

Gatekeepers: These tech firms control what's allowed online

Moderating content isn't just something Facebook and Twitter do. There's a 'stack' of companies that run the Internet — and they are under pressure to act.

By [Geoffrey A. Fowler](#) and
[Chris Alcantara](#)

March 24 at 7:00 AM

Who really runs the Internet? A lot of companies you rarely hear about.

Sure, Facebook, Google and Twitter made headlines for shutting down Donald Trump's accounts after the Jan. 6 riot at the Capitol. But the Silicon Valley giants that have been called to [testify before Congress](#) on Thursday about misinformation and hate on social media are not the only — and hardly the first — tech companies to decide what kinds of online speech are acceptable.

A bunch of other companies, stacked on top of each other like layers in a cake, operate the pipes and services that keep the Internet running.

Joan Donovan, research director at Harvard

University's Shorenstein Center, [proposed](#) this view of the Internet's gatekeepers after deadly shootings in 2019 that [germinated](#) on a message board called 8chan. Online hate and disinformation spread because an entire ecosystem supports them, she said, and the rest of the stack has to step up to break the circuit.

Typically unseen parts of the stack flexed their power after the Capitol riot. Amazon Web Services — which provides the cloud-computing power that keeps many apps and websites running — [ended its contract](#) with social network Parler for having too many violent posts and insufficient moderation. App stores run by Apple and Google kicked out Parler, too, effectively kneecapping the platform. Parler, supported financially by major Trump backer [Rebekah Mercer](#), called the moves part of a “[coordinated effort](#)” to silence Trump and his supporters. (Amazon CEO Jeff Bezos owns The Washington Post.)

It's a lot of power to put into the hands of tech executives who aren't elected or don't necessarily have experience weighing what's right for society.

In some slices of the stack, a small number of companies have inordinate influence. Apple's App Store, for example, is the only way you can

buy apps for iPhones and iPads.

Yet tech companies have long made these kinds of calls, dating back to efforts to thwart child exploitation and police people who pirate music and movies.

A law known as [Section 230 of the 1996 Communications Decency Act](#) says “interactive computer services” — companies up and down the stack — cannot be held legally responsible for what others use their services to say. That provides them with a legal shield, with a few exceptions such as sex trafficking, but also gives companies the right to police content as they see fit.

As more of the Internet permeated our lives, so has the expectation that tech companies share a responsibility for content that’s akin to food companies’ responsibility for public health. A pivotal moment came after the [2017 “Unite the Right” rally in Charlottesville](#).

When platforms such as Facebook at the top of the stack were slow to act, pressure shifted down to critical service companies such as GoDaddy and WordPress to shut white supremacist [websites](#), [fundraising systems](#) and [chat forums](#). No longer just conduits for data, many of these companies became reluctant police officers.

“There’s no way for major consumer brands like PayPal to stay fully out of the culture wars,” says PayPal CEO Dan Schulman, adding that the company, which also owns Venmo, removes from service hundreds of websites and individuals each month for a variety of reasons. “It’s our responsibility to ensure that we don’t allow people to use PayPal or Venmo to advocate for violence or hatred or racial intolerance,” he said.

Anti-hate groups, including [Change the Terms](#) and the [Anti-Defamation League](#), have increased the pressure up and down the stack.

But hidden forces, including governments, hackers and often business considerations, can be what drives tech companies to act, says [Eric Goldman](#), a law professor at Santa Clara University. In February, Facebook removed members’ ability to [share news articles in Australia](#) because of a dispute over a law that forced the company to pay publishers.

Critics, like [Jillian York](#), the author of “[Silicon Values: The Future of Free Speech Under Surveillance Capitalism](#),” say when companies become unaccountable censors, it sets a precedent that endangers political and personal expression of all kinds.

“The sex worker, the Palestinian or Burmese or

Egyptian activist/dissident, the LGBTQ+ rights activist, the person speaking out against terrorism in their community — they often have nowhere else to turn, especially if they live in a country without a free media,” she said.

Do companies have a responsibility to moderate content because they have the technical ability? Or does the fact that they could make the wrong calls mean they should hold back?

The conversation about keeping society safe online only gets more complicated from here — up and down the stack.

What they do: A platform is an online forum. That might not sound important, but it’s the type of business fueling many of the most prominent Internet companies. They’re websites and apps that make money by running ads around what other people post or taking a cut from selling other people’s stuff.

Who they are: Platforms are social networks including Facebook, Twitter, Reddit, Discord, YouTube and Twitch; marketplaces such as eBay, Amazon, Craigslist and GoFundMe; and app stores like the ones run by Apple, Google and Amazon. Even rental service Airbnb and ride-hailing service Uber are platforms.

Why they have power: When you make the

platform, you get to decide who and what stands on it. Those standards can shift, and don't necessarily have to be evenly enforced. When you're cut off from a really big platform — like a social network or an app store with billions of users — it can be difficult to find the same audience elsewhere.

When they've taken action: Moves like Twitter banning Trump permanently from its platform in January often are framed by politicians as partisan decisions. Platforms have made these sorts of daily content calls around the world for years. In 2014, [Twitter took down](#) video of the beheading of American journalist James Foley. In 2018, Twitter said it had [suspended 1.2 million accounts](#) linked to the terrorist group ISIS. In 2019, [Facebook banned](#) conspiracy theorist Alex Jones and Black nationalist minister Louis Farrakhan.

Amazon has removed many products from its store, dating back at least to a self-published book on pedophilia in 2010. Even Airbnb, the home rental company, has, since 2017, researched suspected members of hate groups [to prevent them from renting on the service](#).

Platforms also exert power through the design of software that chooses what information gets amplified — and what gets buried. In 2019, when

a misleading, edited video of House Speaker Nancy Pelosi (D-Calif.) went viral, Facebook decided not to delete it but [“heavily reduce”](#) the video’s appearances in people’s news feeds.

What they do: The cloud is online storage and processing power you can rent. Many companies no longer own and maintain the hardware required to beam out webpages, receive email and interact with apps. Increasingly, they find it cheaper and easier to pay one of these companies to “host” a website or service for them.

Who they are: Website-building and -hosting companies including Squarespace, Wix, WordPress and Shopify, as well as cloud-computing providers AWS, Google Cloud, Microsoft Azure, Joyent and Zoho.

Why they have power: Cut off a site’s hosting and it disappears — at least until it can find another provider. Moreover, switching to a different cloud provider can sometimes take a lot of technical and financial effort: Parler was offline for weeks because it didn’t have a Plan B. [\(It eventually came back via cloud service SkySilk.\)](#)

When they’ve taken action: Amazon’s split with Parler wasn’t the first time it fired a customer. In 2010, when AWS was only four

years old, it cut off WikiLeaks, which published classified U.S. documents about the wars in Iraq and Afghanistan. Amazon said WikiLeaks had violated its terms of service by “securing and storing large quantities of data that isn’t rightfully theirs, and publishing this data without ensuring it won’t injure others.”

Other providers got more involved after Charlottesville. Squarespace stopped hosting sites linked to white supremacists and WordPress shut a white supremacist blog. In 2018, Microsoft and Joyent [suspended accounts for social network Gab](#) for its laissez-faire moderation stance after a shooting at a Pittsburgh synagogue.

What they do: These companies are hidden but critical [traffic controllers](#) of the Internet. They help websites and apps stream video, keep hackers at bay, and deliver money rather than speech. These services require technical expertise, a global network or connections to the banking industry few companies can provide on their own.

Who they are: Cloudflare, Akamai, Peer5 and Amazon Cloudfront, PayPal, Stripe and Apple Pay.

Why they have power: Losing a CDN can leave a site open to denial-of-service attacks.

Payment companies can have different leverage — and more accountability — because they're subject to financial services laws that forbid supporting what might be considered terrorism.

When they've taken action: In 2010, PayPal also made moves against WikiLeaks, freezing the account of a German foundation accepting donations on its behalf. In 2017 after Charlottesville, PayPal, Apple Pay and other services stopped processing payments from white supremacist sites.

CDNs have gotten involved, but with more public reluctance. In 2013, Cloudflare CEO Matthew Prince defended working with a Chechen site accused of fomenting terrorism, saying, "[A website is speech. It is not a bomb.](#)" But in 2017, the firm dropped the neo-Nazi Daily Stormer website after requests by what Prince called "vigilante hackers" for it to stop protecting the site. In 2019, [Cloudflare also dropped 8chan](#) after the shooting in El Paso.

What they do: Companies that run the domain name system, or DNS, are the telephone books of the Internet. They allow a site to register the name you type into a browser, then make sure Web traffic gets directed to the right place.

Who they are: GoDaddy, Google, Tucows, DreamHost and Epik.

Why they have power: Domain registrations are a choke point that can quickly shut down a website. A site would remain offline until it finds a new domain registrar.

When they've taken action: In 2010, a software company called EveryDNS stopped directing traffic to WikiLeaks after it said cyberattacks threatened the rest of its network. After Charlottesville in 2017, GoDaddy joined other companies in evicting the Daily Stormer. In 2018, GoDaddy also dropped Gab.

Epik has emerged as a favored alternative for right-leaning sites, including Gab. Epik CEO Rob Monster has criticized what he calls “[digital censorship](#)” by other registrars, and this year Epik also became the domain registrar for Parler.

What they do: Bring websites and apps to smartphones and homes.

Who they are: Comcast, AT&T, Verizon, Charter, Cox and hundreds of other regional and local providers.

Why they have power: Your broadband or cellular data service provider is the last layer between you and the Internet. Governments can use ISPs as their most direct means of control over Internet. In China, the government forces

ISPs to block connections to certain Internet addresses, including foreign services such as Facebook. In the United States, there have been years of vigorous debate about whether ISPs should be required to carry all websites equally, a concept known as net neutrality.

When they've taken action: In 2011, the Motion Picture Association of America and Recording Industry Association of America asked ISPs to help stop piracy by joining the Copyright Alert System, a six-strikes system for home Internet users caught sharing pirated material. In its first year using the system, 2013, Comcast sent 625,000 warning notices to its customers.

ISPs blocking content for noncommercial reasons is less common. In 2011, one train service in San Francisco [shut off all cell service](#) on its platforms to prevent a possible protest.

In January, Your T1 WiFi, an Idaho-based ISP, [said it would block Facebook and Twitter](#) in retaliation for those services banning Trump — but only for customers who asked.
