CENTER FOR RENEWING AMERICA

EPPC | ETHICS & PUBLIC POLICY CENTER
*Defending American Ideals*

# What Congress Can Do to Restrict Children's Access to Pornography

*by* Adam Candeub, The Center for Renewing America,
Clare Morell, The Ethics and Public Policy Center (EPPC)

December 9, 2021

The unprecedented availability of pornography online is transforming our society and human relationships today in a deleterious manner. With the emergence of "Tube" sites that provide endless, instant, high-definition video, the rise of social media, and the proliferation of smartphones and tablets, pornography, and perhaps human sexuality, is now fundamentally different from the past. Online pornography in particular affects young adults and children whose understanding of sexuality is formative. Pornography has been shown to affect the brain like a drug, leading to addiction, rewiring neural pathways, and impairing the prefrontal cortex that controls our executive function and impulse control, all of which are especially damaging for the brains of adolescents and children who have higher neuroplasticity.[1] This is also threatening on a civilization level, by undermining people's ability to have normal sexual relationships in the long-term that are necessary for establishing healthy marriages and families, the foundation of our society. Today's youth now have 24/7 access to infinite pornographic content at their fingertips. They don't even have to go looking for it - social media is often the entry point to pornographic sites, and they themselves distribute, and even create, pornographic content. A massive experiment is being conducted on today's youth and children—but without parental consent. The time is now to act to do all we can to give parents the power to restrict access to pornography for their children. The Supreme Court has recognized on multiple occasions that the government has a "compelling government interest" to protect the physical and psychological well-being of minors, which includes shielding them from "indecent" content that may not necessarily be considered "obscene" by adult standards. This report outlines three legislative approaches the federal government can take to limit children's access to pornography.

1 Gobry, Pascal-Emmanuel, "A Science-Based Case for Ending the Porn Epidemic," American Greatness, December 15, 2019, https://amgreatness.com/2019/12/15/a-science-based-case-for-ending-the-porn-epidemic/

## 1. Age Verification Law

The federal government could try again with what the overturned Child Online Protection Act (COPA) attempted: age verification for sites that distribute pornography. Congress could require interactive computer services[2] that in the regular course of their trade or business, create, host, or make available obscene, child pornography, or harmful to minors content provided by a user or other information content provider, to adopt and operate age-verification measures on their platforms or websites to ensure that users of the platform are not minors.

Such a law could: (1) require such interactive computer services to adopt age verification measures with clear metrics and processes to independently verify that the user of a covered platform is not a minor; (2) permit such interactive computer services to choose the best verification measure for their service that ensures the independent verification of users, provided that the verification measure chosen by the service effectively prohibits a minor from accessing the platform or any information on the platform that is obscene, child pornography, or harmful to minors. Such verification measures could include adult identification numbers, credit card numbers, bank account payment, a driver's license, or other identification mechanism.

The law could also impose a civil penalty for any violation of the law, and each day of the violation could constitute a separate violation of the law. The statute could also include a private cause of action, or perhaps a class action, as an enforcement mechanism where, for example, parents could sue for damages for the exposure of their children to dangerous material. A website distributing material harmful to minors without an age-verification system could result in a per-violation fine defined as the number of times a child accessed harmful content. Enforcement could also be given to a regulatory agency.

Concededly, this approach involves an effort to control online pornography that the Supreme Court previously has rejected. In Ashcroft v. Am. C.L. Union, 542 U.S. 656, 668 (2004), the Court struck down a similar age-verification requirement for internet sites on the grounds that filtering was more effective and less restrictive than age verification. Nonetheless, another attempt at age-verification is now warranted. Ashcroft's reasoning depends upon the claim that filters are more effective than age-verification in blocking pornography. Nearly twenty years of experience undermines that assumption. Parents have difficulty using and maintaining filters—and devices are not designed to make filtering technologies easy to use or maintain. Given the current state of the internet and the growing acceptance of paywalls and other types of restrictive access, courts may be willing to revisit its conclusion concerning the relative effectiveness and restrictiveness of age-verification versus filtering technologies.

## 2. Amend the Child Online Privacy Protection Act (COPPA)

The extraordinary amount of information that the major internet platforms appropriate from our children and then use to track and market to them threatens the parental control and family autonomy. Yet, the only law that regulates this appropriation, the Child Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 et seq., is absurdly limited in its scope and lacks serious enforcement. COPPA prohibits internet platforms

2 "Interactive computer services" is a broad statutory term taken from the Communications Decency Act, 47 U.S.C. § 230(f)(2)("any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions"). The term includes most web sites that allow user input, search engines, and social media.

from collecting personally identifying information about children, but it only protects children 13 and under and lacks serious enforcement mechanisms. Indeed, under several court cases, the major internet platforms have used COPPA to restricts parents' ability to protect their children's privacy under state law.

In order to have teeth, COPPA should be amended to (i) change the definition of a minor from under 13 years old to under 18 years old; (ii) lower the liability standard from "actual knowledge" to "constructive knowledge"; (iii) include in personal identifying information any data obtained from collecting information from tracking children's internet use; (iv) allow for state private causes of action under state tort law; and (v) provide a private right of action.

First, in its original legislation, COPPA had the age set as 16 but at the last minute lobbying interests pressured legislators to change the effective age to 13. This last-minute caving to the internet giants reflects an unforgivable spinelessness on the part of Congress. Given the well-documented harm, particularly to minors, that social media causes, ranging from increased depression, suicide, mental illness and loneliness,[31] the platforms must not be able to collect information without parental consent. After all, the platforms use this information to better market themselves to children. A toothless COPPA renders parents impotent in preventing their children from exchanging their personal information in exchange for screen diversion—a transaction that only strengthens and empowers the platforms to further entice children to use their services. Amending COPPA to make the age 18, would only allow children on social media platforms with parental consent—returning to parents control over their children's well-being and mental health.

Second, COPPA only covers platforms that have "actual knowledge" that one of their users is underaged. This is the highest liability standard in tort and almost impossible to prove in a court of law because it requires that a plaintiff show that the platform's corporate organization as a whole had specific and certain knowledge that unauthorized, underaged individuals were using its platform. Changing this standard to "constructive knowledge" would make platforms responsible for what they "should know" given the nature of their business and the information they already collect from their users.

Third, COPPA was passed in 1998, a time at which the platforms could not track online behavior to the degree they now do. As a result, its definition of personally identifying information (PII) is quite limited, only including typical categories such as name, address, and email. Given that social media and other websites now obtain the most intimate information about children by tracking their internet viewing habits, PII in COPPA must be expanded to include the storing or analysis of data derived from children's internet usage.

Fourth, there is no private cause of action in COPPA. The Federal Trade Commission (FTC) can bring a deceptive trade practice enforcement action. But a private cause of action, with perhaps the express possibility of class actions, would wield a larger, sharper sword in defense of children's privacy.

Fifth, Congress could amend the statute to eliminate COPPA's preemption provision. Under the current version of the statute, COPPA preempts state torts alleging invasion of privacy. Or, at least, that is how courts interpret the statute.[4]

---

3 Haidt, J., & Twenge, J. (2021). Social media use and mental health: A review. Unpublished manuscript, New York University. Accessed at: https://docs.google.com/document/d/1w-HOfseF2wF9YIpXwUUtP65-olnkPyWcgF5BiAtBEy0/edit

4 "The Court agrees that under the principle of express preemption, Plaintiff's state law claims are preempted." See New Mexico ex rel. Balderas v. Tiny Lab Prods., 457 F. Supp. 3d 1103, 1120 (D.N.M. 2020), on reconsideration, No. 18-854 MV/JFR, 2021 WL 354003 (D.N.M. Feb. 2, 2021).

## 3. Filter Law

Content filters can block access to content on the internet harmful to children. States could pass laws requiring computer and smartphone companies to pre-install filters on all devices they sell that access the internet. These filters would not be easily turned off, relying on techniques that maximize parental control, such as only providing codes to adults (age-verified) who want to deactivate them.

This is what the state of Utah has done. Utah passed a law aimed at making mobile devices automatically filter pornography. The law requires mobile devices to "automatically enable a filter capable of blocking material that is harmful to minors." Utah's H.B. 72 mandates active adult content filters on all smartphones and tablets sold in Utah. Phone makers would provide a passcode to let adult buyers disable the filter. If a filter isn't automatically enabled when a user activates the device, its manufacturer can be held legally liable if a minor accesses harmful content, with a maximum fine of $10 per individual violation.

Apple and Google both offer parental controls on iOS and Android devices, but they're turned off by default. Filters are too complicated to activate, so many parents struggle to know how to turn the filters on appropriately to keep their kids safe from any material. Thus, a filter law is aimed at making companies automatically enable them and add barriers to turning them off. Such a law would not limit in any way an adult's ability to turn the filters off to have any content they choose; it only helps parents keep their children safe, and it passes constitutional muster because adults are able to deactivate the filters. Adults can be given a code to turn off the filters once they prove their age. The law would not apply to devices already owned and in use, nor would it require individual tracking for compliance.

The Supreme Court repeatedly has looked to filters as a constitutional method of protecting children from harmful online content.[3] Filtering technologies, though, have not been very effective to date in protecting minors from accessing online pornographic content, as mentioned above. There are more hopeful possibilities emerging recently.6 But part of the reason filter technology has not developed well is there has not been demand to drive investment in improving filters. Part of the benefit then of a mandatory filter law is creating the level of interest and demand necessary to improve the quality of filters, incentivizing better development, and kicking off a virtuous cycle, where demand increases, quality improves, filters become used more, leading to further demand, etc. The Supreme Court, however, has never ruled on a default filter with an age-verification system to deactivate it, so this is new legal territory. Given that the Supreme Court has supported the use of filters, it seems that this new extension would pass constitutional muster.

---

3 See also Ashcroft v. Am. C.L. Union, 542 U.S. 656, 668 (2004) ("Filters are less restrictive than COPA. . . . Filters also may well be more effective than COPA. . . . By enacting programs to promote use of filtering software, Congress could give parents that ability without subjecting protected speech to severe penalties. . . . the Commission on Child Online Protection, a blue-ribbon Commission created by Congress …. unambiguously found that filters are more effective than age-verification requirements.")