notify the online merchants, demanding that they desist and terminating services if they fail to do so.) As Professor Bridy describes it, payment processors provide a particularly powerful source of online control: "Whereas it is trivially easy for the operator of a seized or blacklisted domain name to relocate objectionable content to another domain, it is much more difficult for a website operator to replace a canceled banking relationship." Annemarie Bridy, *Internet Payment Blockades*, 67 Fla. L. Rev. 1523, 1525 (2015). This is due to market power: approximately 80% of online transactions use a credit or debit card as a method of payment, and most of those transactions go through one of two payment systems: MasterCard or Visa. In the words of Mark MacCarthy, "One conclusion that can be drawn from these examples is that payment intermediary action has been effective." Mark MacCarthy, *What Payment Intermediaries Are Doing About Online Identity and Why It Matters*, 25 Berkeley Tech. Law J. 1037, 1059 (2010), https://btlj.org/data/articles2015/vol25/25_2/25-berkeley-tech-l-j-1037-1120.pdf.
[70] In this case, the Seventh Circuit called the attempted "suffocation" a form of censorship that violated the First Amendment. Backpage.com v. Dart, 807 F.3d 229, 231, 235 (7th Cir. 2015).
[71] *See* Paris Martineau, *A Quiet War Rages Over Who Can Make Money Online,* Wired (Nov. 30, 2018), https://www.wired.com/story/quiet-war-rages-who-can-make-money-online; *see also* Jillian C. York, *Silicon Valley's puritanical war on sex,* Salon (March 27, 2021), https://www.salon.com/2021/03/27/silicon-valleys-puritanical-war-on-sex.