Free Speech Under Threat as the SPLC and Its Cohorts Politicize the "Pipe Bomb" Case and Synagogue Shooting

written by GEG | October 30, 2018

Last week, the Southern Poverty Law Center (SPLC) and the Center for American Progress (founded by John Podesta and financed by George Soros), along with four other organizations, drafted a guide for tech giants Twitter, Facebook and YouTube to police speech on the internet. The policy seeks to deputize intermediaries including social media platforms, payment processors, domain name registrars and chat services to shut down so-called 'hate speech'. In the past, users weaponized the power to flag other users, and it is likely to happen again.

Following the suspicious pipe bomb threats against Democrats and the Tree of Life Synagogue shooting, political groups blamed Trump and his supporters for crimes they did not commit. Victor Davis Hanson says that left commits moral blackmail to enact their agenda, and are coming after free speech. Facebook, Twitter and Youtube can instantly terminate any speech they disagree with in an electronic Reign of Terror, as they refuse to define what permissible speech is. The tech giants apply censorship asymmetrically, and target those who disagree with the left.

A coalition of civil rights and public interest groups issued recommendations today on policies they believe Internet intermediaries should adopt to try to address hate online. While there's much of value in these recommendations, EFF does not and cannot support the full document. Because we deeply respect these organizations, the work they do, and the work we often do together; and because we think the discussion over how to support online expression—including ensuring that some voices aren't drowned out by harassment or threats—is an important one, we want to explain our position.

We agree that online speech is not always pretty—sometimes it's extremely ugly and causes real world harm. The effects of this kind of speech are often disproportionately felt by communities for whom the Internet has also provided invaluable tools to organize, educate, and connect. Systemic discrimination does not disappear and can even be amplified online. Given the paucity and inadequacy of tools for users themselves to push back, it's no surprise that many would look to Internet intermediaries to do more.

We also see many good ideas in this document, beginning with a right of appeal. There seems to be near universal agreement that intermediaries that choose to take down "unlawful" or "illegitimate" content will inevitably make mistakes. We know that both human content moderators and machine learning algorithms are prone to error, and that even low error rates can affect large swaths of users. As such, companies must, at a minimum, make sure there's a process for appeal that is both rapid and fair, and not only for "hateful" speech, but for all speech.

Another great idea: far more transparency. It's very difficult for users and policymakers to comment on what intermediaries are doing if we don't know the lay of the land. The model policy offers a pretty granular set of requirements that would provide

a reasonable start. But we believe that transparency of this kind should apply to all types of speech.

Another good feature of the model policy are provisions for evaluation and training so we can figure out the actual effects of various content moderation approaches.

So there's a lot to like about these proposals; indeed, they reflect some of the principles EFF and others have supported for years.

But there's much to worry about too.

Companies Shouldn't Be The Speech Police

Our key concern with the model policy is this: It seeks to deputize a nearly unlimited range of intermediaries—from social media platforms to payment processors to domain name registrars to chat services—to police a huge range of speech. According to these recommendations, if a company helps in any way to make online speech happen, it should monitor that speech and shut it down if it crosses a line.

This is a profoundly dangerous idea, for several reasons.

First, enlisting such a broad array of services to start actively monitoring and intervening in any speech for which they provide infrastructure represents a dramatic departure from the expectations of most users. For example, users will have to worry about satisfying not only their host's terms and conditions but also those of every service in the chain from speaker to audience—even though the actual speaker may not even be aware of all of those services or where they draw the line between hateful and non-hateful speech. Given the potential consequences of violations, many users will simply avoid sharing controversial opinions altogether.

Second, we've learned from the copyright wars that many services will be hard-pressed to come up with responses that are tailored solely to objectional content. In 2010, for example, Microsoft sent a DMCA takedown notice to Network Solutions, Cryptome's DNS and hosting provider, complaining about Cryptome's (lawful) posting of a global law enforcement guide. Network Solutions asked Cryptome to remove the guide. When Cryptome refused, Network Solutions pulled the plug on the *entire* Cryptome website—full of clearly legal content—because Network Solutions was not technically capable of targeting and removing the single document. The site was not restored until wide outcry in the blogosphere forced Microsoft to retract its takedown request. When the Chamber of Commerce sought to silence a parody website created by activist group The Yes Men, it sent a DMCA takedown notice to the Yes Men's hosting service's upstream ISP, Hurricane Electric. When the hosting service May First/People Link resisted Hurricane Electric's demands to remove the parody site, Hurricane Electric shut down MayFirst/PeopleLink's connection entirely, temporarily taking offline hundreds of "innocent bystander" websites as collateral damage.

Third, we also know that many of these service providers have only the most tangential relationship to their users; faced with a complaint, takedown will be much easier and cheaper than a nuanced analysis of a given user's speech. As the document itself acknowledges and as the past unfortunately demonstrates, intermediaries of all stripes

are not well-positioned to make good decisions about what constitutes "hateful" expression. While the document acknowledges that determining hateful activities can be complicated "in a small number of cases," the number likely won't be small at all.

Finally, and most broadly, this document calls on companies to abandon any commitment they might have to the free and open Internet, and instead embrace a thoroughly locked-down, highly monitored web, from which a speaker can be effectively ejected at any time, without any path to address concerns prior to takedown.

To be clear, the free and open Internet has never been fully free or open—hence the impetus for this document. But, at root, the Internet still represents and embodies an extraordinary idea: that anyone with a computing device can connect with the world, anonymously or not, to tell their story, organize, educate and learn. Moderated forums can be valuable to many people, but there must also be a place on the Internet for unmoderated communications, where content is controlled neither by the government nor a large corporation.

Read full article here…