BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of Section 230 of the Communications Act of 1934	Docket No. RM-11862

Opposition of the Internet Infrastructure Coalition

Scott Blake Harris
Paul Caritj

HARRIS, WILTSHIRE & GRANNIS LLP
1919 M Street, N.W.
8th Floor
Washington, DC 20036
202-649-2700

Counsel to the
Internet Infrastructure Coalition

September 2, 2020

Table of Contents

I. Introduction and Summary 1

II. NTIA overlooks the foundational importance of Section 230 protections throughout ourconnected economy. 3

III. Internet infrastructure companies cannot rely on automated content screening to mitigate risk. 9

IV. The Commission lacks authority to make regulations under Section 230. 12

V. NTIA's proposed rules violate the First Amendment. 14

VI. Conclusion 18

I. Introduction and Summary

Section 230, as it is understood today, is fundamental to free and robust speech on the Internet. In addition to the protections it provides social media companies, Section 230 is also essential to the companies that operate the infrastructure on which speakers depend. While social media platforms dominate the headlines, everything online depends on the Internet's infrastructure, including the services provided by hosting companies, data centers, domain registrars and registries, cloud infrastructure providers, managed services providers, and related services. Many of these companies are members of the Internet Infrastructure Coalition (i2Coalition), an organization formed to ensure that those who build the infrastructure of the Internet have a voice in public policy.

Internet infrastructure providers play a critical role in promoting open and robust Internet speech by not only providing the infrastructure on which much of the Internet depends, but also by providing services that minimize barriers to entry for anyone with a message, no matter their viewpoint. Internet infrastructure providers also drive economic growth by providing small businesses with greater reach and flexibility to innovate. Therefore, we agree with NTIA that protecting the Internet from stagnation and excessive restrictions is a critical goal.

Unfortunately, NTIA's proposal poses a far greater risk to free and open speech on the Internet than the moderation practices of a few private companies ever could. NTIA focuses narrowly on Section 230 of the Communications Decency Act as it applies to a handful of the largest social media platforms and seeks to narrow its protections to combat alleged political biases in these companies' content moderation practices.[1] Unfortunately, in so doing, NTIA not

---

[1] *See* Exec. Order No. 13925: Preventing Online Censorship, 85 Fed. Reg. 34,079, 34,081 (June 2, 2020) (E.O. 13925).

only ignores the law but also misses the vastly diverse array of services and speakers beyond those platforms. And it overlooks the role of the free market — and the marketplace of ideas — in ensuring that fora will always exist for speech for which there is a willing and interested audience, in the absence of government restrictions.

NTIA's proposed regulations would upend the liability protections Internet infrastructure companies rely on to protect them against litigation over content posted by users. Although it would not strip these protections away overtly, it proposes new rules that would call this liability shield into question for any provider that makes decisions that even arguably evince a "discernable viewpoint" — a meaningless standard that invites abuse and subjectivity. NTIA's proposal therefore attempts to force providers into the untenable position of being unable to engage in any form of content moderation or even to choose with whom they do business. In so doing, it exposes Internet infrastructure providers to new risks and requires them to contemplate measures such as pre-screening content and, ironically, far more aggressive content moderation and removal than they would ever have considered otherwise. Not only would such measures stifle a great deal of Internet speech, they would raise costs and erect other new barriers, particularly for small businesses and individuals seeking to build an online presence.

NTIA's proposal would also be illegal. The text of Section 230, its legislative history, and its purpose all clearly indicate that Congress intended Section 230 to be interpreted by the courts, not to serve as a font for vast new FCC regulatory authority. Moreover, NTIA's proposed rules, while putatively promoting free speech, would actually violate the First Amendment by conditioning providers' liability protections on their compliance with content-based distinctions.

II. NTIA overlooks the foundational importance of Section 230 protections throughout our connected economy.

Internet infrastructure providers rely on the protections of Section 230 to make their businesses work. It offers crucial assurances that their companies will not be treated as the publishers or speakers of content made available by others — assurances that have become foundational to the economic diversity and low barriers to entry that characterize today's Internet. These assurances are vital because the nature of critical Internet infrastructure services, such as website hosting and content distribution networks, may create a superficial association between the infrastructure provider and third-party content. Indeed, Section 230(c)(1) has played a key role in protecting such companies against lawsuits relating to content posted by independent third parties, which the infrastructure provider never reviewed and in no way endorsed.

In one dramatic example, the family of one of the victims of the tragic 2019 mass shooting in El Paso, TX,[2] brought a wrongful death suit against Cloudflare, an i2Coalition member, as well as its CEO and numerous other parties.[3] The basis for these allegations was apparently the fact that 8chan, the platform on which the shooter posted racist messages, used one or more of Cloudflare's services before Cloudflare terminated service in August 2019. Cloudflare's cybersecurity services, in some cases, can result in Cloudflare's name appearing in public Domain Name System records associated with its users' websites. This can lead people to misunderstand Cloudflare's relationship with websites and their content, and seek to hold it

---

[2] *See* Molly Hennessy-Fiske, El Paso shooting victim remembered at funeral: 'She was just a beautiful person,' LA TIMES (Aug. 9, 2019, 4:00 PM), https://www.latimes.com/world-nation/story/2019-08-09/funerals-begin-for-shooting-victims-in-el-paso.

[3] *See* Pls.' Pet., Englisbee, et al. v. Cloudflare Inc., et al., 2019 DCV 4202 (Tex. El Paso County Ct. filed Oct. 29, 2019).

liable for this content even though Cloudflare has no opportunity to review it and, in fact, cannot even access content posted on user-generated content sites like 8chan. Cloudflare defended itself in that case by asserting the protections of Section 230(c)(1), among other things, which prevents Cloudflare from being "treated as the publisher or speaker of any information provided by another information content provider."

The facts of this case are thankfully atypical, but Internet infrastructure companies know that there is nothing abnormal about aggrieved parties seeking to hold them liable for content posted by users. Whether they host the content on their servers, accelerate users' access to it using their content distribution network, or use their network to protect the content from cyberattacks, Internet infrastructure companies are the targets of lawsuits even with the robust liability protections of Section 230. Without its protections, or if its protections were restricted, such lawsuits would proliferate, and Internet infrastructure companies would lose a fundamental tool in managing their risk.

Unfortunately, NTIA's proposed restriction of Section 230 threatens to do just that. NTIA proposes a "clarification" of the statute's definition of "information content provider" that would extend that term to cover any service provider that moderates content in a way that evinces "a reasonably discernible viewpoint." Far from a mere "clarification," this extremely broad concept would allow virtually any plaintiff to allege that a service has a "viewpoint," even if the service has moderated or terminated service only rarely and with great care and discretion. This, in turn, would vitiate the protections of Section 230(c)(1) by placing the service provider in the position of an Internet content provider speaking on its own behalf — rather than a service standing apart from content provided by "another information content provider."[4] As the petition

[4] 47 U.S.C. § 230(c)(1).

unabashedly explains, "prioritization of content under a variety of techniques, particularly when it appears to reflect a particular[] viewpoint, might render an entire platform a vehicle for expression and thus an information content provider."[5]

This change would thrust Internet infrastructure companies back into the "moderator's dilemma" created by cases like *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*[6] that Section 230 was specifically designed to correct. Hosting providers and other critical builders of the nation's Internet infrastructure would have to make a choice. They could choose to maintain their liability protections by abstaining from any moderation of objectionable content. Or they could choose to moderate content on their network, consistent with their business needs, but accept that doing so could strip them of their liability protection under Section 230(c)(1). For Internet infrastructure companies, neither option is tenable.

A business that abstains from any moderation would be forced to maintain content on its network regardless of the threat that it may pose to its legitimate business goals. For example, failing to remove some types of content may result in the blacklisting of a provider's Internet Protocol ("IP") addresses either by third-party email providers seeking to block spam or third-party Internet content filtering services. This can have a major impact on a provider's business because the available pool of IP addresses is severely limited and, therefore, each of a provider's IP addresses is commonly shared among numerous customers. In addition, some types of content draw a significantly greater intensity of cyberattacks, greatly increasing the costs of hosting it.

---

[5] Petition for Rulemaking of the National Telecommunications and Information Administration at 42, Docket No. RM-11862 (filed July 27, 2020) ("Petition").

[6] *See* Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (unpublished).

For example, Endurance International Group offers web hosting, domain registration, email marketing, and other Internet infrastructure services through a number of brands including Bluehost, Domain.com, and Constant Contact. Because Endurance recognizes the important role its industry plays in ensuring that anyone can have a presence on the Internet, it exercises great restraint in deciding when content must be removed from its platform. As a general matter, Endurance's policy is not to remove customer content unless a compelling case can be made for doing so. Nonetheless, Endurance has encountered situations where, due to its content, one of its hosted sites attracts incessant cyberattacks. Although Endurance believes that it is not its role to block unpopular content from the Internet, it simply cannot host sites that place such extreme demands on its network, including where a website under attack is hosted on a shared server that might host up to thousands of other websites — one of the most economical options for small businesses, bloggers, and others to try an idea or establish an online presence at very little cost. Today, Section 230 protects Endurance's ability to make such operational decisions, including removing content, to ensure that it can continue to serve its customers reliably and affordably. Under NTIA's proposal, however, such a move could endanger Endurance's Section 230(c)(1) liability protection by inviting litigants to claim that such decisions were made in bad faith or manifest a discernible viewpoint.

Challenges to hosted content on legal grounds would also present major risks under NTIA's proposal. i2Coalition members including Endurance, Rackspace, and others commonly receive requests to take down content that is allegedly defamatory or illegal in other ways that cannot readily be ascertained based on a review of the content alone. However, in the absence of a judgment or other final legal decision, there is often no way for an infrastructure provider to know whether a decision to take the material down or to leave it up would be most in the public

interest or least likely to trigger liability. In a claim that a provider is hosting defamatory content, for example, a provider cannot know whether the complaint is legitimate and leaving the content on its network would perpetuate the defamation — or whether the complaint is spurious and taking the content down would be unjustified and potentially injurious to the content owner or the public at large. For example, review sites are often targets of defamation claims, but they may also warn viewers of fraud or other bad behavior.

Today, Section 230 allows providers to limit their liability in such situations. But NTIA's proposed restrictions would increase the risks associated with such routine decisions, no matter what course the provider chooses. A decision to take the content down could invite arguments that the provider has acted in bad faith or with bias. But a decision to leave it up could increase the provider's risk of liability and perpetuate an ongoing public harm.

Some i2Coalition members have faced similar decisions relating to the ongoing public health crisis caused by the SARS-CoV-2 pandemic. As the U.S. Department of Justice and other law enforcement have cracked down on those who seek to take advantage of the pandemic for their own gain,[7] i2Coalition members have received notices from law enforcement notifying them of *potentially* fraudulent COVID-19-related content. Determining with certainty which content is fraudulent and which is not, however, requires investigative resources well beyond those that Internet infrastructure companies can bring to bear. Indeed, i2Coalition members have, in at least one case, received notice from law enforcement officials that identified a hosted site as providing fraudulent information about COVID-19 testing, only later to learn the site was operated by a small business offering real testing services. Therefore, hosting providers must

[7] *See* Memorandum from the Deputy Attorney Gen., U.S. Dep't. of Justice to All Heads of Law Enforcement Components, Heads of Litigating Divisions, and U.S. Attorneys (Mar. 24, 2020), https://www.justice.gov/file/1262771/download.

decide whether to take such content down, and risk withholding valuable information from the public, or leave it up and risk perpetuating a fraud. Again, today's Section 230 protects businesses' ability to make these difficult decisions without undue risk of liability. NTIA's proposal could strip away this protection whether they leave the information up or take it down — causing utter chaos in the Internet ecosystem.

Worse still, many Internet infrastructure providers, due to their role in the broader Internet infrastructure system, have only blunt tools at their disposal for policing content that could potentially expose them to liability. For example, one i2Coalition member, Donuts, provides domain name registry services for 242 top-level domains, including .live, .photography, and .consulting. As a registry, they perform a role analogous to a wholesaler, providing the services to companies like Domain.com that interact directly with individuals and organizations and allow them to register domain names. Because of this role, however, Donuts's only recourse to avoid liability from problematic content hosted on a .live domain name, for example, would be to suspend or terminate the domain name, essentially disconnecting any associated website, email, application, or other services. Therefore, Donuts only takes action to block content in extremely narrow and serious circumstances. However, erosion of Section 230's liability protections would make such a policy of restraint more difficult to maintain.

Similarly, another i2Coalition member, cPanel, provides management software for website hosts and other types of providers. Some cPanel tools, however, allow users to upload, edit, and manage content in a way that has sometimes caused cPanel to become incorrectly associated with content managed using their tools. However, cPanel has no ability to police individual users' use of its tools. Rather, it licenses its software to website hosts that, in turn, make the tools available to their users. Therefore, cPanel's only potential recourse is to disable software licenses

barring entire companies from using its tools, and disrupting the service provided to all of that host's users. Because this is such a drastic remedy, cPanel has only taken this action in one very unusual case. But NTIA's proposal would greatly increase the risks for businesses that — rightly — take such a hands-off approach.

NTIA's proposal, therefore, would disrupt the basic infrastructure of the Internet even as it drives increased costs for individuals and small businesses. By raising barriers to entry, it would perversely undercut a broad array of competitive services, leaving only well-funded companies with the resources to maintain their own websites. Others, ironically, may be driven onto more closely moderated and tightly structured platforms, such as those offered by large social media companies, which have the greater resources required to take on content screening and increased liability.

III. Internet infrastructure companies cannot rely on automated content screening to mitigate risk.

NTIA glosses over the impact that its proposals would have on tech companies, including Internet infrastructure providers.[8] It asserts that the loss of liability protection under Section 230 is acceptable in the current environment because a platform provider can use artificial intelligence technology and other high-tech tools to ensure that its service remains free of harmful content, thus controlling their liability. Unfortunately, however, NTIA is simply wrong. No technology exists that would allow operators to meaningfully limit their liability in the absence of Section 230's protections.

The most obvious flaw in NTIA's assertion relates to defamatory content. It is extremely doubtful that any company — including the largest social media platforms — will have the

[8] *See, e.g.*, Petition at 9-14.

technology to automatically flag defamatory content today or in the foreseeable future. This is simply because a statement must be false in order to be defamatory.[9] But the truth or falsity of an assertion requires access to information, and the capability to analyze this information, beyond the reach of any automated system that platform providers could foreseeably create. Obscenity presents similar challenges by requiring a highly nuanced understanding of evolving community norms in order to be reliably identified.[10] Justice Stewart may have known obscenity when he saw it,[11] but it is unlikely a computer will have the same degree of skill anytime soon. Any AI-based system is also likely to have a large number of both false positives and false negatives. Thus, it would block a substantial amount of speech that should have been permitted even as it fails to fully control a platform's liability. Simply put, there is no technology today that would automatically flag content with any reliability.

But even if the largest social media platforms could use artificial intelligence to help ease the burden of screening billions of social media posts, this advantage would not be available to Internet infrastructure providers who currently rely on Section 230 protections to host third-party content without undue risk of liability. Unlike social media platforms, Internet infrastructure companies often do not have unrestricted access to users' content — many have no access at all — and have no way of knowing what type of content a third-party has uploaded or in what format, making AI-based screening impossible. At the same time, the services provided by Internet infrastructure companies typically do not involve AI-based categorization, prioritization, or targeting, meaning that they do not have existing AI-based tools that could be repurposed for screening content.

---

[9] Restatement 2d of Torts § 558 (1977).

[10] Roth v. United States, 354 U.S. 476, 489 (1957).

[11] Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J. concurring.).

One i2Coalition member, Rackspace Technology, Inc., for example, provides a wide range of cloud-based services including data management, datacenter colocation, managed clouds, and virtual hosting. In these roles, Rackspace services often host websites and other data that could include content that could expose Rackspace to liability, were it not for the protections afforded providers of "interactive computer services" under Section 230. Indeed, Rackspace devotes considerable resources to ensuring that its network remains "clean" and free of prohibited content, processing as many as 6 million complaints per year.

Given the nature of Rackspace's services, however, there would be no way to effectively screen this content before it can be made available on Rackspace's network. For Rackspace to review and approve every website created, every file uploaded, and every email sent on its network would be literally impossible. And attempting to do so would be profoundly inconsistent with the expectations of Rackspace's customers, and the customers of any other hosting service, who expect that they will enjoy unfettered access to the hosting platform they have purchased.

Unfortunately, the harm of eroding Section 230's liability protections cannot, therefore, be waved away. By undermining the liability protections of Section 230, NTIA's petition would force Internet infrastructure companies to restructure their operations and business practices in ways that would raise costs for consumers and small businesses and potentially curtail important services. For example, U.S. providers may struggle to provide the low-cost hosting services that millions of small businesses rely on today in the absence of reliable legal tools that allow them to limit their liability for hosted content. This would be a major blow for America's small businesses that rely on these services and a major setback for online speech.

IV. The Commission lacks authority to make regulations under Section 230.

For more than twenty years, it has been widely understood that Congress intended Section 230 — directed as it was to insulating providers from common-law tort claims and other forms of legal liability — to be interpreted and applied by the courts. And over those intervening decades that is exactly what has occurred, with courts developing a robust body of case law, with no serious suggestion by the FCC or any other regulator that they might have a role to play in interpreting Section 230's protections.

NTIA now asserts, in effect, that prior Commissions, prior administrations, established industry consensus, and thousands of judicial decisions all got it wrong. Simply because of where it was codified in the U.S. Code, NTIA claims that the FCC possesses previously undiscovered powers to deeply enmesh itself in content-based speech regulation of the Internet by rendering interpretations of, and potentially restrictions on, Section 230's protections. It cannot be denied that the Commission has broad powers to interpret the provisions of the Communications Act. However, this authority does not extend so far as to allow the Commission to make regulations to override longstanding judicial interpretations of Section 230.

Most obviously, the statute includes no language hinting at a regulatory role for the FCC. In fact, it does the opposite: Section 230(a)(4) announces Congress's finding that the Internet has flourished "to the benefit of all Americans, with a minimum of government regulation." Likewise, Section 230(b)(2) explicitly states that it is the policy of the United States to maintain a free market on the Internet "unfettered by Federal or State regulation." The D.C. Circuit has held that such statements of policy "can help delineate the contours of statutory authority."[12] In this case, these findings and policy statements demonstrate that Congress was not silent on the

[12] Comcast Corp. v. F.C.C., 600 F.3d 642, 654 (D.C. Cir. 2010).

question of Commission authority. Congress clearly intended there to be no federal regulation under Section 230.

Even if Congress had not been clear, there are good reasons to conclude that the Commission lacks regulatory authority under Section 230. The regulatory authority NTIA posits in its petition would put the FCC in the position of dictating what types of content are "objectionable," and how a provider should go about making its moderation decisions "in good faith."[13] These decisions would dictate the daily business of Internet infrastructure companies, including cloud providers and content distribution networks whose services support large enterprises, small businesses, blogs, and personal websites, among others. This regulatory authority would therefore reach into virtually every corner of the Internet, influencing the content that may be posted and restructuring longstanding industry relationships by pushing companies to unwillingly step into the role of censor.

But the Supreme Court has held that, when Congress grants a regulatory agency such sweeping authority, it must do so clearly. Just as Congress would not surreptitiously grant the Food and Drug Administration the power to regulate tobacco,[14] or quietly give the Environmental Protection Agency authority to regulate small emitters of greenhouse gases,[15] Section 230 cannot be interpreted as conferring upon the FCC vast authority over Internet content without even a word of explanation. Such claims to sweeping regulatory authority are especially dubious when an agency claims to "discover in a long-extant statute an unheralded power to regulate a significant portion of the American economy."[16] All the more so when, as in

---

[13] Petition at 31-39.

[14] Food and Drug Admin. v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 159 (2000).

[15] Util. Air Regulatory Grp. v. E.P.A., 573 U.S. 302, 324 (2014).

[16] *Id*. (internal quotation marks omitted).

this case, the agency's claim to authority would "render the statute unrecognizable to the Congress that designed it."[17]

Such reservations are amplified, in this case, by the fact that the newly discovered authority not only would grant the FCC new regulatory powers over a significant portion of the U.S. economy, but also would do so in a manner that installs the Commission as an arbiter of acceptable speech. If courts demand a clear expression of congressional intent before allowing a regulator to claim authority over tobacco or greenhouse gases, surely at least this level of scrutiny should be applied when an agency seeks to interpose itself in the exercise of one of our most closely guarded constitutional rights. That NTIA's proposed rules would violate these rights out of the starting gate confirms that restraint is the only prudent course.

V. NTIA's proposed rules violate the First Amendment.

NTIA's proposed rules would impose content-based regulations on private actors' speech in violation of the First Amendment. NTIA proposes a series of definitions for the various categories of content that a provider may remove without liability under Section 230(c)(2)(a). For example, the petition proposes to constrain the definition of the terms "obscene," "lewd," "lascivious," and "filthy" so that they encompass only content that would constitute obscenity under prevailing First Amendment jurisprudence[18] or that would have constituted "obscene libel" banned from the U.S. Mail under the Comstock Act.[19] It defines "excessively violent" to mean either content that is "violent and for mature audiences" or that promotes or constitutes

---

[17] *Id*. (internal quotation marks omitted).

[18] *Compare* Petition at 37 *with* Roth, 354 U.S. at 489 (1957).

[19] Section 3893 of the Revised Statutes made by section 211 of the Criminal Code, Act of March 4, 1909, c. 321, 35 Stat. 1088, 1129. NTIA does not address the fact that this Comstock Act language was held to be constitutional only to the extent that it is coextensive with the definition of obscenity articulated in Roth, 354 U.S. at 492.

terrorism. And it constrains the term "otherwise objectionable" to only content which "is similar in type to obscene, lewd, lascivious, filthy, excessively violent, or harassing materials."

Thus, NTIA's proposal — like Section 230 itself — acknowledges that providers and users of interactive computer services may make certain editorial decisions regarding the content they are willing to allow on their platforms. A platform that seeks to be an appropriate venue for children may, for example, prohibit depictions or descriptions of violence. But it may also choose not to. Similarly, under NTIA's proposal, platforms may choose to bar obscenity, whether or not applicable state laws would require them to do so. In short, platforms may choose — or be forced, for business reasons — not to function as neutral conduits for the speech of others. But, in making decisions such as whether to bar violence and obscenity, they also assume the role of speakers. When they do so, the D.C. Circuit has recognized that "entities that serve as conduits for speech produced by others receive First Amendment protection."[20]

Yet, beyond the narrow categories targeted under NTIA's proposed rules, the petition seeks to penalize the platforms that choose to disassociate themselves from any *other* form of speech. To promote health and human safety online, Donuts, an i2Coalition member, for example, and other leading domain name registries and registrars have agreed to voluntarily take steps to "disrupt the illegal distribution of child sexual abuse materials, illegal distribution of opioids, human trafficking, and material with specific, credible incitements to violence."[21] Removal of some of these categories of content, such as distribution of malware, would be

---

[20] United States Telecom Ass'n v. F.C.C., 825 F.3d 674, 742 (D.C. Cir. 2016). *See also* Zeran v. America Online, 129 F.3d 327, 330 (4th Cir. 1997) (explaining that Section 230 protects a service provider's "exercise of a publisher's traditional editorial functions — such as deciding whether to publish, withdraw, postpone or alter content").

[21] Framework to Address Abuse, DONUTS (Oct. 8, 2019), https://donuts.news/framework-to-address-abuse.

permissible under NTIA's proposed rules. But these efforts to prevent abuse go farther and could include voluntary actions against, for example, websites engaged in the unlicensed distribution of pharmaceuticals. NTIA's rules would penalize Donuts for acting on their belief that such material is dangerous and should not be allowed to proliferate online. Other services may seek to adopt analogous policies seeking to curb types of content even less similar to those targeted by NTIA.

Thus, NTIA's proposed rules plainly disadvantage speakers that seek to limit the speech with which they are associated in ways inconsistent with NTIA's own vision for discourse on the Internet. Users and providers that do so would be excluded from the protections of Section 230(c)(2)(a), raising the specter of liability for such removals. Speakers that only moderate content in a manner with which NTIA agrees, however, would remain insulated from liability. *In other words, NTIA's proposal discriminates between speakers based on the content of their speech.*

It is foundational to our First Amendment jurisprudence, however, that "[r]egulations which permit the Government to discriminate on the basis of the content of the message cannot be tolerated under the First Amendment."[22] It makes no difference that NTIA's proposed rules would withhold the benefit of a liability shield rather than imposing a penalty. The government "may not deny a benefit to a person on a basis that infringes his constitutionally protected interests — especially, his interest in freedom of speech."[23] Nor does it matter that the proposed

---

[22] Regan v. Time, Inc., 468 U.S. 641, 648-649 (1984).

[23] Perry v. Sindermann, 408 U.S. 593, 597 (1972). A parallel line of cases has held that the government may, under limited circumstances, condition the receipt of government funding in ways that burden constitutionally protected interests. *See, e.g.*, Rust v. Sullivan, 500 U.S. 173, 195, n. 4 (1991). *See also* Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc., 570 U.S. 205, 206 (2013) (the government may impose speech-based "conditions that define the limits of the government spending program" but may not "seek to leverage funding to regulate speech outside the contours of the federal program itself"). But this jurisprudence is irrelevant here as

rules would punish speakers for what they choose not to say rather than what is said. In fact, the Supreme Court has held that regulations that compel speech are often more pernicious than those that proscribe it:

> Free speech serves many ends. It is essential to our democratic form of government and it furthers the search for truth. Whenever the Federal Government or a State prevents individuals from saying what they think on important matters or compels them to voice ideas with which they disagree, it undermines these ends.
>
> When speech is compelled, however, additional damage is done. In that situation, individuals are coerced into betraying their convictions. Forcing free and independent individuals to endorse ideas they find objectionable is always demeaning, and for this reason, one of our landmark free speech cases said that a law commanding involuntary affirmation of objected-to beliefs would require even more immediate and urgent grounds than a law demanding silence.[24]

Notably, NTIA's proposed interpretation of Section 230(c)(2) would render the statute unconstitutional by reading a key feature out of its text. First, although NTIA proposes detailed, objective definitions for the various terms listed in 230(c)(2)(a), the statute's standard is subjective: it extends liability protections for decisions to take down content that "*the provider or user considers to be* obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."[25] This subjective standard avoids the pernicious viewpoint-based discrimination inherent in NTIA's attempt to reframe the rule in objective terms. NTIA's omission of this subjective component renders it plainly inconsistent with the statutory test it purports to interpret — another fatal flaw in NTIA's proposal. Second, and even more importantly, however, NTIA's proposed interpretation would convert a viewpoint-neutral statutory provision into one that

---

it deals only with government funding programs. It is animated by the Spending Clause, Art. I, § 8, cl. 1, a distinct source of congressional authority not implicated by NTIA's petition.

[24] Janus v. Am. Fed'n of State, Cty., & Mun. Employees, Council 31, 138 S. Ct. 2448, 2464 (2018) (internal citations and quotation marks omitted).

[25] 47 U.S.C. § 230(c)(2)(a) (emphasis added).

unconstitutionally conditions its benefits on a speaker's compliance with a program of speech restrictions devised by the president and proposed by NTIA under his direction. Such a regulation would clearly violate the First Amendment.

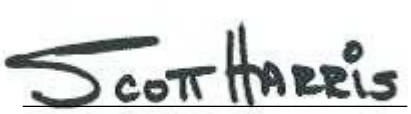
VI. Conclusion

NTIA's petition asks the FCC to vastly expand its regulatory jurisdiction to include decisions made by private companies to keep up or take down content posted by others. This radical expansion of the FCC's authority, however, would overstep the bounds set by both Section 230 and the First Amendment.

Even if the Commission could lawfully exercise these powers, however, the public interest would weigh decisively against doing so. NTIA's proposal would erode or eliminate liability protections that Internet infrastructure providers rely on every day to help small businesses, individuals, and even new Internet services reach their customers and users. Section 230's liability protections allow these infrastructure companies to offer their services on a neutral basis without pre-screening or intrusive content moderation, while retaining the flexibility to address truly harmful content in response to complaints, requests by law enforcement, or other special circumstances. NTIA's proposal would force many infrastructure

providers to choose between these goals, undermining the free and open forum for speech that today's Internet provides and limiting the Internet's potential as an engine for continued economic growth and innovation.

Respectfully submitted,



Scott Blake Harris
Paul Caritj

HARRIS, WILTSHIRE & GRANNIS LLP
1919 M Street, N.W.
8th Floor
Washington, DC 20036
202-649-2700

Counsel to the Internet Infrastructure Coalition

September 2, 2020

Certificate of Service

I, Allison O'Connor, certify that on this 2nd day of September, 2020, I caused a copy of the foregoing comments to be served by postage pre-paid mail on the following:

Douglas Kinkoph
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

/s/ Allison O'Connor