PROTECTING TEENS FROM BIG TECH

Five Policy Ideas for States

Clare Morell
Adam Candeub
Jean Twenge
Brad Wilcox

August 2022
ABOUT THE AUTHORS

Clare Morell is a policy analyst at the Ethics and Public Policy Center, where she works on the Technology and Human Flourishing Project. She worked in the White House Counsel’s Office and the Justice Department during the Trump administration.

Adam Candeub is currently Professor of Law at Michigan State University, where he directs its IP, Information and Communication Law Program, and is a Senior Fellow at the Center for Renewing America. Prior to joining MSU, he was an advisor at the Federal Communications Commission. In 2019, he served in the Trump administration as Deputy Assistant Secretary of Commerce for Telecommunications and Information and as Acting Assistant Secretary. He later joined the Department of Justice as Deputy Associate Attorney General.

Jean M. Twenge is a Professor of Psychology at San Diego State University and is the author of iGen: Why Today’s Super-Connected Kids Are Growing Up Less Rebellious, More Tolerant, Less Happy—and Completely Unprepared for Adulthood. She holds a BA and MA from the University of Chicago, and a Ph.D. from the University of Michigan.

Brad Wilcox is the Future of Freedom fellow at the Institute for Family Studies, visiting scholar at the American Enterprise Institute, and the director of the National Marriage Project at the University of Virginia. Wilcox has published widely on marriage, cohabitation, fatherhood, and the welfare of children.

ACKNOWLEDGEMENTS

The conclusions and recommendations in this legislative brief are those of the authors alone and do not necessarily reflect the opinions of our sponsor or advisers. The authors wish to acknowledge the arguments and insights put forward by Thomas D. Lehrman and Brad Wilcox in a WSJ op-ed entitled, “No Instagram or TikTok Without Parental Consent,” as well as the guidance and direction of Michael Toscano, who facilitated the brief’s production. We would also like to acknowledge the Center for Renewing America, which helps support Adam Candeub’s research on technology policy. This brief was edited by Alysse ElHage and designed by Matthew Minsk.
Introduction

Around 2012, something began to go wrong in the lives of teens. Depression, self-harm, suicide attempts, and suicide all increased sharply among U.S. adolescents between 2011 and 2019, with similar trends worldwide. The increase occurred at the same time social media use moved from optional to virtually mandatory among teens, making social media a prime suspect for the sudden rise in youth mental health issues.

In addition, excessive social media use is strongly linked to mental health issues among individuals. For example, teens who spend five or more hours a day on social media are twice as likely to be depressed as those who do not use social media. Several random assignment experiments demonstrate that social media use is a cause, not just a correlation, of poor mental health.

One possible mechanism is sleep deprivation. Teens who are heavy users of social media sleep about an hour less a night, and sleep deprivation is a significant risk factor for depression among adolescents. Between 2011 and 2016, as social media became popular, sleep deprivation among U.S. teens increased by 17 percent.

Thus, there is ample evidence that social media use is harmful to the mental health of teens. However, social media use is virtually unregulated among minors. This failure stems mainly from U.S. Supreme Court decisions, at the infancy of the world wide web, that limited Congress’s power to regulate the Internet to protect children. In addition, Congress has been unable to pass enforceable laws to protect kids online, and the laws it has managed to pass have mostly backfired.

In the 1996 Communications Decency Act, Congress prohibited the “knowing transmission of obscene or indecent messages to any recipient under 18 years of age,” or the “knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age.” However, in Reno v. ACLU, the Supreme Court struck down this provision, finding its prohibitions so vague that they would limit First Amendment-protected speech. However, Reno rested on several factual grounds that now seem quaint—if not tragically wrong—suggesting that the Court might reconsider its ruling. To take one such example, the Court found that:

- the Internet is not as ‘invasive’ as radio or television… [and] that [c]ommunications over the Internet do not ‘invade’ an individual’s home or appear on one’s computer screen unbidden.
- Users seldom encounter content by accident… [and] odds are slim that a user would come across a sexually explicit sight by accident.

In 1998, Congress tried again to protect children from harmful content online with the Child Online Protection Act (COPA). It required age-verification for minors visiting sites with material “harmful to children.” The Supreme Court, in Ashcroft v. ACLU, struck down this statute on the grounds that “filters are more effective than age-verification requirements” and would place a lesser burden on First Amendment rights. However, filters have since not proved particularly effective at protecting kids from harmful and obscene content online. (COPA never ended up taking effect, as three separate rounds of litigation led to a permanent injunction against the law in 2009.)

Lastly, Section 230 of the Communications Decency Act of 1996 was passed to “protect children from sexually explicit internet content.” (This portion of the law was not challenged in Reno v. ACLU.)
Thus, Section 230 was meant to not only be a shield for internet service providers but also a sword against illicit content, allowing platforms to remove content like pornography to protect children, without being held liable for doing so. The statute’s Good Samaritan provision, Section 230(c)(2), explicitly protects internet platforms, including social media platforms, from liability for removing any “obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable” content.\(^6\)

However, several court rulings have unreasonably expanded Section 230 to protect (1) social media companies from liability for their users’ posts and activities, even if social media companies know about users’ unlawful content, and (2) nearly all social media’s content moderation decisions, even if they have nothing to do with the types of content that section specifies.\(^7\) On net, therefore, Section 230 is all carrot and no stick when it comes to preventing harm to children. It has encouraged platforms to moderate content in ways that best fit their own financial interests but has not led to family-friendly online environments.\(^8\)

On a more fundamental level, the federal government’s historical focus on communications regulation is not addressing the challenges that social media present to society. From the government pressure throughout the 20\(^{th}\) century on the motion picture industry and broadcasters, to current FCC indecency regulations, government efforts have focused mainly on limiting harmful content.\(^9\) Federal law has not focused on the unique disruption to children’s psychological development that social media’s pervasive presence appears to cause.

The Children’s Online Privacy Protection Act (COPPA) of 1998\(^10\) is a notable exception. In theory, it is supposed to allow parents to control the interaction between websites (which now include social media platforms) and children, but due to several loopholes, it fails. In fact, because it preempts state torts in the area of children’s online privacy, it is arguably worse than nothing.\(^11\)

While waiting for Congress to pass better legislation to protect children online—most importantly by updating COPPA—states can take action now to protect children online and empower parents. This memo outlines five legislative strategies states can take toward these ends.

### 1. Mandate Age-Verification Laws

#### A. AGE-VERIFICATION FOR PORN WEBSITES

Under current law, age verification requirements for minors visiting pornographic sites are unconstitutional. Because the Supreme Court found that “filters are more effective than age-verification requirements,” it struck down COPA,\(^22\) which required sites with material “harmful to children” to obtain age verification.\(^23\) Given the manifest ineffectiveness of filters and the changed technology of smartphones, however, the Supreme Court might now revise its decision. A state law could prompt that change by specifically challenging the precedent set in Ashcroft.

State legislatures could pass laws to require interactive computer services in the regular business of creating or hosting obscene content, child pornography, or other content harmful to minors to operate age verification measures on their platforms or websites to ensure that any users of the platform in that state are not minors. Such a law could: (1) require such interactive computer services to adopt age verification measures that independently verify that the user of a covered platform is not a minor (i.e. it would not be sufficient for someone to type in a birth date; to independently verify
would require them to use other means to confirm a user is not a minor); (2) permit interactive computer services to choose the best verification measure for their service that ensures the independent verification of users and effectively prohibits minors from accessing it.

Such verification measures could include adult identification numbers, credit card numbers, a bank account payment, a driver’s license, or another 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. 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 face a per-violation fine defined as the number of times a child accessed harmful content (see more about possible enforcement mechanisms and damages below in number 5).

B. AGE-VERIFICATION FOR SOCIAL MEDIA PLATFORMS

States could also pass an age-verification law to require social media platforms to verify the age of any users in that state so that no minors under the age of 13 could create social media accounts. Under current federal law, COPPA prohibits internet platforms from collecting personally identifying information about children ages 13 and under. Platforms therefore are allowed to collect data on anyone over the age of 13 without parental consent, and since their business model operates off the collection of user data, they have set the age at 13 for creating an account. (In its original legislation, COPPA set the age at 16, but at the last-minute, lobbying interests pressured legislators to change the age to 13). Increasingly, children younger than 13 are gaining access to social media, and these younger children are more vulnerable to its harmful mental health effects. For example, Facebook’s internal research showed that Instagram had the largest negative effects on the body image of younger teens, and links between social media use and poor mental health are also more pronounced among younger teens. Age-verification would help ensure the current age limit is effectively enforced.

States could also require social media platforms to independently verify the age of its users in the state, which means potential users could not just enter a birth date in a text box (a very low barrier that children can easily get around) but would have to adopt age-verification measures to independently verify a user’s age. Such measures could include a driver’s license, a passport, a birth certificate, or a signed, notarized statement from a parent attesting to a minor’s date of birth, for example. Social media companies have considerable resources to employ toward instituting robust processes for verifying the age of users and would be more incentivized to do so if they were held liable.

To date, companies have had few incentives to require robust age-verification because they have not been held liable for minors under age 13 being on their platforms. That occurs because COPPA currently only covers platforms that have “actual knowledge” that users are underage. This is one of the highest legal liability standards 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 (i.e., the platforms would essentially have to have people’s birth certificates in hand to be liable for knowing a minor was on the platform). If Congress changed COPPA’s standard to “constructive knowledge,” it would also help this issue by making platforms responsible for what they “should know,” given the nature of their
business and the information they already collect from their users. This would incentivize them to prevent minors under age 13 from accessing their platforms.

2. Require Parental Consent for Contractual Offerings Over the Internet for Those Under the Age of 18

States dissatisfied with the current de facto age of 13 (due to COPPA) for social media could take a further step. Contract law is, for the most part, state law, and so states could prohibit a social media company or website from offering any account, subscription service, or contractual agreement to a minor under 18 years old in their state, absent parental consent.

This law would be quite controversial, but it stands on firm First Amendment grounds. As a general rule, all contracts by a minor with certain exceptions are voidable. And even though a minor can void most contracts he enters into, most jurisdictions have laws that hold a minor accountable for the benefits he received under the contract. Thus, children can make enforceable contracts for which parents could end up bearing responsibility, so, it is a reasonable regulation that parental consent would be required for such contracts.

Furthermore, while few courts have addressed the question of the enforceability of online contracts with minors, the handful of courts that have done so held the contracts enforceable on the receipt of the mildest benefit. Therefore, parents have an undeniable interest in controlling when and with whom children enter into contracts.

Further, at least in the context of solicitations by mail, the Supreme Court has upheld laws that allow parents to prohibit mailings from sources known to send sexual or otherwise non-family friendly solicitations. In *Rowan v. U.S. Post Off. Dept.*, the Supreme Court upheld Title III of the Postal Revenue and Federal Salary Act of 1967, under which a person may require that a mailer remove his name from its mailing lists and stop all future mailings to the householder. The law was

> a response to public and congressional concern with use of mail facilities to distribute unsolicited advertisements that recipients found to be offensive because of their lewd and salacious character. Such mail was found to be pressed upon minors as well as adults who did not seek and did not want it.

It would seem that if parents can prevent a mailer from sending solicitations to their kids, state laws could require parents to approve any online contractual offer.

The effect of such a law could be significant. When individuals join social media websites or use most commercial websites, they agree to terms-of-service, which are binding contracts. Depending on the sanction for forming such a contract without parental consent (see number 5 below for guidance on sanctions), these laws could change the way web sites function. If the sanction is severe enough, it could also effectively force web sites to verify users’ age, to ensure that parental consent is being given for any account formed by an individual under age 18.
3. Mandate Full Parental Access to Minors’ Social Media Accounts

States could also pass laws requiring social media platforms to give parents or guardians full access and control of all social media accounts created by minors between the ages of 13 and 17. While a state may not want to take on the challenge of enacting a complete ban on social media use for minors (see bonus option below), states could at least mandate that social media companies give parents full access to minors’ accounts so parents are able to see all that their children are doing online.

While this idea is distinct from the second recommendation above, it would also effectively mean that all minor social media accounts would have to be created with the parent’s full knowledge and approval, since the parent would have to be given access and included on the account with the child. Requiring companies to make the default setting of any minor account to be full parental access and control, with an option for parents to opt-out if they wanted to, would ensure that parents have the control of their minor’s account settings so they can restrict the privacy of the account, approve or deny friend requests, and set daily time limits for how long and when the child can be on the account.

Full access would most importantly allow parents to know exactly what their child is doing online, who they are interacting with, direct messages they are exchanging, and what they are posting and seeing, so they can protect them accordingly. While parents can currently utilize various private, for-purchase parental control apps (like Bark, Qustodio, or Circle, for example) to monitor their children online, certain social media apps are not able to be covered, like TikTok, or parents are unable to fully monitor all aspects of the account. Government intervention is needed to provide parents’ full, unrestricted access, and to empower all parents, not just those able to afford a private control option, to better protect their children.

Most importantly, the accounts would no longer require minors to grant their parents access, the way many of the platforms’ current parental control options do. For example, Meta currently insists on teens’ granting permission for parental controls to be enabled (and teens can revoke them at any time). Rather, states could pass laws so that permission flows from the parent to the child, not the other way around. This would empower parents with the knowledge needed to have proactive conversations with their kids about what they may be encountering on social media. It would help ensure that parents are still the primary authority in children’s lives rather than social media influencers.

4. Enact a Complete Shut-down of Social Media Platforms at Night for Kids

States could also pass a law requiring social media companies to shut down access to their platforms for all 13- to 17-year-olds’ accounts in that state during bedtime hours. Then, minors would not be able to access social media from, for example, 10:30 PM to 6:30 AM, to align with the usual nighttime sleep hours of teens. This would ensure teens could get a full eight hours of sleep or more at night without the temptation to stay up late on social media. Parents, of course, could use parental controls (see recommendation number 3) to set further time restrictions for their child, but at the very least, companies would be required to shut down all access to their platforms for minors during nighttime sleep hours.
While various private parental control apps, as mentioned in number 3, already allow parents to set time restrictions and down times for certain websites and apps, a complete nighttime shutdown for social media would empower all parents from having to fight one more battle over social media use by making it a non-option at night. The effects of nighttime social media use and the ensuing sleep deprivation are incredibly harmful for children and teens.

The law could be strengthened by also requiring the platforms to age verify (see recommendation number 1 above) in order to effectively enforce this curfew on 13 to 17-year-olds. The effectiveness of this law would turn on the sanction. The strength of the sanction would turn, of course, on the sanctions (size of fines) for violations, as well as on who can bring a suit for a violation (see recommendation number 5 for sanction options).

Given that states and localities may legally impose curfews on minors, a state law requiring a nighttime ban on social media would probably be acceptable.

5. Create Causes of Action for Parents to Seek Legal Remedies with Presumed Damages

Any law, such as the above four options, that a state passes to protect kids online should include a strong enforcement mechanism. In order for a law to be effective, it has to carry with it the real threat of holding social media companies accountable for any violation. We recommend that whatever laws are instituted also include a private cause of action to enable parents to bring lawsuits on behalf of their children against tech companies for any violation of the law. These companies aim to maximize profit, so there must be a sizeable enough threat to their profits in order for them to correct their behavior and follow the law.

Parents could be authorized to sue for damages for the exposure of their children to dangerous material. For example, when considering the four laws above, a parent could be empowered to sue respectively: (1) a website or platform for distributing material harmful to minors without having an age-verification system in place, or that is found to be guilty of allowing minors under the age of 13 on their platform; (2) a platform for creating an account for a minor without parental consent; (3) a platform that does not allow full parental access; (4) or a platform that allows minors on the platform during night hours. Along with the private cause of action, a law could also include the possibility for class actions.

Along with creating a private cause of action, these laws should also include and specify presumed damages. Given the difficulty of ascertaining the harm caused by any particular infraction of the above four laws mentioned, presumed damages might be essential to make these laws effective. For example, in the context of the Fair Credit Reporting Act of 1970 (FCRA), the Supreme Court ruled that violations of privacy procedural requirements must rise to the level of “a concrete injury even in the context of a statutory violation.” Without “concrete injury,” plaintiffs lack standing to sue in federal courts. Most state courts have similar standing requirements.

On the other hand, most courts likely would not place too high a bar for demonstrating “concrete injury” in the context of pornographic and other unlawful materials being displayed to minors. Unlike procedural violations of the FCRA, such as an incorrect zip code on one’s privacy notice, displaying pornography to a child would likely seem injurious to most people. Nonetheless, including presumed
damages in these laws—backed up with legislative findings about the costs of internet exposure in terms of increased psychological care, higher education costs, and lower educational attainment—would considerably strengthen any such legislation and its enforcement. For example, if a website or platform is shown to have violated the law, the damages owed could be a per-violation fine defined as the number of times a child accessed harmful content, or accessed the platform underage, or accessed it after hours, or without their parent fully on the account.

Bonus Proposal:
Enact a Complete Ban on Social Media for Those Under Age 18

This would be the boldest approach a state could take on protecting children from social media. But it is not unprecedented. Some states already place age restrictions on numerous behaviors known to be dangerous or inappropriate for children, such as driving, smoking, drinking, getting a tattoo, and enlisting in the military, among other things. Similarly, a state could recognize social media as a prohibited activity for minors.

Currently, the burden has been on parents to place limits on their children’s use of platforms and devices, but the problem of social media is no longer a private one. Social media use by even a few children in a school or organization creates a “network effect,” so even those who do not use social media are affected by how it changes the entire social environment. A collective solution to the problem that social media use poses for children is thus needed. We have enough evidence on the harms and dangers of social media use by children that a state would be well-justified in limiting social media by law to only adults, or at the very least to people 16 years and older. An across-the-board, enforceable age limit would place the burden where it belongs: back on the social media companies themselves who have designed their platforms to addict users, especially the most vulnerable, children.

As one scholar put it in National Review,

\[
\text{like an automobile, social media have both benefits and serious potential risks if used irresponsibly. Age limits would treat social-media platforms as tools that require some maturity and training to operate. Such forms of regulation are apolitical but would help parents in their efforts to keep kids safe, as driver’s licensing and seat-belt and liquor laws do.}^{37}
\]

A flat ban on social media use for children would present novel legal issues. It is hard to predict how a court would rule. Undoubtedly, the state has a right to regulate activities that are harmful to children. In Ginsberg v. New York, the Court upheld laws prohibiting the sale of obscene books to children. The Supreme Court has also upheld indecency regulations of broadcast radio and television with the goal of protecting children and the rights of parents.

On the other hand, the Supreme Court has recognized and upheld children’s First Amendment rights, famously remarking that “[i]t can hardly be argued that either students or teachers shed their constitutional rights to freedom of speech or expression at the schoolhouse gate.” It is not clear how a court would balance children’s First Amendment rights against society’s desire to protect them against social media’s harms.
Conclusion: States Must Take Action to Protect Teens

The federal government has not moved clearly and forcefully to address the harms poised by Big Tech to American teens. From surging rates of depression to suicide, American adolescents—and their families—are paying a heavy mental and emotional price for their use of social media. However, even in the face of mounting evidence that Big Tech is exacting an unacceptable toll on our teens, neither Congress nor the Courts have taken adequate steps to protect children from platforms that promote anxiety, envy, pornography, loneliness, sleeplessness, and suicide.

Thus, it falls to the states to step into the breach created by the federal government’s failure to act to protect children. In this report, we have detailed five discreet policy ideas—and one dramatic idea—that states should consider to help protect kids from the tentacles of Big Tech. At a minimum, state lawmakers should consider measures like requiring parental consent for minors to form social media accounts and shutting down social media platforms for minors at night. At maximum, states should consider prohibiting social media use for all those under 18 years old.

One day, we will look back at social media companies like ByteDance (Tiktok) and Meta (Facebook and Instagram) and compare them to tobacco companies like Philip Morris (Marlboro) and R.J. Reynolds (Camel). For a time, Big Tobacco enjoyed immense profits and popularity. But eventually, Big Tobacco’s culpability in causing immense physical harm to Americans—and in trying to obscure the science regarding that harm—became known. They were eventually held accountable for their deceptive advertising to children using “Joe Camel.” We are living at a moment when we are just learning of the social and psychological harms of social media, and of Big Tech’s efforts to obscure those harms from the public.

It now falls to a few pioneering states to inaugurate a new era of regulatory reform for Big Tech that treats the industry much like we now treat the tobacco industry. Given social media’s baleful influence on our children, we must pursue a range of creative legislative strategies to limit the industry’s power over America’s kids before it’s too late. This report provides a guide to at least five such possible strategies for state legislators who are serious about protecting children online.


4 Luby, J., & Kurtz, S. (2019). “Increasing suicide rates in early adolescent girls in the United States and the equalization of sex disparity in suicide: The need to investigate the role of social media.” JAMA Network Open 2, no. 5 (2019); Spiller, H. A.,
Protecting Teens from Big Tech: Five Policy Ideas for States


Id. At 871.


Gen. Steel Domestic Sales, L.L.C. v. Chumley, 840 F.3d 1178, 1181 (10th Cir. 2016), quoting FTC v. LeadClick Media, LLC, 838 F.3d 198, 173 (2d Cir. 2016).


Ashcroft v. Am. C.L. Union, 542 U.S. 656, 668 (2004). COPA used a definition of “harmful to children” that seemed quite similar to the Miller obscenity and the FCC’s indecency definitions: “any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that—

(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;

(B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.” § 231(e)(6); see Ashcroft v. Am. C.L. Union, 542 U.S. 656, 661-62 (2004).

When we refer to social media or social media platforms, we mean an Internet website or application that is open to the public, allows a user to create an account, and enables users to communicate with other users for the primary purpose of posting information, comments, messages, or images. The major platforms we have in mind today are Instagram, TikTok, Facebook, and Snapchat.

While not a state-level solution, as Chris Griswold has written in *National Affairs* (Griswold, C. “Protecting Children from Social Media,” *National Affairs*, No. 52, Spring 2022), the federal government could create a simple public system for age-verification that allows Americans to use the personal data that the government creates and maintains, like birth dates and Social Security numbers, to *anonymously* prove to a platform whether they exceed a given age. He writes, “one possibility would be for the SSA to offer a service through which an American could type his Social Security number into a secure federal website and receive a temporary, anonymized code via email or text, like the dual-authentication methods already in widespread use. Providing this code to an online platform could allow it to confirm instantly with the SSA whether the user exceeds a certain age without further personal data reaching the platform or the government.” The point is there are ways of independently verifying a user’s age without compromising user privacy if companies were required to do so.

§ 10:1. The right of a child to make contracts and disaffirm them, 1 Leg. Rts. Child. Rev. 3D § 10:1 (3d ed.)


397 U.S. 728 (1970)


Id. at 731.


Twenge, J. M. “Why increases in adolescent depression may be linked to the technological environment.” *Current Opinion in Psychology* 32 (2020): 89-94.


F.C.C. v. Pacifica Found., 438 U.S. 726, 750 (1978) (“The ease with which children may obtain access to broadcast material, coupled with the concerns recognized in Ginsberg, amply justify special treatment of indecent broadcasting.”)