Social Media: Rhetoric and Reality

Millions of teenagers across the United States access the internet and social media platforms daily. According to Pew Research, 97 percent of teenagers use the Internet daily, with 46 percent saying they use it almost constantly.¹ Both the internet and social media have become part of modern adolescence in a way that was not true for previous generations.

For most, these visits will be harmless—to catch up on the latest news, connect with friends and family, conduct research for a school project, or tweet their latest thoughts or feelings. But, unfortunately, while the vast majority will have a positive experience on social media, others will interact with cyber bullies, cyber criminals and, potentially, child predators.² Such dangers have led lawmakers across the political spectrum and at every level to propose legislation designed to keep teens safe online, particularly when using social media platforms.

Given the prominence of social media in daily life, fears have been raised about its effects on teens’ mental health. Experts have raised concerns about alleged links between social media and “depression, anxiety, and loneliness.”³ These fears came to a head in 2021 when, during the height of the COVID-19 pandemic and after the tumultuous 2020 presidential election, the Centers for Disease Control reported that 42 percent “of high school students felt so sad or hopeless almost every day for at least two weeks in a row that they stopped doing their usual activities” and 29 percent “of high school students experienced poor mental health.”⁴

As these concerns have proliferated, the links between social media activity and adverse mental health outcomes for teens are a subject of much debate as to the direct causal relationship, with writing and research offering differing conclusions as to the correlation.⁵ As noted by researchers at Harvard University, “the link between social media use and health is equivocal and inconclusive.”⁶ Without clear links, it’s possible that other factors are responsible for the decline of mental health among American teens and social media—given its widespread use—has become
a scapegoat for more complex factors. Further questioning the links between social media use and teenage mental health, the American Psychological Association notes “using social media is not inherently beneficial or harmful to young people,” but they do need to learn how to stay safe online.  

As noted by The Atlantic’s Derek Thompson, liberal teenagers could be feeling depressed or anxious over social issues such as climate change, school shootings, the perceived rise of anti-LGBTQ+ policies, or the continued specter of Donald Trump in American politics. 6 Conservative teens, on the other hand, would likely point to the “baleful effects of identity politics or the isolation created by Covid-era lockdowns.”

Another possible explanation is that the United States is experiencing another wave of poor teenage mental health. Researchers from the Center for Growth and Opportunity have noted that the recent CDC figures suggest “a trend” or “a cycle” of poor mental health. Specifically, Barkley and Rinehart show similar declines in teenage mental health in the 1990s and 2010s, well before the dominance of social media. 10

If the cause of declines in teenage mental health is more complex than simply social media or widespread internet usage, passing legislation to target these platforms will inevitably fail and cause more problems that exacerbate declines in teenage mental health.

In many ways, concerns surrounding teen use of social media mirror historical anxieties surrounding rock music. In 1984, a group of women dubbed the “Washington Wives” due to their connections to influential politicians founded the Parents Music Resource Center with the express aim of educating and “informing parents of this alarming new trend . . . towards lyrics that are sexually explicit.” 11 Similar to today’s anxieties over social media use, PMRC sought to “show the causal link between rock music and social problems,” such as poor mental health and an increasingly violent society. 12 While initially seeking to place rating stickers on albums, it became clear that PMRC’s “crusade was indeed a reactionary form of censorship” designed to shut down artists deemed obscene by the “Washington Wives” or that conflicted with traditional values. 13 As John Denver stated to the U.S Senate, any effort by the federal government to regulate music would amount to censorship and grant Washington the power to determine what is and what is not appropriate, not parents. 14

The Risks

While online safety bills are often well-intentioned, lawmakers’ desire to “do something” risks crafting legislation that disrupts the free market, undercuts entrepreneurship, grows the size and power of government, creates privacy and cybersecurity concerns, or violates constitutional protections of free speech. Additionally, passing onerous online safety bills risks putting the government in a co-parenting relationship with parents, something conservatives and advocates of limited government have historically condemned, especially when pushed by Democratic politicians. 15

As lawmakers in state houses across the country grapple with the issue of online safety, concerns must be addressed to ensure balanced legislation that does not create more problems than it solves and continues to empower parents to make choices about their teen’s digital and real-life lives.

When considering the risks of social media use, lawmakers must also acknowledge its benefits. For example, Pew Research notes that teens “credit these platforms with deepening connections and providing a support network when they need it.” 16 Pew’s findings dovetail with those of the American Academy of Pediatrics (AAP), whose research found that “adolescents use social media” and the wider internet “to develop and maintain friendships” and that this allows them to “understand their friends’ feelings and feel more connected to them.” Additionally, AAP found that social media can “provide a good forum to practice skills related to identity development, such as self-presentation and self-disclosure.” 17 Cutting off or heavily restricting teenage use of social media will ultimately deny them these benefits, further exacerbating any mental health issues they currently face.

Conservative parents should be especially concerned about how curtailing social media usage could affect their children. As school administrators and academic institutions take an increasingly left-wing turn, 18 social media and internet usage more broadly allows children to access Conservative viewpoints that they would otherwise be denied. In effect, curtailing social media and internet usage could deny children the opportunity to challenge the dominant left-wing ideology and have access to a community of like-minded conservative students.

The Federal Landscape:

Congress passed the Children’s Online Privacy Protection Act (COPPA) in 1998, recognizing the importance of keeping teens safe online. 19 When it took effect two years later, COPPA required the Federal Trade Commission (FTC) “to issue and enforce regulations concerning children’s online privacy.” Acting on its new mandate, the FTC required websites that collect personal information to:

1. Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children;
2. Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children;
3. Give parents the choice of consenting to the operator’s
collection and internal use of a child’s information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents);
4. Provide parents access to their child’s personal information to review and/or have the information deleted;
5. Give parents the opportunity to prevent further use or online collection of a child’s personal information;
6. Maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security;
7. Retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use; and
8. Not condition a child’s participation in an online activity on the child providing more information than is reasonably necessary to participate in that activity.20

Federal Proposals:

Recognition that COPPA was passed before many of today’s internet users were born has led to demands that Washington update online safety legislation to reflect contemporary internet usage. In 2021, Senators Markey (D-MA) and Cassidy (R-LA) proposed updating COPPA by passing the Children and Teens’ Online Privacy and Protection Act (CTOPA), known colloquially as COPPA 2.0. Had Congress enacted CTOPA, it would have prohibited “internet companies from collecting personal information from anyone 13- to 15-years old without the user’s consent; creating an online ‘Eraser Button’ by requiring companies to permit users to eliminate personal information from a child or teen; and implementing a Digital Marketing Bill of Rights for Minors that limits the collection of personal information from teens.”21 While the bill enjoyed bipartisan support and cleared the powerful Senate Commerce Committee, it never received a vote in the full Senate and subsequently died.

Other federal proposals include Senators Richard Blumenthal (D-CT) and Marsha Blackburn’s (R-TN) Kids Online Safety Act (KOSA). Had Congress passed KOSA, it would have created a duty of care for social media platforms, required platforms to “perform an annual independent audit assessing risks to minors,” and given minors “options to protect their information, disable addictive product features, and opt-out of algorithmic recommendations—and requires platforms to enable the strongest set-

While well-intentioned, KOSA would have curtailed digital freedoms for adults and left teens no safer online. As noted by the Family Online Safety Institute (FOSI), provisions in KOSA “could easily become surveillance controls.”23 FOSI continued, warning that for older teens, these tools could deny them access to “vital information” on a range of important developmental topics as well as the ability to “privately and anonymously report domestic abuse in their household.”24

As noted by TechFreedom, KOSA would have created an unconstitutional age verification regime, mandated an unworkable and unconstitutional duty of care that would have threatened adults’ first amendment rights by limiting speech that Americans are constitutionally permitted to receive.25

Limiting speech that Americans are constitutionally entitled to receive is problematic because the Supreme Court ruled in 1997 that the Communications Decency Act was unconstitutional as it “placed an unacceptably heavy burden on protected speech.”26 KOSA would likely have suffered the same fate had Congress enacted it.

After the previous iteration of the bill failed to gain traction in the 117th Congress, Senators Blackburn and Blumenthal reintroduced KOSA in April 2023. Despite claiming they had addressed flaws in the bill, civil liberties groups have continued to warn that the legislation would “expose the very children it seeks to protect” to a range of avoidable dangers.27 TechFreedom maintained its criticisms, arguing that “KOSA remains a ham-fisted approach that will do much more harm than good, and make the Internet worse for everyone.”28

Senator Josh Hawley (R-MO) has also proposed a federal online safety bill. Hawley’s Making Age-Verification Technology Uniform, Robust, and Effective Act (MATURE Act) would prohibit those under 16 from operating a social media account and require platforms to verify the age of all users by requiring users to provide an image of a government-issued identification document.

Senator Hawley’s proposal, while well-intentioned, is hazardous because the requirement that platforms age-verify users with government-issued ID risks creating a vast database of sensitive information for cybercriminals and denying millions of teenagers the potential benefits of intelligent social media use. Additionally, teenagers under 16 still enjoy First Amendment rights that would almost certainly be denied if they were prohibited from accessing social media platforms.

Another federal proposal that has raised alarm bells is Senators Graham (R-SC) and Blumenthal’s Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT). While the premise of the bill is to “encourage the tech industry to take online child sexual exploitation seriously,”29 the provisions of the bill could have profound implications for users’ privacy and
growing the federal government's power over individuals' digital lives. Specifically, EARN IT would remove Section 230 liability protection for platforms where Child Sexual Assault Material (CSAM) is hosted. Secondly, EARN IT "removes the federal knowledge standard for child sexual abuse materials, making it easier for courts to make the argument that a tech company was negligent in offering encryption because it knew it could be used to transmit child sexual abuse materials."

Concerns have been raised that removing liability protections and altering the federal knowledge standard could force platforms to end encrypted messaging services and require them to scan all messages between users, virtually eliminating any prospect of privacy online. It's also possible that by removing liability protections, state and federal authorities could use child safety as an excuse to pressure platforms to remove digital speech, denying Americans their First Amendment rights.

Illinois Senator Richard Durbin has also proposed his own legislation to combat CSAM. Entitled Strengthening Transparency and Obligation to Protect Children Suffering from Abuse and Mistreatment Act of 2023 (STOP CSAM Act), Durbin's bill would provide a private right of action for victims of CSAM to sue platforms that fail to remove CSAM material and expands the scope of mandatory reporting for platforms. While well-intentioned, the Center for Democracy and Technology has warned that increasing providers' incentives to over-report and over-remove people's online content, the STOP CSAM Act risks inundating NCMEC and law enforcement with useless reports, squandering resources that should be directed towards combatting child exploitation.

EARNIT and STOP CSAM also ignore the difficult work many private sector providers undertake to combat CSAM, placing them in legislative crosshairs, not bad actors. For example, the National Center for Missing and Exploited Children has reported that "in 2022, 99% of CyberTipline reports were submitted by" Electronic Service Providers. In 2022, Facebook made over 21 million reports to NCMEC, and Google filed over 2 million reports. Similarly, Twitter reports that it removed over 404,000 accounts from its platform that posted CSAM. Recognizing the work platforms are doing to fight CSAM, it should be clear to lawmakers that the target of any child online safety legislation should be criminals, not those making critical contributions to child safety.

The Growing Patchwork of Protections

With Congress failing to pass any meaningful updates to COPPA or establishing a minimum standard that applies across the board, it has increasingly fallen to state governments to enact legislation to keep teens safe online. Unfortunately, the movement away from Washington and toward state capitols risks creating a patchwork of legislation nationwide and a zip-code lottery of protections. Not only does such patchwork create uneven protections whereby a child in California enjoys greater protections than a child in neighboring Oregon, but it also raises compliance costs for businesses operating across state lines. The dangers of a state patchwork are most clearly evidenced in data privacy, where it costs small businesses $60,000 for every new state that enacts data privacy legislation. Large companies can meet this cost, but small businesses are left with a choice between raising prices or not operating in that state.

As state legislatures explore child safety measures, these protections will only become more uneven, and the cost of doing business will only increase, particularly for small and medium-sized enterprises.

California's Age-Appropriate Design Act

Due to the state's liberal political orientation, it's no surprise that California has taken the lead in passing onerous legislation under the guise of protecting teens online. In August 2022, for example, California enacted the California Age-Appropriate Design Code Act that places significant restrictions on "companies with respect to online products and services that are likely to be accessed by children under the age of 18." Specifically, the bill requires businesses to:

1. Configure all default privacy settings in the best interests of children.
2. Provide privacy information, terms of service, policies and community standards, using clear language suited to the age of the children
3. Estimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the business's data management practices, or apply the privacy and data protections afforded to children to all consumers.

The legislation also severely limits how private companies can use data collected on teens.

The restrictions imposed by California's Age-Appropriate Design Act present numerous issues. Firstly, because the legislation "deputizes online services to act as roving Internet censors at the
out First Amendment protections for adults and teenag-
media, they are also denied the ability to learn how to stay safe on
social media platforms, creating a generation of adults who don’t
know how to operate safely online.

Content Filters

One popular proposal that has emerged throughout state cap-
itals over the last year is mandating device manufacturers place
content filters on their devices to prevent teens from accessing
harmful material such as pornography. So far, only Utah has been
able to pass content filter legislation into law.46

While lawmakers across the country have been advocating for
this style of legislation, these proposals present numerous chal-
enges, both constitutionally and practically. Firstly, filtering con-
tent is likely unconstitutional because it could prevent adults from
receiving speech they are constitutionally entitled to receive.47
Secondly, mobile application developers have created thousands
of content filters available to consumers on either a free or sub-
scription basis. Such a wide variety of free and paid filters allows
consumers to select firstly whether they want a content filter and,
if so, which one best suits their needs. Mandating a content filter
would ultimately undercut these options.

Pillars of good policy:

1. Online Safety classes: Lawmakers must recognize that
even with outright bans, teens will access social media.
Lawmakers must also recognize that social media plat-
forms provide legitimate benefits for teenagers. Rather
than trying to stop access altogether, state lawmakers
can mandate social media or online safety classes that
educate teens about the dangers of social media and in-
ternet use and provide them with best practices for stay-
ing safe online.

2. Age verification for harmful content: In 2022, Louisi-
aana became the first state to require websites that host
harmful content, specifically pornography, to verify that
their users are over 18. While this approach is not per-
fected and may have some First Amendment concerns, it
only prevents teenagers from accessing harmful content
and ensures adults are still able to receive digital content
they are constitutionally permitted to receive. The Louisi-
aana law also prevents private companies from holding
on to government-issued identification, so it minimizes
cybersecurity risks.

3. Ensure that child safety proposals do not infringe on
constitutionally protected speech: While keeping teens
safe online is a noble goal, proposals must not infringe
on First Amendment protections for adults and teenag-

Outright Bans: Utah and Arkansas

While most state governments have considered legislation to
keep teens safe online, Utah and Arkansas recently passed legislation
that would severely restrict teens’ access to social media plat-
forms, potentially denying them access to social media’s identified
benefits and denying them an understanding of how to use social
media in an age-appropriate way.

Beginning in 2024, social media companies operating in Utah
will be required to “verify the age of a Utah resident seeking to
maintain or open an account and would require the consent of a
parent or guardian before a minor under age 18 could maintain
or open an account.”43 Such verification likely means presenting
government-issued identification documents such as a driver’s li-
cense, passport, or birth certificate.

Arkansas recently passed similar legislation, the Social Me-
dia Safety Act, into law.44 From September 1, 2023, social media
companies must "contract with third-party vendors to perform
age verification checks.” This likely means forcing individuals to
"upload a digital copy of a driver’s license or government-issued ID.”45 Anyone younger than 18 will be required to obtain parental
consent before opening an account.

Such heavy-handed restrictions pose several difficulties. First-
ly, requiring social media platforms to collect additional data on
parents and minors will create unnecessary cyber vulnerabilities
and a goldmine of sensitive data for cybercriminals. Secondly, de-
ning teens access to social media accounts could cut off support
services, including resources to help them escape abusive rela-
tionships or homes. Finally, when teens are denied access to social
ers. When lawmakers construct barriers to speech by requiring social media age verifications, they stifle online speech and deny Americans constitutional rights. Measures that infringe on the first amendment also risk forcing their state into expensive litigation that must be paid for by taxpayers.

4. **Ensure that teen safety legislation does not create cybersecurity vulnerabilities:** Efforts to keep teens safe on social media should not force Americans to hand over sensitive data or government-issued identification documents to private platforms or government agencies. Such requirements would only create a goldmine of sensitive information for cybercriminals.

5. **Target Bad Actors, Not Partners:** Social media platforms and websites can be vital partners in the fight against harmful content and CSAM. Any legislation designed to protect teenagers from online harm must target perpetrators, not platforms or websites that are reporting illegal content to law enforcement.

---

**References**


19 15 U.S. Code § 6501
24 Ibid.
28 Ibid.
30 Ibid.
35 Ibid.
36 Twitter Safety, Twitter Post, February 1, 2023. Available Online: https://twitter.com/twittersafty/status/1620908364543967232
39 Ibid.
40 NetChoice v. Bonta, Available Online: https://netchoice.org/netchoice-v-bonta/
41 Ibid.
44 Arkansas State Legislature, “SB396 - To Create The Social Media Safety Act; To Require Age Verification For Use Of Social Media; And To Clarify Liability For Failure To Perform Age Verification For Use Of Social Media And Illegal Retention Of Data.” Available Online: https://www.arksansonline.com/news/2023/apr/13/arkansas-governor-signs-social-media-bill/