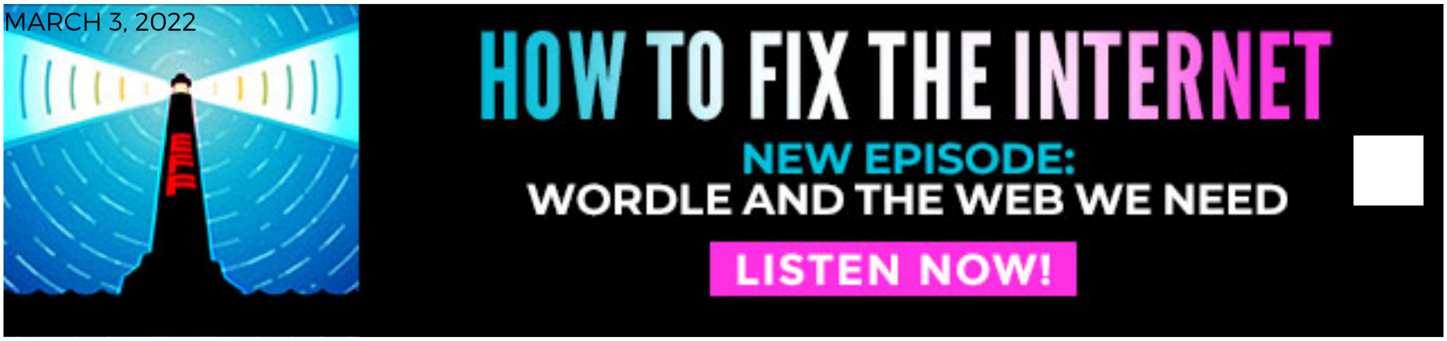
MARCH 3, 2022



ELECTRONIC FRONTIER FOUNDATION

Wartime Is a Bad Time To Mess With the Internet

РУССКИЙ УКРАЇНСЬКА

Like most people, we at EFF are horrified by Russia's invasion of Ukraine. Also like most people, we are not experts on military strategy or international diplomacy. But we do have some expertise with the internet and civil liberties, which is why we are deeply concerned that governments around the world are pressuring internet companies to interfere with fundamental internet infrastructure. Tinkering with the internet as part of a political or military response is likely to backfire in multiple ways.

There is already heavy pressure on social media platforms. Russia is demanding that various companies from Facebook to Google and Netflix carry its state-sponsored content. The European Union, in an unprecedented move, has decided to prohibit the broadcasting and distribution of content by these outlets throughout the European Union, and Ukraine is asking the European Commission to do far more.

But now the government of Ukraine has called on ICANN to disconnect Russia from the internet by revoking its Top Level domain names, ".ru", ".рф" and

".su" from the root zone, in an attempt to make access to Russian websites and email difficult for people outside as well as inside of Russia. Ukraine also reached out to RIPE, one of the five Regional Registries for Europe, the Middle East and parts of Central Asia, asking the organization to revoke IP address delegation to Russia.

As a practical matter, some of these calls are essentially impossible; ICANN can't just press a button and boot a country offline; RIPE can't just revoke IP addresses. But those are not the only problems: remaking fundamental internet infrastructure protocols is likely to lead to a host of dangerous and long-lasting consequences.

Here are a few:

It deprives people of the most powerful tool for sharing information just when they need it most.

While the internet can be used to spread misinformation, it also enables everyone, including activists, human right defenders, journalists and ordinary people, to document and share the real-time facts and resist propaganda. Indeed, Russia has reportedly been trying for years to "unplug" from the internet so it can completely control communications in the country. Internet providers shouldn't help the Russian government, or any government, keep people within an information bubble.

It sets a dangerous precedent.

Intervention pathways, once established, will provide state and state-sponsored actors with additional tools for controlling public dialogue. Once processes and tools to take down expression are developed or expanded, companies can expect a flood of demands to apply them, inevitably to speech those tools were not originally designed, and the companies did not originally intend, to target. At the platform level, state and state-sponsored actors have long since weaponized flagging tools to silence dissent.

It compromises security and privacy for everyone.

Any attempt to compromise the internet's infrastructure will affect the security of the internet and its users. For example, revocation of IP addresses means that things like the Routing Policy Specification Language (RPSL), used by ISPs to describe their routing policies, and Resource Public Key Infrastructure (RPKI), which is used to improve the security for the internet's BGP routing infrastructure, would be severely compromised. This would expose users to man-in-the-middle attacks, compromise daily activities like bank transactions, and undermine the privacy because users would have nowhere to hide.

It undermines trust in the network and the policies upon which it is built.

Trust is paramount to the way networks self-organize and interoperate with other networks. It is what ensures a resilient global communications infrastructure that can withstand pandemics and wars. That trust depends, in turn, on imperfect but painstaking multi-stakeholder processes to develop neutral policies, rules, and institutional mechanisms. Bypassing those mechanisms irretrievably undermines the trust upon which the internet is founded.

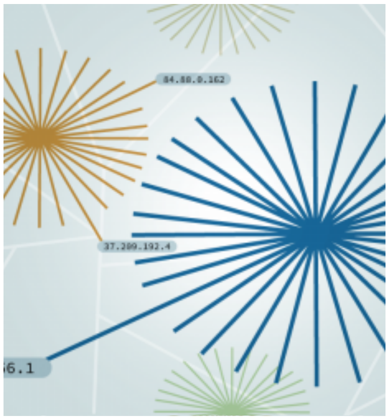
We were relieved to see that ICANN and RIPE have declined to comply with the Ukrainian government’s requests, and we hope other infrastructure organizations follow suit. In moments of crisis, we are often tempted to take previously unthinkable steps. We should resist that temptation here, and take proposals like these off the table altogether. In dark times, people must be able to reach the light, reassure their loved ones, inform themselves and others, and escape the walls of propaganda and censorship. The internet is a crucial tool for all of that – don’t mess with it.

SUBMIT

RELATED UPDATES

DEEPLINKS BLOG BY ALEXIS HANCOCK | MARCH 15, 2022

You Should Not Trust Russia's New "Trusted Root CA"



DEEPLINKS BLOG BY MITCH STOLTZ | APRIL 1, 2021

Ethos Capital Is Grabbing Power Over Domain Names Again, Risking Censorship-For-Profit. Will ICANN Intervene?

How We Saved .ORG: 2020 in Review

.ORG Domain Registry Sale to Ethos Capital Rejected in Stunning Victory for Public Interest Internet

DEEPLINKS BLOG BY ELLIOT HARMON | DECEMBER 23, 2020

PRESS RELEASE | MAY 1, 2020

DEEPLINKS BLOG BY KAREN GULLO, MITCH STOLTZ | APRIL 30, 2020

Victory! ICANN Rejects .ORG Sale to Private Equity Firm Ethos Capital

EFF, Other Nonprofits, and California's Attorney General Tell ICANN To Stop The Private Equity Takeover of .ORG

DEEPLINKS BLOG BY MITCH STOLTZ | APRIL 16, 2020

DEEPLINKS BLOG BY KATHARINE TRENDACOSTA | MARCH 27, 2020

Members of Congress Once Again Urge ICANN to Save Dot Org

DEEPLINKS BLOG BY ELLIOT HARMON, MITCH STOLTZ | MARCH 9, 2020

NGO Community Urges ICANN to Scrutinize the .ORG Sale

.ORG Isn’t Broken, and We Don’t Need Private Equity to ‘Fix’ It

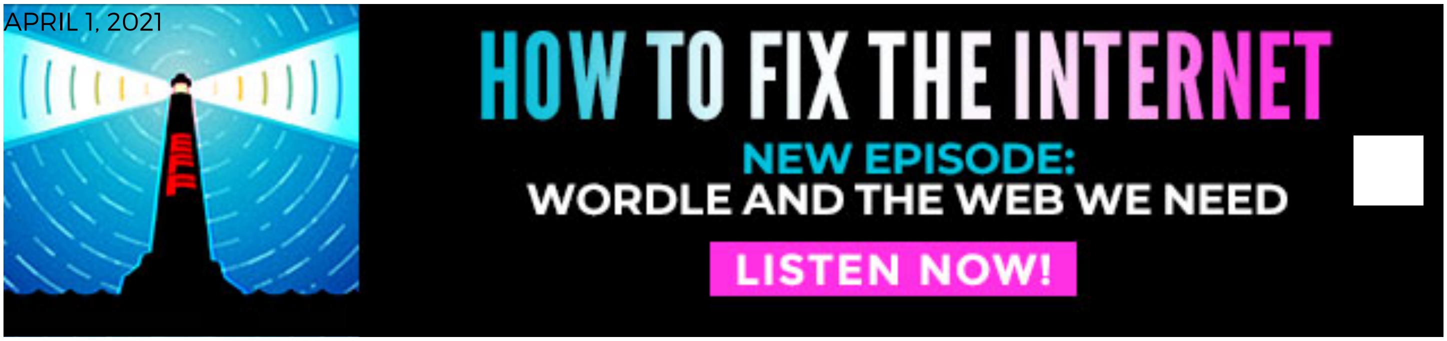
DEEPLINKS BLOG BY CARA GAGLIANO | MARCH 4, 2020

DEEPLINKS BLOG BY ELLIOT HARMON, MITCH STOLTZ | FEBRUARY 26, 2020

Empty Promises Won’t Save the .ORG Takeover

ELECTRONIC FRONTIER FOUNDATION
eff.org

APRIL 1, 2021



ELECTRONIC FRONTIER FOUNDATION

Content Moderation Is A Losing Battle. Infrastructure Companies Should Refuse to Join the Fight

It seems like every week there's another Big Tech hearing accompanied by a flurry of mostly bad ideas for reform. Two events set last week's hubbub apart, both involving Facebook. First, Mark Zuckerberg took a new step in his blatant effort to use 230 reform to entrench Facebook's dominance. Second, new reports are demonstrating, if further demonstration were needed, how badly Facebook is failing at policing the content on its platform with any consistency whatsoever. The overall message is clear: if content moderation doesn't work even with the kind of resources Facebook has, then it won't work anywhere.

Inconsistent Policies Harm Speech in Ways That Are Exacerbated the Further Along the Stack You Go

Facebook has been swearing for many months that it will do a better job of rooting out "dangerous content." But a new report from the Tech Transparency Project demonstrates that it is failing miserably. Last August, Facebook banned some militant groups and other extremist movements tied to violence in the U.S. Now, Facebook is still helping expand the groups' reach by automatically creating new pages for them and directing people who "like" certain militia pages to check out others, effectively helping these movements recruit and radicalize new members.

These groups often share images of guns and violence, misinformation about the pandemic, and racist memes targeting Black Lives Matter activists. QAnon pages also remain live despite Facebook's claim to have taken them down last fall. Meanwhile, a new leak of Facebook's internal guidelines shows how much it struggles to come up with consistent rules for users living under repressive governments. For example, the company forbids "dangerous organizations" —including, but not limited to, designated terrorist organizations—but allows users in certain countries to praise mass murderers and "violent non-state actors" (designated militant groups engaged that do not target civilians) unless their posts contain an explicit reference to violence.

A Facebook spokesperson told the *Guardian:* "We recognise that in conflict zones some violent non-state actors provide key services and negotiate with governments – so we enable praise around those non-violent activities but do not allow praise for violence by these groups."

The problem is not that Facebook is trying to create space for some speech – they should probably do more of that. But the current approach is just incoherent. Like other platforms, Facebook does not base its guidelines on international human rights frameworks, nor do the guidelines necessarily adhere to local laws and regulations. Instead, they seem to be based upon what Facebook policymakers think is best.

The capricious nature of the guidelines is especially clear with respect to LGBTQ+ content. For example, Facebook has limited use of the rainbow "like" button in certain regions, including the Middle East, ostensibly to keep users there safe. But in reality, this denies members of the LGBTQ+ community there the same range of expression as other users and is hypocritical given the fact that Facebook refuses to bend its "authentic names" policy to protect the same users.

Whatever Facebook's intent, in practice, it is taking sides in a region that it doesn't seem to understand. Or as Lebanese researcher Azza El Masri put it on Twitter: "The directive to let pro-violent/terrorist content up in Myanmar, MENA, and other regions while critical content gets routinely taken down shows the extent to which [Facebook] is willing to go to appease our oppressors."

This is not the only example of a social media company making inconsistent decisions about what expression to allow. Twitter, for instance, bans alcohol advertising from every Arab country, including several (such as Lebanon and Egypt) where the practice is perfectly legal. Microsoft Bing once limited sexual search terms from the entire region, despite not being asked by governments to do so.

Now imagine the same kinds of policies being applied to internet access. Or website hosting. Or cloud storage.

All the Resources in the World Can't Make Content Moderation Work at Scale

Facebook's lopsided policies are deserving of critique and point to a larger problem that too much focus on specific policies misses: if Facebook, with the money to hire thousands of moderators, implement filters, and fund an Oversight Board can't manage to develop and implement a consistent, coherent and transparent moderation policy, maybe we should finally admit that we can't look to social media platforms to solve deep-seated political problems – and we should stop trying.

Even more importantly, we should call a halt to any effort to extend this mess beyond platforms. If two decades of experience with social media has taught us anything, it is that the companies are bad at creating and implementing consistent, coherent policies. But at least, when a social media company makes an error in judgement, its impact is relatively limited. But at the infrastructure level, however, those decisions necessarily hit harder and wider. If an internet service provider (ISP) shut down access to LGTBQ+ individuals using the same capricious whims as Facebook, it would be a disaster.

What Infrastructure Companies Can Learn

The full infrastructure of the internet, or the "full stack" is made up of a range of companies and intermediaries that range from consumer facing platforms like Facebook or Pinterest to ISPs, like Comcast or AT&T. Somewhere in the middle are a wide array of intermediaries, such as upstream hosts like Amazon Web Services (AWS), domain name registrars, certificate authorities (such as Let's Encrypt), content delivery networks (CDNs), payment processors, and email services.

For most of us, most of the stack is invisible. We send email, tweet, post, upload photos and read blog posts without thinking about all the services that have to function to get the content from the original creator onto the internet and in front of users' eyeballs all over the world. We may think about our ISP when it gets slow or breaks, but day-to-day, most of us don't think about AWS at all. We are more aware of the content moderation decisions—and mistakes—made by the consumer facing platforms.

We have detailed many times the chilling effect and other problems with opaque, bad, or inconsistent content moderation decisions from companies like Facebook. But when ISPs or intermediaries decide to wade into the content moderation game and start blocking certain users and sites, it's far worse. For one thing, many of these services have few, if any, competitors. For example, too many people in the United States and overseas only have one choice for an ISP. If the only broadband provider in your area cuts you off because they (or your government) didn't like what you said online—or what someone else whose name is on the account said—how can you get back online? Further, at the infrastructure level, services usually cannot target their response narrowly. Twitter can shut down individual accounts; when those users migrate to Parler and continue to engage in offensive speech, AWS can only deny service to the entire site including speech that is entirely unobjectionable. And that is exactly why ISPs and intermediaries need to stay away from this fight entirely. The risks from getting it wrong at the infrastructure level are far too great.

It is easy to understand why repressive governments (and some advocates) want to pressure ISPs and intermediaries in the stack to moderate content: it is a broad, blunt and effective way to silence certain voices. Some intermediaries might also feel compelled to moderate aggressively in the hopes of staving off criticism down the line. As last week's hearing showed, this tactic will not work. The only way to avoid the pressure is to stake out an entirely different approach.

To be clear, in the United States, businesses have a constitutional right to decide what content they want to host. That's why lawmakers who are tempted to pass laws to punish intermediaries beyond platforms in the stack for their content moderation decisions would face the same kind of First Amendment problems as any bill attempting to meddle with speech rights.

But, just because something is legally permissible does not mean it is the right thing to do, especially when implementation will vary depending on who is asking for it, when. Content moderation is empirically impossible to do well at scale; given the impact of the inevitable mistakes, ISPs and infrastructure intermediaries should not try. Instead, they should reject pressure to moderate like platforms, and clarify that they are much more like the local power company. If you wouldn't want the power company shutting off service to a house just because someone doesn't like what's going on inside, you shouldn't want a domain name registrar freezing a domain name because someone doesn't like a site, or an ISP shutting down an account. And if you would hold the power company responsible for the behavior you don't like just because that behavior relied on electricity, you shouldn't hold an ISP or a domain name registrar or CDN, etc, responsible for behavior or speech that relies on their services either.

If more than two decades of social media content moderation has taught us anything, it is that we cannot tech our way out of a fundamentally political problem. Social media companies have tried and failed to do so; beyond the platform, companies should refuse to replicate those failures.

TAGS:

COMO

SUBMIT

RELATED UPDATES

DEEPLINKS BLOG BY CHRISTOPH SCHMON, HALEY PEDERSEN | JUNE 8, 2022

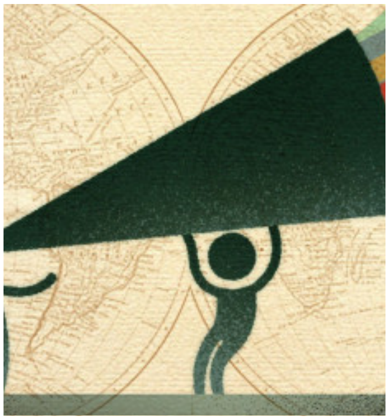
Platform Liability Trends Around the Globe: Moving Forward

DEEPLINKS BLOG BY MERI BAGHDASARYAN, KATITZA RODRIGUEZ, KAREN GULLO, DAVID GREENE | JUNE 6, 2022

Speech-Related Offenses Should be Excluded from the Proposed UN Cybercrime Treaty

Platform Liability Trends Around the Globe: Recent Noteworthy Developments

11th Circuit's Ruling to Uphold Injunction Against Florida’s Social Media Law is a Win Amid a Growing



DEEPLINKS BLOG BY CHRISTOPH SCHMON, HALEY PEDERSEN | JUNE 1, 2022

DEEPLINKS BLOG BY KAREN GULLO | MAY 26, 2022

Pack of Bad Online Speech Bills

DEEPLINKS BLOG BY CHRISTOPH SCHMON, HALEY PEDERSEN | MAY 25, 2022

Platform Liability Trends Around the Globe: Taxonomy and Tools of Intermediary Liability

EFF to Court: California Law Does Not Bar Content Moderation on Social Media

DEEPLINKS BLOG BY JASON KELLEY | MAY 23, 2022

DEEPLINKS BLOG BY CHRISTOPH SCHMON, HALEY PEDERSEN | MAY 19, 2022

Platform Liability Trends Around the Globe: From Safe Harbors to Increased Responsibility

PRESS RELEASE | MAY 17, 2022

EFF to Supreme Court: Put Texas Social Media Law Back on Hold

In a Blow to Free Speech, Texas' Social Media Law Allowed to Proceed Pending Appeal

EFF Statement on the Declaration for the Future of the Internet

DEEPLINKS BLOG BY KAREN GULLO | MAY 12, 2022

DEEPLINKS BLOG BY KAREN GULLO | APRIL 28, 2022

ELECTRONIC FRONTIER FOUNDATION
eff.org