



June 13, 2025

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

Re: Proposed Rules – 15 CSR 60-18.010 Definitions; 15 CSR 60-18.020 Operation of an Internet Platform, Application, or Search Engine; 15 CSR 60-18.030 Reasonable Age Verification Methods; 15 CSR 60-18.040 Applicability of This Rule; 15 CSR 60-18.050 Counting Violations; 15 CSR 60-18.060 Requirement to Create Device-Side Verification Option; 15 CSR 60-18.070 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. 691-712 (May 15, 2025), the Computer & Communications Industry Association (CCIA)¹ submits the following comments. CCIA firmly believes that children are entitled to greater security and privacy online. Our members have designed and developed settings and parental tools to individually tailor younger users' online use to their developmental needs. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools allow parents to block specific sites entirely.² This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.

However, although well-intentioned, the Proposed Rules raise serious constitutional concerns. Additionally, mandatory, one-size-fits-all age verification could unintentionally harm kids and families in Missouri by jeopardizing their privacy.

Federal courts have recently and repeatedly held that laws requiring age verification online violate the First and Fourteenth Amendments.

In 2004, the U.S. Supreme Court struck down the Child Online Protection Act (COPA),³ Congress's attempt to criminalize the posting of content deemed "harmful to minors" unless the poster required "'use of a credit card' or 'any other reasonable measures that are feasible under available technology'" to confirm that the viewer was not a minor.⁴ The Court reasoned

¹ 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>.

² Competitive Enterprise Institute, *Children Online Safety Tools*, <https://cei.org/children-online-safety-tools/> (last updated Feb. 19, 2025).

³ 47 U.S.C. § 231 (1998).

⁴ *Ashcroft v. ACLU (Ashcroft II)*, 542 U.S. 656, 656 (2004).

that since “filtering software is a less restrictive alternative” that would allow “childless adults [to] gain access to speech they have a right to see without having to identify themselves or provide their credit card information,”⁵ COPA violated the First Amendment. COPA’s definition of “harmful to minors” closely parallels the Proposed Rules’ definition of “pornographic for minors,”⁶ and the same principles apply — since filtering and blocking software provides a less restrictive means of achieving the same end that does not force childless adults to identify themselves, the Proposed Rules likely violate the First Amendment.

Recent state legislation requiring age verification for social media sites has also faced numerous successful constitutional challenges. Federal courts in Arkansas and Ohio have held that such laws violate both the First Amendment’s guarantee of free speech and the Fourteenth Amendment’s Due Process Clause. In Arkansas, the court held that “The State does not have the power to prevent children from hearing or saying anything without their parents’ prior consent. Such laws do not enforce parental authority over children’s speech . . . ; they impose *governmental* authority, subject only to a parental veto.”⁷ Missouri proposes a similar state-mandated system within the rule, and does not allow parents to make decisions about their child’s internet use.

A similar Ohio law was also found to violate the Fourteenth Amendment’s Due Process Clause, in part because it exempted the indefinite category of “‘established’ and ‘widely recognized’ media outlets whose ‘primary purpose’ is to ‘report news and current events,’” with the court concluding that “Such capacious and subjective language practically invites arbitrary application of the law.”⁸ Missouri creates a similarly vague exception for “a newspaper, news publication, or news source, printed or on an online or mobile platform, of current news and public interest.” There is no clear standard for what constitutes “public interest,” and the rule will therefore be enforced in a similarly subjective and arbitrary manner.

Numerous other federal judges have placed similar laws on hold until challenges can be fully reviewed, including in California,⁹ Florida,¹⁰ Mississippi,¹¹ Texas,¹² and Utah.¹³ In California, the Ninth Circuit recently issued a temporary stay against a state law with many similar provisions¹⁴ after the District Court found the law to be “content-based on its face”¹⁵ and to “likely fail strict scrutiny.”¹⁶ Chief Judge Walker in the Northern District of Florida recently summarized the consensus view, stating that “like other district courts around the country, this Court simply recognizes that the First Amendment places stringent requirements on the State to avoid substantially burdening speech unless the State can show that doing so is necessary to achieve its significant interests.”¹⁷

⁵ *Id.* at 657.

⁶ Compare *id.* at 661-62 with 15 CSR 60-18.010(7).

⁷ *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 at *31 (W.D. Ark. Mar. 31, 2025) (quoting *Brown v. Ent. Merchs. Ass’n*, 564 U.S. 786, 795) (internal quotation marks omitted) (emphasis in original).

⁸ *NetChoice v. Yost*, No. 2:24-cv-00047, 2025 WL 1137485 at *36 (S.D. Ohio Apr. 16, 2025).

⁹ See, e.g., *NetChoice v. Bonta*, No. 24-cv-07885, 2025 WL 28610 (N.D. Cal. Jan. 2, 2025); *NetChoice v. Bonta*, No. 22-cv-08861, 2024 WL 5264045 (N.D. Cal. Dec. 31, 2024).

¹⁰ See, e.g., *CCIA v. Uthmeier*, No. 24-cv-438, 2025 WL 1570007 (N.D. Fla. June 3, 2025).

¹¹ See, e.g., *NetChoice v. Fitch*, No. 24-cv-00170, 2024 WL 3276409 (S.D. Miss. July 1, 2024).

¹² See, e.g., *CCIA v. Paxton*, 747 F. Supp. 3d 1011 (W.D. Tex. 2024).

¹³ See, e.g., *NetChoice v. Reyes*, No. 23-cv-00911, 2024 WL 4135626 (D. Utah Sept. 10, 2024).

¹⁴ *NetChoice v. Bonta*, No. 24-cv-07885 (9th Cir. Jan. 28, 2025) (order granting motion for injunctive relief).

¹⁵ *NetChoice v. Bonta*, No. 22-cv-08861, 2025 WL 807961, at *6 (N.D. Cal. Mar. 13, 2025).

¹⁶ *Id.* at *14.

¹⁷ *Uthmeier* at *1.



An age verification mandate would curtail individuals' ability to tailor their preferences regarding content and services and violate their privacy.

It is possible to protect children online without a statewide age verification mandate. Many products, both digital and physical, can have effective child safety features installed on them even if they are primarily designed for adults. For example, automobiles are designed with seats and seatbelts for adult consumers. However, parents can install car seats designed specifically for children's safety. Likewise, many devices and services have content filtering technologies that allow parents to individually tailor settings and preferences to select age-appropriate content for themselves and their children. These types of filters and settings, however, are not activated by default.

The Proposed Rules would also cause digital services to restrict content that is not subject to the regulations to avoid liability. This would restrict Missouri users' access to information that is socially valuable and contains a variety of viewpoints, like content related to sexual abuse prevention or other public service announcements. As there is no single, blanket method to identify and filter all pornography on the internet, the Proposed Rules create serious concerns regarding compelled speech and free expression for internet users of all ages.

Additionally, the Proposed Rules would also require individuals to share personal information with third parties, including IDs or biometrics, making any holder or processor of the information a prime target for cyberattacks or data breaches.¹⁸ Furthermore, the requirements would call into question government surveillance practices of material related to accessing online sexual content. To comply with the proposed requirements, companies would be required to collect sensitive identification information that they normally would not, and government officials could access this sensitive data through enforcement inquiries and processes.

The Proposed Rules would burden smaller digital services, developers, and overall innovation in Missouri.

As several Proposed Rules acknowledge, compliance "costs may range from \$0 to \$4,608,000 annually for social media platforms or websites and \$0 to \$70 million annually for internet search providers." This would drastically increase operating costs for digital services that host any type of content, not just that which is allegedly "pornographic for minors." These obligations would burden companies through payment for verification systems as well as the legal services needed to protect this kind of information. This requirement would not only harm existing digital services, but would especially harm startups operating in the state or ones that provide content to Missouri residents, impacting their ability to compete in the market.¹⁹

The Proposed Rules also raise concerns about implementation. For example, the directive to blur out or make "unavailable images, GIFs, or videos depicting material pornographic for minors" carries significant compliance hurdles that are both impractical and burdensome.

¹⁸ Age-verification legislation discourages data minimization, even when legislators don't intend that, R St. Inst. (May 24, 2023), <https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/>.

¹⁹ More than just a number: How determining user age impacts startups, Engine (Feb. 2024), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/65d8b6ab876bfd5b70f8795e/1708701355604/FINAL+-+2024+More+Than+Just+A+Number.pdf>.



Furthermore, the Proposed Rules would force companies to figure out how to either geofence Missouri users or seek other ways of compliance, despite potential conflicts with other state laws.

As explained above, CCIA believes that an alternative to solving these complex issues is to offer more targeted protections, including parental controls, filtering tools, and media literacy education. By working with businesses to continue their ongoing private efforts to implement safety and security mechanisms, the state can provide greater flexibility for families and service providers alike, and better safeguard free speech and privacy.

The Proposed Rules go far beyond what is permitted by the Missouri Merchandising Practices Act.

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 Attorney General lacks the authority to install a system for verifying the ages of users, as well as deeming what is and isn’t “inappropriate” online. This makes the Proposed Rules not a permissible objective under the MMPA as it is currently written.

For example, Proposed Rule 15 CSR 60-18.060 is a ludicrously broad proposed expansion of the MMPA’s scope: “It is an unfair, deceptive, fraudulent, or otherwise unlawful practice for any provider or operator of a mobile operating system present on at least ten million devices in the United States to provide or operate the mobile operating system unless the mobile operating system has the capacity to provide digital age-verification identification as contemplated in 15 CSR 60-18.030 that a website or application can use to comply with 15 CSR 60-18.020.” Deeming something as “an unfair, deceptive, fraudulent, or otherwise unlawful practice” is not an incantation that makes it automatically in scope of the MMPA.

* * * * *

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