

What States 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 four main legislative approaches states 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. Filter Laws

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.

The State of Utah has already passed such a law. It aims 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. (“Content that is harmful to minors, is defined in Utah as some form of “nudity, sexual conduct, sexual excitement, or sadomasochistic abuse,” which when “taken as a whole does not have serious value for minors.”)

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, the law is aimed at making companies automatically enable them and add barriers to turning them off. The Utah law unfortunately doesn’t take effect though until five other states pass equivalent laws. If none pass before 2031, the law will automatically sunset.

The 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 harmful material from children, 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 on-line content.² Filtering technologies though have not been very effective to date in protecting minors from accessing online pornographic content.

There are more hopeful possibilities emerging recently.³ 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 mandatory filter laws 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.

² 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.”)

³ Canopy, <https://canopy.us/>, has a SafeSmart Internet Filter that uses artificial intelligence to scan, detect, and eliminate explicit content on web browsers in milliseconds, before it reaches the screen. The filter blocks inappropriate images and videos in web browsers, replacing them with harmless white rectangles. It makes real-time decisions about content, and doesn’t rely on an incomplete or outdated list of inappropriate sites.

2. Age-Verification Laws

State legislatures could pass laws to require interactive computer services⁴ that are in the regular course of the trade or business to 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 or harmful to minors, including child pornography. 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. It 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.

This approach does present some constitutional risks. *Ashcroft v. Am. C.L. Union*, 542 U.S. 656, 668 (2004) struck down a similar age-verification requirement for internet sites on the grounds that filtering was more effective and a less restrictive means than age verification. However, given that filters in their current form have not been the most effective in limiting the availability of pornography and 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 this conclusion.

3. Broadband bills that require (or prioritize) companies to add a default pornography filter to their internet services.

States could pass a law that requires broadband companies to make users opt in to receive pornography channels/streaming through the company. States could regulate pornography at the Internet Service Provider level by passing a law requiring ISPs in their state to provide a default version of the Internet that is filtered of indecent content, while allowing adult users the ability to opt in to an unfiltered version of the Internet.⁵ The ISP would be required to set up an opt-in system, using a ratings system that provides differently filtered versions of the Internet with a default pornography-free setting of 16+.

⁴ “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”). It is a broad term that includes most web sites.

⁵ There are potential First Amendment concerns here. On one hand, the federal government can condition speech restrictions on the receipt of financial support. Constitutional. *Rust v. Sullivan*, 500 U.S. 173, 181 (1991). On the other hand, government has limited power to censor or control speech that it plays a role in creating. See *Denver Area Educational Telecommunications Consortium, Inc.*, 518 U.S. 727, 744 (1996).

This past legislative session in Texas, House Bill (HB) 5 — which would create a Broadband Expansion Office tasked with awarding federal money to contractors who agree to expand internet access to underserved areas — tacked on an amendment to prioritize contracts for companies that agree to add a pornography filter to their services. Offered by Rep. Jeff Cason (R-Bedford), the amendment reads, “The office shall ... prioritize an applicant that the broadband provided by the applicant will maintain a program to, by default, block access to pornographic or other obscene materials.” While the final version passed did not contain this amendment, it serves as a possible legislative model for other states to use or for Texas to try to pass again.

4. Taxes on commercial websites conditioned on effective measures to protect children from obscene and harmful content.

States could use their power of taxation to encourage websites and social media firms to adopt child-friendly policies. As a general rule, states have been hesitant to impose taxation on social media firms. This hesitance stems from the constitutional problems that present themselves whenever a state taxes an entity located outside its borders, as well as the Internet Tax Freedom Act (ITFA), which prohibits taxes on “internet access” and “discriminatory taxation.”⁶ A properly written state tax, however, could avoid these obstacles. Significantly, the tax could apply only to websites above a certain size and states could impose the tax obligation only on sites or platforms who have not put effective measures in place to protect children from obscene and harmful content.

The landmark Supreme Court case *South Dakota v. Wayfair, Inc.*⁷ eliminated the requirement that an entity must have a physical presence in the state as a condition for a state to require such entity to remit taxes on the sale of good and services sold therein. Rather, the constitutional power of the states to impose taxes is limited by the *Complete Auto Transit* case which holds that “state taxes, which will be sustained so long as they (1) apply to an activity with a substantial nexus with the taxing State, (2) are fairly apportioned, (3) do not discriminate against interstate commerce, and (4) are fairly related to the services the State provides.”

Several types of taxes could satisfy the *Wayfair* requirements. A state could impose a tax on revenue associated with advertisements read within or aimed at the particular state, or a state could impose a per subscriber tax. If particular advertisements were aimed at multiple states, there would need to be some sort of apportionment principle so that they apply equally to entities within and without the state—and could only be applied to advertisements directed at the state or its citizens. Another way to avoid the discriminatory tax concern would be to have a state charge major interactive service providers a quarterly fee on their active in-state users. This would avoid discrimination issues. States would estimate the number of platform users either using existing commercially available services or conducting their own surveys, though administrative records could also be used.

There is one last obstacle for a state tax on the platforms. ITFA prohibits states from taxing “internet access.” Because ITFA’s definition of “internet access” encompasses most online platforms⁸, ITFA would prohibit taxing the social media platforms. Fortunately, there is an exemption. ITFA expressly permits state fees that

⁶ Pub. L. No. 105-277, 112 Stat. 2681-719 (1998).

⁷ 138 S. Ct. 2080, 585 U.S. ____ (2018).

⁸ See 47 U.S.C. § 151 (“The term ‘internet access’ – (A) means a service that enables users to connect to the Internet to access content, information, or other services offered over the Internet ... (E) includes a homepage, electronic mail and instant messaging (including voice- and video-capable electronic mail and instant messaging), video clips, and personal electronic storage capacity, that are provided independently or not packaged with Internet access.”).

fund universal service programs.⁹ Provided a state has such a program — and the overwhelming number of states do — taxes on social media sites could be used to expand broadband access and other communications services.¹⁰

Such a fee on active in-state users or a tax on advertisement revenue thus could be imposed upon social media or internet firms, again using the “interactive computer services” definition discussed above (Note 2), but only on those firms above a certain number of in-state subscribers or annual revenue. Lastly, the tax could be conditional upon a firm’s successful adoption of an effective system to protect minors from obscene and harmful content. If the firm has an effective system, it would be exempt from the tax, so it would only be imposed on companies that had failed to set up adequate protections. Metrics for “success” to determine whether a firm’s system is effective could be adopted by law or regulation, perhaps in the state revenue code.

⁹ See 47 U.S.C. § 151, note (“Nothing in this Act shall prevent the imposition or collection of any fees or charges used to preserve and advance Federal universal service or similar State programs ... authorized by section 254 of the Communications Act of 1934 (47 U.S.C. 254).”).

¹⁰ FCC Commissioner Brendan Carr recently proposed extending federal universal service fees to tech platforms on this basis (Federal Communications Commission, Carr Calls For Ending Big Tech’s Free Ride On The Internet, May 24, 2021).