July 16, 2025

Attorney General's Office
ATTN: Proposed Rulemaking
Supreme Court Building
207 W. High Street, PO Box 899
Jefferson City, MO 65102
regulations@ago.mo.gov

Re: Proposed Rules – 15 CSR 60-19.010 Definitions; 15 CSR 60-19.020 Prohibition on Restricting Choice of Content Moderator; 15 CSR 60-19.030 Prohibition on Onerous and Unnecessary Access Requirements; 15 CSR 60-19.040 Severability, Construction, and Effective Date (Oppose)

Dear Attorney General Bailey:

In response to the Proposed Rules and Notice to Submit Comments published by the Attorney General's Office in the Missouri Register at 50 Mo. Reg. 852-58 (June 16, 2025),[1] the Computer & Communications Industry Association (CCIA)[2] submits the following comments explaining how the Proposed Rules are unconstitutional and preempted, threaten free expression and security online, and would chill innovation and competition in the state.

CCIA's comments also provide a broad overview of content moderation and trust and safety from an industry-wide perspective, including explaining that content moderation is a tool (and right) employed by digital services to protect users while facilitating speech; digital services' legal compliance obligations prompt and impact content moderation decisions; and services must employ diverse and context-based approaches to content moderation given varied considerations and evolving trust and safety expectations of users.

I. Digital Services Exercise Their First Amendment Right to Curate Content to Promote Trust and Safety and Free Expression

Leading digital services are committed to ensuring consumer trust and safety online for all users, especially children. Bad actors like predators and criminals misuse services to perpetrate fraud, scams, viruses, or malware, and a significant amount of content moderation is focused on these and similar harms. Responsible services invest heavily in combating this illegal and dangerous content that violates their terms of service, with content moderation at scale requiring both automated tools and human review.

[1] 50 Mo. Reg. 852-58 (June 16, 2025).
[2] CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

Facing millions of content moderation decisions daily and confronted with a spectrum of bad actors, dangerous content, and harmful material, digital services employ various content moderation tools to protect their users, and themselves. Removing content is not the only tool in the content moderation toolbox. For example, mechanisms like community notes enable individuals to provide context in some situations, helping users find high-quality information they can trust.

Furthermore, some digital services already provide controls for users to curate how they interact with content. For example, Facebook and Instagram provide controls for users to see content in chronological order, with the most recent posts at the top. Users also have the ability to further personalize their feed by selecting "Show More", "Show Less", "Hide", or "Unfollow" on posts. Users can adjust these controls at any time to change the amount of political content recommended to them. The policies and practices underlying these decisions are constantly evolving as service providers improve their methodologies and engage with consumers to improve user experiences and safety. Digital services have diverse content moderation policies, and these policies may be implemented in various ways based on user demand.

When companies have to make millions of calls in real time at scale, not everyone is going to agree with every decision. Regardless, private companies have constitutional rights to curate what information they display. The First Amendment of the United States Constitution protects digital services' editorial discretion to decide what speech to host or not, and enables them to define themselves in part by those decisions. As the Court ruled in *Moody v. NetChoice, LLC*, "The government may not, in supposed pursuit of better expressive balance, alter a private speaker's own editorial choices about the mix of speech it wants to convey."[3] Along with the First Amendment, Section 230 of the Communications Act protects companies from liability for their content moderation decisions — including the speech they host. Together, these protections have allowed digital services to develop a vibrant and expansive environment of communication and exchange of ideas.

Consumers are empowered to choose online communities that fit their values and interests, including picking services whose content moderation terms align with how the consumers define harmful content. This facilitates robust competition throughout the technology sector by enabling organizations of all sizes online to differentiate themselves with their featured content and policies, ensuring that users online can access the information most important to them.

As the Supreme Court has repeatedly made clear, no government actor may prevent—or compel—speech, as doing so violates the First Amendment of the U.S. Constitution.[4]

II. There Is No One-Size-Fits-All Approach to Trust and Safety

There is no one-size-fits-all approach to trust and safety work, and individual companies have their own content policies guided by their values, products, and risks. Digital services' content moderation actions and trust and safety operations are business judgments about security and liability risk. These decisions also reflect each service's preferences and the brand they seek to

[3] 144 S. Ct. 2383, 2403 (2024).
[4] *See, e.g.*, *id.*; *303 Creative LLC v. Elenis,* 600 U.S. 570 (2023); *Reno v. ACLU,* 521 U.S. 844 (1997); *Erznoznik v. City of Jacksonville,* 422 U.S. 205 (1975).

develop and market to users. Services are consistently enforcing operational and legal actions that are crucial to maintaining their business.

Many businesses offline engage in similar activities, such as vetting users to ensure their services are not being used to fund fraud, terrorism, or other illegal activities. Private organizations must also consider reputational consequences and the views of shareholders and customers, and digital services are no different. Research demonstrates the financial impact on websites, influenced by advertisers and their users, from harmful content.[5]

Digital services must develop internal frameworks that account for context, purpose, and evolving approaches to controversial issues. Content moderation policies with 'one-size-fits-all' rules that do not consider context can inadvertently restrict all forms of speech, including educational and news content or historical and academic content about difficult topics or events. One user may see a piece of journalistic or educational content as documenting a past historical event or current news, while another may see it as glorifying terrorism. Many digital services therefore rely on case-by-case decisions and avoid treating all information about a controversial topic in the exact same way, and instead require differential treatment of both users and content.

Rather than "censoring" a particular viewpoint or limiting discussion, this approach protects users, complies with existing laws, and enables free expression online. Good-faith approaches to moderating content prompt digital services to thoughtfully consider the context and impact of speech.

III. The Proposed Rules Exceed Missouri's Constitutional and Statutory Authority

The Proposed Rules purport to be authorized by the Missouri Merchandising Practices Act (MMPA). The MMPA, however, does not grant the Missouri Attorney General the authority to adopt rules (like the Proposed Rules) beyond the law's specified scope, which is merchandising practices—i.e., consumer fraud protection and ensuring fairness in commercial transactions. The Proposed Rules would extend the Act to completely new subject matter, which is far beyond the MMPA's capabilities.

The Proposed Rules' alleged basis under the MMPA relies on a blatantly cherry-picked misreading of a line from *Moody* that mentioned "enforcing competition laws." However, in context it's clear that their reading is precisely backwards.[6] In *Moody*, the Court also recognized that: "In a better world, there would be fewer inequities in speech opportunities; and the government can take many steps to bring that world closer. But it cannot prohibit speech to improve or better balance the speech market. On the spectrum of dangers to free

[5] Melissa Pittaoulis, *Hate Speech & Digital Ads: The Impact of Harmful Content on Brands*, CCIA Research Center (Sept. 5, 2023), https://ccianet.org/research/reports/hate-speech-digital-ads-impact/.
[6] *See* Mike Masnick, *Missouri AG Thinks Supreme Court Ruling Lets Him Control Social Media Moderation (It Doesn't)*, Techdirt (May 15, 2025), https://www.techdirt.com/2025/05/15/missouri-ag-thinks-supreme-court-ruling-lets-him-control-social-media-moderation-it-doesnt/ ("The Court couldn't be more clear: while states can enforce genuine competition laws, they absolutely cannot use that power as a backdoor to control content moderation decisions.").

expression, there are few greater than allowing the government to change the speech of private actors in order to achieve its own conception of speech nirvana."[7]

Deeming something as "an unfair, deceptive, fraudulent, or otherwise unlawful practice" is not an incantation that makes it automatically in scope of the MMPA. Similarly, framing something that is clearly related to constitutional speech as related to "antitrust" or "market power" does not magically make government action immune to First Amendment scrutiny.

Digital services' exercise of their First Amendment right to editorial discretion is not only a method of expression; it is also a business decision. Curating content thoughtfully while advancing the free expression of users is how digital services distinguish themselves and compete with one another—just as a newspaper establishes its value and character through editorial decisions. In fact, the Proposed Rules would inhibit, rather than foster, competition.

IV. The Proposed Rules' Definition of "Social Media" Is Overbroad and Likely Unconstitutional

The Proposed Rules' expansive definition of "social media platform" includes sites with the "primary purpose of posting or receiving user-generated content." This definition likely encompasses many online services that do not function as social networks, such as cloud storage and file sharing services. In straying from the traditional understanding of social media, it mischaracterizes the "primary purpose" of many digital services.

Moreover, federal courts have found that regulating websites based on their "primary" purpose or function creates content-based distinctions in violation of the First Amendment and is unconstitutionally vague in violation of the Fourteenth Amendment. An Arkansas federal court recently invalidated a law defining a "social media company" as having the "primary purpose of interacting socially with other profiles and accounts" because the law "[did] not define 'primary purpose'—a term critical to determining which entities fall within its scope," and was "ambiguous as to whose 'primary purpose' is being considered— the user in creating the account or the company in making the forum available."[8] The court also found that regulating websites on this basis was inherently content-based, as "whether any particular [company or platform] falls within the ban is determined by the content of the [posts] resting inside that [company or platform]."[9] An Ohio federal court recently invalidated a similar law on the same grounds, noting that defining "social media platform[s]" based on their "predominant or exclusive function" was "a proxy for 'differential treatment' of specific types of speech,"[10] and that regulating websites based on their "primary purpose" violated the Fourteenth Amendment.[11] Such reasoning applies equally to the Proposed Rules' definition of "social media platform."

Overall, this kind of vagueness would invite inconsistent enforcement and even incentivize digital services to limit user expression capabilities to avoid the kind of scrutiny this definition

[7] *Moody v. NetChoice*, 144 S. Ct. 2383, 2407 (2024).
[8] *NetChoice, LLC v. Griffin*, No. 23-cv-05105, 2025 WL 978607 at *36 (W.D. Ark. Mar. 31, 2025).
[9] *Id.* at *22. *See also* Jesse Lieberfeld, *Constitutional Barriers to Social Media Regulation*, Disruptive Competition Project (Apr. 14, 2025), https://project-disco.org/privacy/constitutional-barriers-to-social-media-regulation/.
[10] *NetChoice, LLC v. Yost*, No. 2:24-cv-00047, 2025 WL 1137485 at *39 (S.D. Ohio Apr. 16, 2025).
[11] *Id.* at *46.

invites. This would discourage all kinds of innovation, including community-led content creation and collaborative functions that are crucial to the online information ecosystem.

V. Forced Interoperability Harms Digital Security

The Proposed Rules also require the enabling of third-party content moderation, which introduces significant risks to Missourians' privacy and online safety and security. Mandating data access for content moderation will undermine sites' cybersecurity and violate users' privacy, putting their data at risk. Requiring digital services to allow users to "select a third-party content moderator of their choice" exposes them to technical and legal risks. Such actions would require access to user data and account behavior, which would make services unable to guarantee user safety or comply with privacy laws due to giving moderation control to unaffiliated entities.

Additionally, the Proposed Rules prohibit covered platforms from vetting these third parties' privacy and security practices, effectively removing any check against bad actors posing as content moderation services in order to access user data. Even well-intentioned content moderator tools may lack adequate privacy and security practices and become targets for criminals, hackers, and foreign state actors.

Furthermore, the Proposed Rules seem to approach the contemplated third-party content moderator industry with the mindset of "if you build it, they will come". At present, there is no meaningful third-party content moderator industry, and it is doubtful that such a high-cost business model would even be viable. Realistically, the Proposed Rules will encourage third-party content moderators to collect and then sell user data to cover the substantial costs of storing and processing massive amounts of content. Because the Proposed Rules do not limit what content moderator services can do with people's private information, there is a very real threat that these services could sell access to people's data in order to recoup their costs. Contrary to the Proposed Rules' assertion, this proposal would put Missourians' data at unacceptable risk.

VI. The Proposed Rules Would Burden Smaller Digital Services, Developers, Overall Innovation, and User Experience in Missouri

As outlined in the Proposed Rules, the compliance cost for digital services would be up to $34.6 million for initial development and maintenance, followed by up to $7.36 million per year for user content moderation services. Given these extremely large costs, small and medium-sized businesses are likely to seek other places for their organizations, due to these burdensome obligations. Entrepreneurs and other innovative businesses seek out clarity and predictability, and often do not have the capacity to implement expensive requirements or large legal departments. Despite the Proposed Rules exempting covered platforms that fall under a specific threshold, this would hurt innovation in the state, creating uncertainty in the landscape, especially for startups that are looking to grow and expand.

The rule will also likely worsen Missouri users' experiences. Users often choose websites based on the development and customization options they offer, and the Proposed Rules

would disincentivize improvements to these features. This approach is likely to lead to the fragmentation of safety standards due to regulatory burdens on organizations of all sizes.

* * * * *

Overall, the Proposed Rules' regulation of content moderation would be an extreme expansion of the MMPA's scope, with serious consequences for innovation, digital services' rights and capabilities, and Missouri users' private data and security online.

We appreciate your consideration of our comments and stand ready to provide additional information as Missouri considers proposals related to online safety.

Respectfully submitted,

Megan Stokes
State Policy Director
Computer & Communications Industry Association