PROTECT THE STACK

Infrastructure Providers Should Not Be Content Police

Protect the Stack: Infrastructure Providers Should Not Be Content Police

Providers of internet infrastructure services are under pressure to play a greater role in policing online content and participation. Some are deciding to intervene on their own. This is a dangerous trend that must end now.

While the call to enlist the full “stack” in the fight to end harmful speech may be understandable in some cases, it will lead to a host of unintended consequences, particularly for the least powerful users. Subject to rare exceptions, governments should not require such interventions and infrastructure companies should not intervene voluntarily.

Background

Users and policymakers are very familiar with platforms like Facebook, Twitter, or YouTube. But those services are not the internet. In fact, online communication and commerce also depend on a wide range of service providers, including ISPs and telcos, like Comcast, Orange, MTN, Airtel, Movistar, or Vodafone; domain name registrars such as Namecheap or GoDaddy; support services such as Amazon Web Services (AWS), certificate authorities (such as Let’s Encrypt), payment processors such as PayPal and M-Pesa, email, messaging services, and more. Taken together, these providers are sometimes called the “tech stack.”

Most users use the internet without thinking about all those underlying infrastructure services. But those services are essential to online expression, privacy, and security. And when these providers—many of which have little if any contact with users—intervene based on content, their choices can have huge impacts on human rights that may be difficult or impossible to redress.

The specific pitfalls and risks for expression and privacy may vary depending on the nature of the service. But for every infrastructure provider, some combination of the following concerns will apply. Taken together, they powerfully demonstrate why, with rare exceptions, infrastructure providers should stay out of content policing.

A Note on “The Stack”

The stack is a term borrowed from computer science and software engineering, used to describe a combination of tools, processes, programming languages, and mechanisms used in combination to build an application or product. In this context, we are using it to describe the internet as we know it, the service providers, platforms, processes, and various other players that make the modern web possible.

The tech stack includes user-generated content platforms such as Facebook and Twitter as well as the range of infrastructure providers referenced above. Social media platforms rest at the top of the stack, while core infrastructure providers such as your ISP lie at the bottom, with a wide array of intermediaries—including payment processors, and registrars, among others—sit in between.

The Risks to Human Rights

1. Most infrastructure services cannot tailor their intervention practices to be necessary and proportionate.

Platforms often have a variety of moderation options. By contrast, many infrastructure services cannot target their response with the precision human rights standards demand. Twitter blocks specific tweets; Amazon Web Services denies service to an entire site or account, which means its interventions inevitably affect far more than the objectionable speech that motivated the action. Government hijacking of telecommunications services to disrupt the internet for an entire country is particularly egregious.

Egregious actions also occur at the domain level, where registrars that object to speech on a website do not target just that speech, but rather suspend and/or deregister the entire site. For example, ARTICLE 19 has documented multiple instances of “DNS abuse”: the suspension and deregistration of domain names as means of stifling dissent.

We can take a lesson here from the copyright context, where we have also seen domain name registrars and hosting providers shut down entire sites in response to infringement notices targeting a single document. It may be possible for some services to communicate directly with customers where they are concerned about a specific piece of content and request that it be taken down. But if that request is rejected, the service has only the blunt instrument of complete removal at its disposal. And some services may not have a viable way to communicate directly with the source of the content at all.

2. Meaningful notice and appeal is rarely possible, especially for the less powerful.

Human rights standards and due process principles demand that service providers notify users that their speech and/or account has been—or will be—taken offline, and offer users an opportunity to seek redress. At the infrastructure level, such notice and opportunities for redress may be impossible. Infrastructure services are frequently unable to communicate directly with internet users since the services commonly do not have a direct relationship with either the speaker or the audience for the expression at issue. And unlike platform-level content hosts, who can leave an explanatory notice at the original location of a removed post (in a practice sometimes called "tombstoning"), infrastructure providers typically lack the practical ability to notify future users about the ways in which the provider has impeded access to content.

Thus, for example, if a user discovers that a link sent by a friend does not work, they can't easily know whether there was a problem with the link, whether the owner took the site down voluntarily, or whether it was blocked. Users of a service that relies on a payment processor may also be startled to find the service disappear because, unbeknownst to them, the processor shut down payment to that service. In Argentina, for example, Uber was cut off overnight thanks to a court order requiring a payment processor to block payments to the service.

Users are essentially held to the terms and conditions of every service in the chain from speaker to audience, even though they may not know what those services are or how to contact them. Given the potential consequences of violations, and the difficulty of navigating the appeals processes of previously invisible services (assuming such a process even exists), many users will simply avoid sharing controversial opinions altogether. Relatedly, where a service provider has no relationship to the speaker or audience, takedowns will be much easier and cheaper for the business than a nuanced analysis of a given user's speech.

3. Content-based interventions at the infrastructure level cause collateral damage that will disproportionately harm less powerful groups.

Those with power and influence inevitably exploit all systems for censorship to suppress unpopular voices and ideas. Indeed, infrastructure blocking is a favorite tool of authoritarian governments. During a period of sustained social unrest in October 2019, internet users in Ecuador faced repeated network blockages. Nigeria required ISPs to ban Twitter for months. Thanks to an overbroad application of U.S. sanctions, AWS has blocked Iranian users from its services. Cloudflare denied service to a Mastodon instance that hosted a sex worker collective based in Australia, citing U.S. regulations. And of course several countries have shut down the internet altogether.

Moreover, even well-intentioned decision-makers regularly undervalue the speech of marginalized peoples. At the platform level, companies that engage in content moderation consistently reflect and reinforce bias against marginalized communities. Examples abound: Facebook decided, in the midst of the #MeToo movement's rise, that the statement "men are trash" constitutes hateful speech; Twitter decided to use harassment provisions to shut down the verified account of a prominent Egyptian anti-torture activist; various content moderation decisions prevented women of color from sharing with their friends and followers stories of harassment they experience; Twitter decided to mark tweets containing the word "queer" as offensive, regardless of context.

Even patients who can't afford prescription drugs are affected. In an effort to police the use of the word "opioid" and related words in hashtags, Instagram shut down and banned accounts that "appeared" to sell opioids. One consequence was shutting down PharmacyChecker's account, which provides verification and price information about online pharmacies that help patients and their caregivers afford medication through importation, but does not sell medication.

There is no reason to think that infrastructure companies will be any better than platforms at making these calls, and many reasons to think they will be worse.

4. State and private actors may seek to hijack any content-based intervention pathway and expand control over it.

Intervention pathways, once established, may provide state, state-sponsored, and private actors with additional tools for controlling public dialogue. Once processes and tools to interfere with expression are developed or expanded, companies can expect a flood of demands to apply them more broadly. At the platform level, state and state-sponsored actors have weaponized flagging tools to silence dissent. And Cloudflare, which provides a variety of services, including protections from DDos attacks, reports that, after it withdrew security services from a neo-Nazi site conspiracy theory site, it saw a dramatic increase in requests from authoritarian regimes that it do the same with respect to human rights organizations.

In the copyright context, private actors regularly exploit easy takedown processes to silence critics. There is no reason to expect things will be any different at the infrastructure level.

5. Lack of competition and switching costs make it hard or impossible to hold some companies accountable for mistakes or overreach.

When an ISP decides to shut down an individual user's account, in much of the world, no other provider is available: the user is in effect kicked offline. At other layers of the stack, such as the domain name system (DNS), there are multiple providers from which to choose—a speaker whose domain name is frozen can take their website elsewhere. But the existence of alternatives alone is not enough; one must evaluate the costs and ease of switching providers. There is rarely any cheap or easy alternative. And in some locales, government actors may be closely tied to infrastructure companies; for instance, the government of Kenya has 35% ownership in telecommunications company Safaricom. And even where switching is easy, it will not help if all providers at a certain level of the stack choose, or are pressured, to censor the same content, speakers, and/or viewpoints. Finally, the problem may be compounded where service providers are smaller and, therefore, potentially more vulnerable to pressure from governments and private actors.

6. Intervention requirements may be counter-productive.

Intervening to target online speech may actually undermine the goals it is supposed to serve. For example, efforts to police "extremist" content have led to blocking or erasure of work by journalists and human rights defenders to document terrorism and other atrocities. Pressure to block access to internet services in particular countries has undermined efforts to help people bypass government censorship and access accurate information.

7. Infrastructure-level content-based interventions may undermine fundamental internet protocols and compromise security.

Some content-based interventions from infrastructure providers, such as inserting Deep Packet Inspection (DPI) on the network or blocking DNS queries, may reshape the internet's architecture to the detriment of privacy and security. For example, if operators of DNS resolvers began redirecting queries for certain domains based on content alone, it would vastly complicate efforts to make DNS resistant to malicious tampering, because computers cannot distinguish "good" redirections from attempts at website spoofing. If certificate authorities decide they will revoke digital certificates for some websites because they object to their content, the "chain of trust" upon which much internet security depends will be compromised. In addition, by violating a key design principle of the open internet, infrastructure level interventions may accelerate its fragmentation, as people build new infrastructure to bypass such interventions and existing infrastructure providers are faced with conflicting rules and blocking in one country or another based on which they obey.

8. Inconsistent rules are inevitable.

Infrastructure providers, like all service providers that operate across multiple jurisdictions, already face conflicting requirements based on the rules and values of the countries in which they operate. Complying with those conflicting rules is both expensive and, sometimes, impossible. By engaging in content policing, they invite new sets of obligations that may lead to a proverbial race to the bottom, e.g., blocking as much content, across the service, as is required to satisfy the most censorious jurisdiction.

Conclusion

The internet is an essential resource for billions of people around the world. We use it to communicate, to organize, to protest, to work, to learn, to buy and sell, to access government services and more. If the internet is to continue to play that role, we need it to be strong, flexible and secure. We need infrastructure providers to stay focused on their core mission: supporting a robust and resilient internet. That mission is far more important, and more protective of human rights, than attempting to build out content-based intervention processes that will inevitably cause more harm than good.

Signed

Access Now

American Civil Liberties Union (ACLU)

ARTICLE 19

ARTICLE 19 México y Centroamérica

ASEAN Youth Forum

Asociación por los Derechos Civiles (ADC)

Asociația pentru Tehnologie si Internet (ApTI)

Association for Progressive Communications (APC)

Bits of Freedom

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)

Chaos Computer Club (CCC)

Citizen D / Državljan D

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Comun.al, Laboratorio de resiliencia digital

Data Privacy Brasil Research Association

Derechos Digitales - América Latina

Digitale Gesellschaft Schweiz (Switzerland)

Don’t Delete Art (DDA)

Electronic Frontier Foundation (EFF)

Epicenter.works - for digital rights

European Center for Not-for-Profit Law (ECNL)

European Digital Rights (EDRi)

Fight for the Future (FFTF)

Förderverein Informationstechnik und Gesellschaft (Fitug e.V.)

Foundation for Media Alternatives (FMA)

Freemuse

Fundación Huaira

Fundación InternetBolivia.org

Fundación Karisma

Fundación Vía Libre

Global Forum for Media Development (GFMD)

Hiperderecho

Homo Digitalis

Instituto Nupef

Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC)

Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec)

Instituto de Referência em Internet e Sociedade (IRIS)

Intervozes - Coletivo Brasil de Comunicação Social

IT-Pol Denmark

Kandoo

Masaar - Technology and Law Community

National Coalition Against Censorship (NCAC)

Open Knowledge Foundation

OpenMedia

Open Rights Group

Red en Defensa de los Derechos Digitales (R3D)

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)

SeguDigital

SMEX

Southeast Asia Freedom of Expression Network (SAFEnet)

TAPOL

Taraaz

The Sex Workers Project of the Urban Justice Center

The Tor Project

The William Gomes Podcast

The Woodhull Freedom Foundation

Usuarios Digitales