

# Protecting Kids Online: Legislative Summary

**Adam Candeub**, Center for Renewing America  
**Clare Morell**, Ethics and Public Policy Center  
**Michael Toscano**, Institute for Family Studies  
*Endorsed by the Family Policy Foundation*

ETHICS  
AND  
PUBLIC  
POLICY  
CENTER  
*Shaping Policy,  
Renewing Culture.*



## Summary

---

In the past year, four states—Utah, Arkansas, Louisiana, and Texas—have passed social-media parental-consent laws based on ideas put forward in a joint report from the Ethics and Public Policy Center and Institute for Family Studies, titled “[Protecting Teens from Big Tech](#)” (August 2022). These laws have important differences. Some include requiring full parental access or certain parental tools, some limit certain features for minor accounts, and others provide expansive exemptions. The upshot of this is that some laws are stronger than others. Evaluating the different provisions is important, as these laws are being challenged in court. In light of recent litigation and other states’ desires to pass similar laws, Clare Morell, Adam Candeub, and Michael Toscano have put together a model bill for states to use, drawing on aspects of Utah’s initial legislation and incorporating key edits and provisions—based on the recent injunction against Arkansas’s law—to strengthen it against legal challenges. The underlying approach of their model bill—the same as the laws passed thus far—is to require (1) online platforms to age-verify their users in the respective state and (2) obtain parental consent for a minor to open or operate a social media account if a user is under the age of 18. The goal is to restore parental authority and rights over children’s online behavior.

## The Need for Legislation

---

These laws are needed because parents are effectively powerless to oversee their children’s online behavior, and there is a collective nature to the harms of social media. First, parents need help. Even the best parental-control software available for purchase does not offer full protection. Apps like TikTok or Snapchat don’t provide access to such external

controls, and certain app features, like Instagram’s direct messaging, are beyond a parent’s view. Given the lack of current requirements for age verification, a child can easily falsify his age and go behind his parents’ back to open social media accounts—or open secret secondary accounts of which parents are unaware. For parents to effectively oversee their children’s online behavior, meaningful age verification and parental consent over social media account formation are necessary. Second, the collective nature of the harms of social media necessitates public-policy solutions. Individual parents are powerless against mammoth Big Tech companies and face

enormous social pressure to allow kids access given the ubiquity of social media and their extensive use by school, sports, and other institutions and activities that are part of growing up in America today. These laws restore parental authority and provide parents a means of enforcement for age verification and parental consent. These laws open up channels of litigation for parents to hold platforms accountable, which have been closed to them till now.

## Components of the Model Bill

---

- The bill defines what platforms are covered by the law, focusing on social-media platforms and also including interactive gaming. Our model's definition is drawn from Texas's common carrier social-media law. This definition was upheld by the U.S. Court of Appeals for the Fifth Circuit, and, given a recent ruling from the Arkansas federal district court, is preferable to the definitions used in other social-media laws because it is content-neutral.
- It requires covered platforms to conduct age verification of their users and requires them to offer as many acceptable means as efficiently and practically possible, specifically mentioning methods for preserving user privacy against threats (e.g., biometric options are not required or mentioned in the bill), to avoid burdening adult speech.
- For users under the age of 18, "minors," the companies are required to verify and obtain parental consent, as well. The bill outlines acceptable means for obtaining such consent.
- The bill requires that all identifying information used to verify age or parental consent shall not be retained once access to the platform is granted. Companies will delete any such information, and if found retaining anything, are in violation of the law. This helps ensure user privacy.
- The model also recommends full parental access for minor accounts. This provides ongoing parental supervision, rather than a one-time grant of permission to open an account. Parental involvement, as the judge who enjoined the Arkansas law states, is key to protecting children online. If a state does not opt for full parental access, our model also includes a second option to, at minimum, mandate that platforms provide certain tools for parental supervision.
- Finally, the bill outlines enforcement mechanism options, either by state division or state attorney general's office. Whichever state enforcement chosen, our model recommends also including a private cause of action so parents can bring lawsuits on behalf of their children against tech companies for any violation of the law. These companies aim to maximize profit, so a sizeable threat to their profits is needed to correct their behavior and follow the law. The private cause of action should also include presumed damages. We recommend \$10,000 per incident of violation. Given the difficulty of ascertaining the harm caused by any particular infraction, presumed damages could be essential to make the laws effective. It should also be pointed out that if the statute *only* has a private cause of action, it will be much harder to challenge in court. A federal court [recently dismissed](#) facial challenge to Utah's age-verification for adult websites law precisely on that ground.

# Legal Rationale

---

The legal approach is innovative and defensible by drawing on contract law. Creating a social-media account and agreeing to its terms of service (TOS) is entering a contract. In fact, the companies typically state in the terms of service that their terms “form a legally binding agreement between you and us.” These TOS are comprised of technical jargon and important details cloaked in fine print that no child can understand. Children cannot form fully enforceable contracts, and given that they *can* create liabilities for the child and parent, states often require parental consent for entering into such contracts. These laws follow uncontroversial legal precedents requiring parental consent for tattoos or liability waivers and restore to parents what the Supreme Court has recognized as fundamental to our democracy: the power to control, even online, who educates our kids.

## Challenges to Overcome

---

### 1. Clarify the category distinction that these laws are not content-based restrictions but are fundamentally contract laws.

Just as states require parental consent for kids to sign liability waivers or life-insurance contracts, so states may require parental consent for the platforms’ terms of service that give away their kids’ rights to data, privacy, and a host of other legal rights. And, even though the platforms’ terms of service contract

involves “expression,” it does not fall out of the general rule that parents can control their kids’ contractual obligations. States routinely require parental consent for tattoos—and they are quite expressive (and First Amendment protected).

Furthermore, even if it is regulated speech, these laws are not content-based, but content-neutral. Social media, as media, regardless of the type of content, is inherently harmful. The research is clear. Its aggressive algorithms prey on children’s vulnerabilities. Children and teens suffer because they live in constant need of “likes” on their posts—a product design feature of these platforms. Social-media age verification does not target certain types of speech—it targets a form of communication that encourages social exclusion, competition for approval, and fear of isolation. These laws are thus not age-gating certain types of content like age-verification laws for adult websites, but seeking to guard children from the harms inherent to the design of these platforms by restoring parental authority. Social media age verification laws are narrowly tailored. Social media, as a form, is harmful to kids. These laws regulate that—and no more.

### 2. Defend parental authority over minors’ speech against arguments for the free speech rights of minors.

Justice Thomas has written that “the ‘freedom of speech,’ as originally understood, does not include a right to speak to minors (or a right of minors to access speech) without going through the minors’ parents or guardians.” Social media companies certainly do not have a First Amendment right to speak to children over parental objection, which is what is at issue, and this is precisely what social media companies have been getting away with. For example, 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, as in the case of *Rowan v. U.S. Post Office Department*.

It would seem that if parents can prevent a mailer from sending solicitations to their kids, state laws can require parents to have oversight of the communications their children are receiving and sending online. The Supreme Court in *FCC v. Pacifica Foundation* also upheld indecency regulations of broadcast radio and television with the goal of protecting children and the rights of parents to protect the sanctity of the family from inappropriate communications. The questionable and limited free speech rights of minors must not be elevated over parents' right to raise their children, a precedent recognized for a century in cases such as *Pierce v. Society of Sisters*.

### **3. Show these laws are not burdensome to adult speech and privacy (and be willing to challenge precedent).**

Clare Morell and John Ehrett published a [report](#) earlier this year on age verification to show there are methods that are both effective and that protect user privacy, such as a third-party conducting verification via a two-step process, or, even more securely, deploying cryptographic techniques like “zero knowledge proofs” to verify users. Adam Candeub recently published a [white paper](#) outlining these cryptographic techniques. These are readily available and pose minimal threat to user privacy or speech and can all be done in less than 60 seconds, rendering absurd the fear that such an anonymous process would chill adult speech. Anonymous authentication methods completely transform the First Amendment analysis for age-verification requirements. It is time to challenge the old age-verification precedents from 20 years ago; because of changes in technology, the factual predicates of those cases (*Reno v. ACLU* and *Ashcroft v. ACLU*) are no longer true. Age-verification is no longer burdensome on adults in terms of expense, trouble, and privacy. The more states that pass these laws, the better chance there is that the Supreme Court will revisit and correct these unhelpful precedents.

## **About the Authors**

---

**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.

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

**Michael Toscano** is executive director of the Institute for Family Studies. He has written on family policy, tech policy, the uses of technology to reshape work, and the effect of technological change on America's republican form of government. His writing has appeared in the *Wall Street Journal*, *Newsweek*, the *New York Post*, *First Things*, *Compact*, *The American Conservative*, *National Review*, and elsewhere.