ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

How to Address Children's Online Safety in the United States

ASHLEY JOHNSON I JUNE 2024

Protecting children from online harms requires a careful balance between ensuring safety and safeguarding free speech, user privacy, and parents' rights. The most effective approach would split responsibility between the government, parents, and online services.

KEY TAKEAWAYS

- Debates over how best to protect children are much older than the Internet, and the harms children face online are many of the same harms children face in the physical world.
- Existing federal legislation outlaws child sexual exploitation in both the physical and digital worlds and protects the privacy of children under age 13, while states have more recently passed laws imposing specific requirements on online services.
- Many of the current proposals to protect children online do not strike the right balance, overburdening parents or businesses or trampling on users' rights in the name of safety.
- A more effective approach requires regulation in areas such as privacy, digital identification, and child labor combined with industry-led efforts to give parents and children more control over their online experience.

CONTENTS

INTRODUCTION

Louisiana became the first state to pass a law, in 2022, mandating that websites containing at least one-third adult content verify their users' ages to ensure none are under 18.[1] Within a matter of months, other states followed, creating age verification requirements not just for adult websites but also for social media platforms. These laws reignited the debate surrounding children's safety online, raising questions of what potential harms children face in the digital world, whose job it is to protect children from those harms, and what form that protection should take.

Some child safety advocates argue that the Internet, and particularly social media, is responsible for a vast array of potential harms to younger users—including, but not limited to, bullying, addiction, sexual exploitation, and poor physical and mental health outcomes such as depression, body image disorders, self-harm, and lack of physical activity and exercise. On the other hand, the Internet and social media can and have improved young people's lives, connecting them with entertainment, education, and community. Ensuring young people get the best possible online experience—balancing safety with utility—is difficult considering every child and teenager has different needs and faces unique circumstances. One-size-fits-all regulation—such as age verification mandates—will not solve all these issues.

This report dives into the current debate surrounding children's online safety, beginning with existing legislation at the federal and state levels, including child sexual exploitation law, children's privacy legislation, and state age-appropriate design and age verification laws. It then analyzes the different proposals to address various children's online safety issues, including privacy, age verification, harmful content, child sexual abuse, and child labor. Finally, it recommends 10 steps the federal government should take to effectively protect children online without placing an undue burden on online services or infringing on users' free speech and privacy or parents' rights:

1. The Federal Trade Commission (FTC) should update the Children's Online Privacy Protection Act (COPPA) rule to reflect technological changes since 2013 while maintaining COPPA's actual knowledge standard and remaining within the law's scope of protecting children's individually identifying information.
2. Congress should pass comprehensive federal privacy legislation that addresses actual privacy harms, preempts state laws, and includes additional protections for children between ages 13 and 17.
3. Congress should pass legislation creating a national, interoperable framework for securely issuing and validating digital IDs across all levels of government.
4. Congress should provide more funding for research and testing of photo-based artificial intelligence (AI) age estimation.
5. Congress should pass legislation requiring device operating systems to create an opt-in "trustworthy child flag" and requiring apps and websites that serve age-restricted content to check for this signal.
6. Congress should amend COPPA so that websites directed at a general audience with common features, such as user feedback forms or customer service chatbots, are not required to obtain parental consent to collect information from users indicated as children by a trustworthy child flag.
7. Congress should pass legislation establishing a government-led forum to create a voluntary industry standard for interoperability on cross-platform parental controls.
8. Congress should increase funding for law enforcement to investigate child sexual abuse material (CSAM) reports and prosecute perpetrators.
9. Congress should pass federal legislation similar to the Coogan Act and Illinois' child influencer legislation that protects child performers in traditional and digital media.
10. Congress should provide funding for digital literacy campaigns that teach both children how to stay safe online and parents how to keep their children safe online.

THE CURRENT DEBATE

Debates over how best to protect children, and what potential harms society needs to protect children from are much older than the Internet and encompass much more than online harms. Problems facing children in society have never been easy to solve, and solutions to those problems often raise similar concerns to many of the proposed solutions to online harms, such as free speech, privacy, and parents' rights.

For example, the debate over how to protect children from gun violence in schools has been a key issue in America, particularly since the Columbine High School shooting in 1999.[2] The number of school shootings has trended upward since then, with a temporary dip in 2020 as many children were social distancing and learning online at the height of the COVID-19 pandemic. In 2023 alone, there were 82 school shootings.[3] Proposed solutions range from gun control to increasing school security and mental health resources, with fierce partisan debate over the effectiveness of these solutions and their Second Amendment implications.

Issues at the heart of the debate surrounding children's use of social media, such as youth mental health and suicide or youth body image and disordered eating, are not restricted to the digital world either. Diagnoses of depression and anxiety in children have increased over time, from 5.4 percent in 2003 to 8.4 percent in 2011–2012.[4] These mental health conditions can be life-threatening, with nearly 19 percent of adolescents ages 12 to 17 reporting that they seriously considered suicide and nearly 9 percent attempting suicide over a 2018–2019 reporting period.[5]

No amount of regulation will completely eradicate all potential harms that children face in the digital and physical worlds.

Body image and disordered eating also pose serious risks. Eating disorders such as anorexia nervosa and bulimia have high mortality rates and cause long-term health impacts even for those who recover.[6] An estimated 2.7 percent of U.S. adolescents have, do, or will suffer from an eating disorder.[7] Social media use is just one of the many theorized environmental and genetic factors that might impact a young person's risk of developing a psychiatric malady such as depression, anxiety, or an eating disorder. Likewise, bullying—another significant problem among young people—is much older than social media and the Internet.

No amount of regulation will completely eradicate all potential harms that children face in the digital and physical worlds. The issue at hand, then, is finding the balance of regulation that effectively addresses concrete harms without overly infringing on everyday Americans' civil liberties, including their rights to privacy and free speech. Not only do regulations sometimes infringe on adults' rights to privacy and free speech, but these regulations also sometimes

infringe on the rights of the very children they aim to protect. Indeed, these kinds of rules, if not designed appropriately, can trample on children's right to engage with their friends and access appropriate information online.

Similarly, lawmakers could intervene in every facet of children's lives to help ensure their safety, but not only is this unfeasible, most parents would object to the government dictating how they can raise their children. This is another area where lawmakers need to find a balance. Regulation can set guardrails that aim to prevent concrete harms and provide new tools for user safety, but some amount of parental control is necessary because every child is different. In most cases, parents will understand their own child's unique needs better than the government will. At the same time, not every child lives in a home with parents willing or able to look out for their best interests online. Even parents who have the time and skills to monitor their children's use need tools to make that easier or, in some cases, possible.

And finally, while technologies have provided new avenues for bad behavior, they can also encourage prosocial behavior, bringing young people together in positive ways. In fact, individuals from marginalized populations who are often victims of bullying can find community online in ways that were never possible before the Internet. Children whose friends move away can keep those friendships alive through free online messaging and video calls. Any regulation designed to protect children online needs to find a balance between minimizing the risks and maximizing the benefits of various online activities for children.

Existing Legislation

There is some existing legislation governing various aspects of children's online safety at the federal and state levels. At the federal level, child sexual exploitation law protects children from sexual abuse while children's privacy legislation protects children's personal information online. At the state level, various states have passed legislation related to age-appropriate design and age verification requirements for social media and adult websites. Meanwhile, other countries around the world, such as the United Kingdom, are having similar debates over how to protect children online and coming to different regulatory conclusions, including establishing duties of care for online services likely to be accessed by children.

Child Sexual Exploitation Law

There are many existing laws governing children's safety in both the physical and digital worlds, protecting children from abuse, neglect, exploitation, and physical harm. Particularly relevant to the debate surrounding children's online safety are laws surrounding CSAM, formerly known as child pornography, as many current proposals to address children's online safety focus on these problems.

The term "child sexual exploitation" covers a range of crimes including kidnapping, sex trafficking, sexual abuse, and the production, distribution, receipt, possession, or importation of CSAM. Child sexual exploitation is a federal crime carrying a minimum sentence of 10 years in prison and the requirement to register as a sex offender.[8] While child sexual exploitation predates the Internet, criminals can and do use the web to facilitate child sexual exploitation, requiring law enforcement, online services, and nonprofit organizations such as the National Center for Missing and Exploited Children (NCMEC) to dedicate significant resources to preventing and responding to online child sexual exploitation.

Notably, NCMEC operates the CyberTipline, a centralized reporting system for online child sexual exploitation. Online services and their users can report suspected child sexual exploitation to the CyberTipline. NCMEC staff review these tips and report them to the appropriate law enforcement agencies for investigation.[9] In 2022, the CyberTipline received over 32 million reports of suspected child sexual exploitation, with over 99.5 percent of those reports representing incidents of suspected CSAM. U.S.-based online services are legally required to report suspected CSAM to the CyberTipline, and in 2022, online services accounted for 99 percent of CyberTipline reports.[10]

Federal, state, and local law enforcement cooperate to combat online child sexual exploitation via the Internet Crimes Against Children (ICAC) Task Force Program, established in 1998 by the U.S. Department of Justice. Since the program's inception, ICAC task forces have reviewed more than 800,000 reports of child sexual exploitation and made nearly 90,000 arrests. Today, the program boasts a network of 61 task forces representing over 5,400 law enforcement agencies.[11]

Children's Online Privacy Protection Act

While the United States lacks a comprehensive federal data privacy law, it does have a federal children's data privacy law: COPPA. Congress passed COPPA in 1998 and the law went into effect in 2000, implemented by the FTC's Children Online Privacy Protection Rule, with the most recent updates to this rule going into effect in 2013.[12]

COPPA imposes privacy protections that online services must adhere to if their services are directed to children under age 13 and they have "actual knowledge"—awareness of a fact or circumstance and no doubt that it exists—that a minor under 13 uses their service. These protections include providing notice of what information the service collects from children and how the service uses that information; obtaining verifiable parental consent before collecting, using, or disclosing a child's personal information; allowing parents to review the personal information collected from their child(ren) and opt out of the information's further use; not condition a child's participation in any activity that involves disclosing more personal information than is reasonably necessary; and maintaining reasonable security practices for children's personal information. Violations are considered unfair or deceptive practices.[13]

The FTC's 2013 updates to the COPPA rule included several significant changes, most notably expanding the definition of personal information to include "persistent identifiers," information that identifies users over time and across different online services, such as IP addresses, device serial numbers, or customer numbers. Other changes included additional modifications to the definition of personal information, a new approval process for obtaining parental consent, disallowing collection of children's personal information via plug-ins without parental consent, strengthening data security requirements, strengthening oversight of safe harbor programs, and requiring data retention and deletion procedures.[14]

State Laws

Since COPPA's 2013 update, and particularly in the past few years, several states have passed various laws of their own. These laws fall into one of three categories: age-appropriate design codes, age verification requirements, and protections for child influencers.

California enacted its Age-Appropriate Design Code Act (CAADCA) in 2022, which requires online services that operate in California that children are "likely to access"—not just services

directed at children—to consider the best interests of children when designing products, services, and features and to prioritize children's privacy, safety, and well-being over commercial interests. These online services must also complete a Data Impact Assessment for each new product, service, or feature they offer, determining whether the product, service, or feature could subject children to harmful or potentially harmful content.[15]

The tech industry association NetChoice sued the state of California over the CAADCA, arguing that the law gives the California state government unconstitutional control over online speech by punishing online services if they do not protect underaged users from harmful or potentially harmful content and prioritize content that promotes minors' best interests, with fines of up to $7,500 per affected child for violations.[16] A federal judge granted a preliminary injunction against the CAADCA in September 2023.[17] Other states have considered age-appropriate design codes of their own, but none have passed, likely because states are waiting on the outcome of NetChoice's case against California.

When it comes to age verification, state laws fall into two further subcategories: age verification requirements for adult websites and social media platforms. The first category includes laws passed by states such as Arkansas, Louisiana, Mississippi, Montana, North Carolina, Texas, Utah, and Virginia requiring online services with a certain amount of adult content to verify that users are over 18 or risk fines.[18] The second category includes laws passed by such states as Arkansas, Connecticut, Louisiana, Ohio, and Utah requiring social media platforms to verify that users are over either age 16 or 18 and require parental consent from users under that age limit.[19]

NetChoice has sued Arkansas, Ohio, and Utah over their social media age verification laws, arguing that they violate the First Amendment by requiring users to hand over sensitive personal information in order to access online communication tools.[20] Meanwhile, the Free Speech Coalition, a trade association representing the adult industry, has sued Louisiana, Utah, and Texas over their adult website age verification laws for similar reasons.[21]

Finally, in the third category of child influencer protections, Illinois amended its child labor laws in 2023, entitling children featured in at least 30 percent of their parents' income-generating online content over a 30-day period to a percentage of their parents' earnings if the content earns at least 10 cents per view. Parents must put the child's earnings in a trust fund that the child can access upon turning 18 or being emancipated. Children can sue their parents for violating the law, which is modeled after California's Coogan Law designed to protect child performers.[22]

An International Comparison

The debate over children's online safety is a global one, with multiple other countries considering regulations to address various online harms.[23] As an example, the United Kingdom's Online Safety Act gained international attention, generating debate over some of its more controversial provisions.[24] Despite this controversy, Parliament passed the act in October 2023, with enforcement going into effect in phases overseen by the United Kingdom's Office of Communications, or Ofcom, the country's telecommunications regulator.[25]

The Online Safety Act is designed not only to protect children online but also to regulate online content more broadly. The law applies to any online service that hosts user-generated content or a search engine that "has links with the United Kingdom," such as a significant number of U.K.

users or a target market of U.K. users. For these services, the act establishes "duties of care," a legal obligation to adhere to a standard of reasonable care in order to avoid causing harm. These duties include a wide range of requirements such as conducting risk assessments, reporting and removing certain content, ensuring freedom of expression and privacy, and keeping certain records. "Category 1 services," the largest online services, face even more requirements such as conducting additional risk assessments, ensuring adults' online safety, and protecting journalistic content and "content of democratic importance."[26]

Online services "likely to be accessed by children" face two additional duties: to conduct children's risk assessments and protect children's online safety. The duty to protect children's online safety requires online services likely to be accessed by children to use age verification or age estimation to identify which users are children and take measures to mitigate and manage the risk of harm to children and prevent children from encountering harmful content. The act's definition of "content that is harmful to children" includes pornography, suicide promotion, self-harm promotion, eating disorder promotion, abuse toward marginalized groups, inciting hatred toward marginalized groups, encouraging violence, bullying, depictions of graphic violence, online challenges that would likely result in serious injury, or encouraging others to ingest harmful substances. In order to determine which services are likely to be accessed by children, all covered online services must conduct children's access assessments.

The debate over children's online safety is a global one, with multiple other countries considering regulations to address various online harms.

Other provisions of the Online Safety Act relevant to children's online safety include a requirement to scan for and report CSAM (referred to as "child sexual exploitation and abuse," or "CSEA," in the Act) to the United Kingdom's National Crime Agency and disclose certain information about deceased child users to a child's parents. Notably, even online services that use end-to-end encryption—a type of encryption that prevents anyone but the sender and recipient of a message or other data from accessing that data, including the service used to host or transmit the data—must scan for CSAM. The act also instructs Ofcom to carry out reviews of content harmful to children on online services and publish reports on these reviews, as well as on age verification technology and children's app store use.[27]

Critics of the Online Safety Act primarily focus on the requirement for online services to scan for CSAM and to break end-to-end encryption to do so, violating users' privacy and compromising their data security.[28] Critics have also pointed out the likely flaws of the act's age verification mandate, which could likewise erode users' privacy by forcing them to turn over sensitive personal information in order to prove their age.[29]

CHILDREN'S PRIVACY

Even as Congress struggles to advance comprehensive federal data privacy legislation, federal children's privacy legislation has existed since COPPA's passage in 1998, demonstrating the relative importance of children's privacy in the eyes of lawmakers and the general public. As technology continues to develop and children spend more time online—and as a federal data privacy law remains a mere hypothetical—children's privacy advocates have argued for updates to children's privacy legislation that expand on existing protections.

Congress has considered amending COPPA via the Children and Teens' Online Privacy Protection Act (COPPA 2.0), introduced in 2021 and reintroduced in 2023 by Sens. Ed Markey (D-MA) and Bill Cassidy (R-LA).[30] Currently, COPPA applies when an online service has "actual knowledge" that a user is under 13, and prohibits online services from collecting those users' personal information without parental consent.[31] COPPA 2.0 would expand protections to users ages 13 to 16 and require online services to comply with the COPPA rule if they have actual knowledge or "knowledge fairly implied on the basis of objective circumstances" that a user is under 17.[32]

The issue of where to draw the line when extending additional protections to users under a certain age is a difficult one considering there is a lack of research that identifies a single age at which children mature past needing such protections.[33] On the one hand, the lack of a comprehensive federal privacy law that would protect all users regardless of age means that teenagers' personal data is not covered by current federal privacy law. On the other hand, if Congress does extend COPPA protections to users between ages 13 and 16, many online services that target this demographic would likely significantly change the way they operate or stop providing services for that demographic altogether, as many social media platforms already do by banning users under age 13. Online services that choose to keep children ages 13 to 16 as a target audience will see a decrease in revenue that will lead to even less innovation in the space.

Less innovation in online services designed for children and teens means less educational content and wholesome entertainment, which many families rely on to keep children engaged and learning. It also means fewer online social spaces for teens, which have become an integral part of the average American teenager's social life and development.[34] Digital connection was a lifeline for teens social distancing during the COVID-19 pandemic, not to mention LGBTQ teens in unaccepting environments, teens who face bullying in the physical world, and teens with physical or mental health conditions seeking community. A decrease in the number and quality of online services aimed at teens would significantly degrade teens' online experience, and perhaps provide greater incentive for children to lie about their age online to gain access to online services aimed at adults.

Likewise, switching from an actual knowledge standard to an implied knowledge standard would create a minefield of potential liability for online services that have already sunk years of

experience and millions of dollars into complying in good faith with COPPA's actual knowledge standard. Navigating this minefield would be costly, taking resources away from innovating new products, services, and safety features and funneling them into compliance efforts. It may also require online services to collect more personal information about their users in order to determine who is an adult and who is a child. Without a comprehensive federal data privacy law that protects all users' data from misuse, these data collection efforts could lead to more harm than they would prevent.

As an alternative to amending the law, the FTC could update the COPPA rule, a process the agency has already begun. The FTC initiated its most recent review of the COPPA rule in 2019, seeking public comments on whether additional changes were needed after the last round of changes in 2013.[35] The agency then issued a notice of proposed rulemaking in January 2024 seeking comment on proposed changes.[36]

The issue of where to draw the line when extending additional protections to users under a certain age is a difficult one considering there is a lack of research that identifies a single age at which children mature past needing such protections.

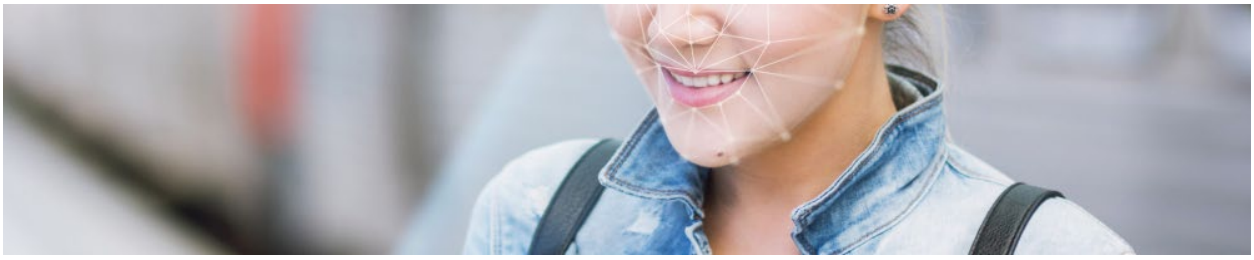
Some of these changes would arguably go beyond the scope of protecting children's individually identifying information, such as limiting the collection of persistent identifiers for contextual advertising and adding all forms of biometric identifiers to the definition of personal information. These proposed changes would come with high costs, in the form of direct compliance costs and "hidden" costs such as lower productivity and less innovation, for little benefit.[37] Additionally, the FTC's proposal to require online services to obtain separate verifiable parental consent for disclosure of a child's personal information to third parties may also impose an unnecessary burden on both parents and businesses.

Despite these flaws, aspects of the FTC's proposed rulemaking would be beneficial for the U.S. digital economy. Most importantly, the FTC maintains COPPA's actual knowledge standard, thus ensuring online services can continue to comply in good faith with COPPA's requirements and protect children without significantly increasing compliance costs. Finally, the FTC's proposal to allow operators to conduct an analysis of their audience composition to avoid classification as a child-directed online service would not only benefit those operators, but also incentivize more online services to analyze their audience and provide the FTC with this information, which could inform future rulemaking.[38]

A final proposal to protect children's privacy is to ban targeted advertising to children, either as part of an update to COPPA—COPPA 2.0, for example, includes such a ban—or as separate legislation.[39] Under COPPA, online services must obtain verifiable parental consent in order to collect or maintain personal information from children under age 13 for targeted advertising.[40] An outright ban on targeted advertising to children would likely lead online services to collect less data from children, but it would also, like other provisions of COPPA 2.0, lead to less innovation in free or low-cost online services designed for children and teens. Much of the Internet relies on targeted advertising to pay for services instead of charging users a fee. Taking away this important source of revenue would lead to an even greater lack of free entertaining and educational resources for children, which would be detrimental to all families, especially to lower-income households.[41]

Moreover, many concerns about targeted advertising stem from a misunderstanding of how targeted ads work. Online services collect information about their users, but in most cases, they do not sell that personally identifiable information to third parties for advertising. Instead, they sell the opportunity to advertise to a certain demographic. Companies that want to advertise to a younger audience, then, are not purchasing young people's data; they are purchasing the digital ad space that will show up on young people's screens. This process is anonymous and much more privacy protective than critics purport.[42]

AGE VERIFICATION



One of the most controversial topics within the broader children's online safety debate is age verification. Multiple states have passed or considered legislation that would restrict children under a certain age from accessing certain online services without parental consent, or at all.

There are multiple different ways online services can verify users' ages, and each of these methods comes with different strengths and weaknesses. Some are more accurate but more invasive, whereas others are less invasive but also less accurate. Before the passage of any age verification laws, many online services, including adult websites and social media platforms, required users to either check a box indicating they are over a certain age or input their date of birth to confirm they are over a certain age. This form of self-verification is the least invasive, because it only requires users to disclose, at most, one piece of personal information: their date of birth. Because many people can share the same birthday, this piece of information cannot uniquely identify an individual. However, this method is also the least reliable, as underage users can and often do lie about their age in order to gain access to certain online services.[43]

On the other end of the spectrum when it comes to accuracy and invasiveness is the ID check. This form of age verification is common in physical spaces, such as bars, casinos, and liquor stores, where customers must provide a valid government-issued ID in order to prove they are above the minimum age required to enter an age-gated space or purchase an age-gated product. It is also highly accurate, as government-issued IDs are more difficult to falsify than checking a box or entering one's date of birth. However, because bars, casinos, and liquor stores do not store a copy of each customer's ID, these in-person ID checks pose lower privacy risks than do online ID checks, where an online service may store the information from users' IDs, including their full name, gender, home address, and photograph. Additionally, as many as 7 percent of Americans do not have a government-issued ID, with rates even higher among lower-income individuals, Black and Hispanic individuals, and young adults.[44] Finally, there are no free speech implications involved in providing an ID to drink alcohol, as opposed to providing an ID to access certain content online.

Digital forms of government-issued identification could solve some of the privacy concerns associated with ID checks for age verification, as well as make the process more efficient.

Currently, online ID checks typically require users to upload a photo of their physical ID as well as sometimes additional steps to prove the ID belongs to them, such as uploading a current image of their face to compare to the photograph on the ID. If designed right, digital IDs would streamline this process and allow users to only share necessary information. For example, individuals trying to access an age-restricted online service could verify that they are over a certain age without providing their exact date of birth, let alone all the other information a physical ID would reveal. Currently, only 10 states offer a digital form of identification, and there is no digital ID program at the federal level.[45] Moreover, some current state-level digital IDs are not designed for online age verification.

In between self-verification and ID checks, there is a third potential method of age verification using AI to estimate users' ages from an image of their face. Combined with privacy protections requiring online services to delete users' images after the age estimation process is complete, this would minimize the amount of personal information users have to give up in order to verify their age. Of course, age estimation technology is not perfectly accurate and likely never will be—no form of age verification is—but it is constantly improving. In 2023, age estimation provider Yoti reported that the company's technology could accurately estimate 13- to 17-year-olds as under 25 with 99.93 percent accuracy and 6- to 11-year-olds as under 13 with 98.35 percent accuracy, with no discernable bias across gender or skin tone. Yoti's mean absolute error—the average error the technology makes when estimating an individual's age—is 1.3 years for children ages 6 through 12 and 1.4 years for teenagers ages 13 through 17.[46]

Digital forms of government-issued identification could solve some of the privacy concerns associated with ID checks for age verification, as well as make the process more efficient.

In addition to the three methods of age verification, there are three different levels at which age verification for online services can occur. The first is the approach existing state legislation takes, requiring age verification at the platform level. Under this approach, users must verify their age every time they create an account on an age-gated online service, such as an adult website or social media platform. This is the most burdensome approach for users and the most likely to result in data privacy or security violations. Users would turn their personal information over to many different online services, each of which could have different privacy and security practices, some of which would be bound to be more protective than others, particularly in the absence of comprehensive federal legislation that sets a national standard for data privacy and security.

Age verification could also take place at the app-store level. Under this approach, users would verify their age once when creating an account on their device's app store, and the app store would not allow users to download age-gated apps unless they were over the required age. This would be less burdensome than the previous approach, as users would have to verify their age only once or, at most, a few times on different app stores. Meta championed this approach with a 2023 proposal for federal legislation requiring app stores to get parents' approval for children under 16 to download apps, arguing that it is a more privacy-protective approach to age verification.[47] However, this approach does not address age verification for websites, a considerable gap.

Finally, age verification could take place at the device level. Under this approach, users would verify their age once with their device's operating system when creating an account on their

device, and the device would not allow users to download age-gated apps or visit age-gated websites unless they were over the required age. Like Meta's app-store proposal, this would be less burdensome for users and create less of a privacy and security risk. It would also create less of a gap than would Meta's proposal, as accessing the Internet requires some form of device, whether it be a smartphone, laptop, desktop computer, smart TV, or even a virtual reality headset, though there would still be a gap for public devices wherever users do not create an account, such as computers at a library or shared devices such as a family tablet. However, owners of shared devices could solve this by defaulting to stricter parental controls on those devices.

Beyond concerns over feasibility and potential privacy and security risks associated with various methods of verifying users' ages, age verification laws have raised additional concerns surrounding their impact on free speech. Existing age verification laws have so far singled out two targets: adult websites and social media platforms. The free speech concerns for these two different categories of laws are related, but differ in several important ways.

The reasoning behind age-gating adult websites is straightforward: These websites prominently feature sexually explicit content that is considered inappropriate for underaged users. Most sexually explicit content is protected speech under the First Amendment, unless it is illegal (e.g., CSAM or nonconsensual pornography) or obscene (according to the standard set out in the Supreme Court case *Miller v. California*, which defined "obscenity" as anything that depicts sexual content in a patently offensive way according to an average, contemporary person and that has no serious literary, artistic, political, or scientific value).[48] Thus, adults have a free speech right to access sexually explicit content. However, the government may impose regulations even on protected speech, such as sexually explicit content, if the regulations "promote a compelling interest" and are "the least restrictive means" to achieve that interest.[49]

Proponents of age verification requirements for adult websites argue that these regulations promote a compelling interest by preventing children from accessing inappropriate content online.[50] Meanwhile, the Free Speech Coalition, which sued three states over their age verification laws, argues that these regulations are not the least restrictive means of preventing children from accessing inappropriate content online, given alternatives such as parental controls and filtering software. The Coalition further argued that age verification laws are ineffective, as they do not prevent users from encountering adult content by accident on websites meant for a general audience, which 58 percent of teens report having happened to them.[51] Additionally, underage individuals seeking adult content online may go to foreign websites outside the jurisdiction of U.S. courts instead of American ones. Finally, there are existing parental controls that can block adult websites on children's devices or shared family devices.

Age verification requirements for social media platforms are even more fraught with potential First Amendment violations. While adult websites prominently feature content that may be inappropriate for underaged users, thus giving the government a compelling interest to protect children from this content, social media platforms feature a wide variety of content, much of which is not only appropriate for minors but also actively beneficial. Additionally, while adults have a free speech right to access sexually explicit content, Americans of all ages have an even more compelling free speech right to access the social media platforms where much of today's social and political discourse occurs, where any individual user can share their thoughts and

opinions with a wide audience and view the thoughts and opinions of millions or billions of other users.

Proponents of age verification requirements for social media argue that there is an overabundance of harmful or inappropriate content on these platforms and that social media usage can lead to other harms, particularly if children become addicted to social media. However, this interest may not be compelling enough to warrant restricting users' free speech—and even if it is, mandating all users verify their age in order to access social media may not pass the test of being the least restrictive means of achieving this interest. In addition, children can become addicted to many things that are not regulated, including television shows, comic books, and video games. Finally, young people have their own free speech rights, and restricting their access to social media because of their age infringes on those rights, which may be unconstitutional regardless of the impact on adults. This is important to remember, because much of this debate treats children as completely lacking these rights.

An alternative to age verification would require device operating systems to create a "trustworthy child flag" for user accounts that signals to apps and websites that a user is underage and require apps and websites that serve age-restricted content to check for this signal from their users and block underage users from this content. Rather than using ID checks to determine whether to activate this child flag option, this would be an opt-in process built in to existing parental controls on devices. Parents could activate or disable the child flag option depending on their own values and the maturity of their children. Additionally, devices could default to certain parental controls recommended for children.

An alternative to age verification would require device operating systems to create a "trustworthy child flag" for user accounts that signals to apps and websites that a user is underage.

Because this approach does not require anyone to disclose or verify their identity, it does not create privacy risks by forcing users to share their government IDs or allowing online services to link their online activity to their offline identities. It is also a low-impact approach, allowing adults to continue using the Internet as they do today. Similarly, the vast majority of websites and apps that are meant for the general public would not have to take any action. Third, it would be entirely voluntary for users. Parents who want to control what their children see on the Internet could choose to use this feature and other parents could choose not to.

The biggest risk with this approach is that Congress could inadvertently (or intentionally) expose many innocuous apps and sites to liability for collecting information from children. Requiring apps and websites to recognize a "child flag" could make many sites start complying with COPPA rules even if they do not host age-restricted content because they now have actual knowledge of children using their service.[52] As such, there should be a clear carveout or exemption for these sites so that they do not face liability.

PROTECTING CHILDREN FROM HARMFUL CONTENT

The argument that the government needs to regulate various forms of media in order to prevent children from encountering inappropriate or harmful content is much older than the Internet. From novels and radio to television and video games, moral panic surrounding children's consumption of media is as old as media itself.[53] The Internet, and particularly social media, is merely the latest iteration of this trend.

There is inappropriate content or content that is potentially harmful to children on the Internet and on social media, just as there is in any form of media. This may include adult content, bullying, hate speech, and depictions or promotion of self-harm, suicide, eating disorders, substance abuse, or violence. Most of these forms of content violate most online services' community guidelines, and most online services work diligently to remove harmful content, but the sheer amount of content online means that some of it will inevitably slip through the cracks in content moderation. Online services that do allow adult content typically have restrictions in place meant to ensure only adult users seeking out such content are exposed to it or offer alternative versions of their services targeted at a younger audience.

For other forms of media, protections for children have taken the form of both government regulation and industry-led standards. For example, the Federal Communications Commission (FCC) regulates radio and television in the United States. Broadcast television and radio stations are prohibited from airing "indecent" material between the hours of 6:00 AM and 10:00 PM.[54] Film, on the other hand, has utilized an industry-led approach since 1968, with the Motion Picture Association (MPA) assigning ratings that reflect a film's content, taking into account elements such as violence, profanity, depictions of substance use, and sexual content.[55] This allows parents to decide which films they believe are appropriate for their children. The video game industry uses a similar rating system overseen by the Entertainment Software Rating Board (ESRB).[56]

Requiring age verification, parental consent for children under a certain age, or both to access social media is one approach some states have taken to protect children from inappropriate or harmful content online. Age-appropriate design, exemplified by the CAADCA, is another approach, which defers to considering the best interests of children when designing digital products, services, and features. The CAADCA imposes this requirement, and the requirement to prioritize children's privacy, safety, and well-being over commercial interests, on any online service children are likely to access. Before making any new service, product, or feature available to the public, these online services must conduct a Data Protection Impact Assessment to determine whether the service, product, or feature and any associated algorithms or targeted advertising systems could cause harm to children and how the service, product, or feature uses children's personal information.

Other provisions in the CAADCA require online services that children are likely to access to estimate the age of child users, configure default privacy settings provided to children to a high level of privacy, provide privacy information and terms of service in clear language suited to children, provide an obvious signal to children when a parent or guardian is monitoring their online activity or tracking their location, enforce published terms of service and community standards, and provide tools to help children exercise their property rights and report concerns.[57]

While age-appropriate design provides a useful set of guiding principles for online services with underaged users, enforcing these standards the way the CAADCA does would cause more harm than good. Requiring companies to act in the best interests of children—or face fines up to $7,500 per affected child—is an incredibly broad and ill-defined standard that is difficult, if not impossible, for online services to perfectly follow. Additionally, as NetChoice outlined in its lawsuit, the CAADCA may also violate the First Amendment by giving the government of California power to dictate online services' editorial decisions.[58]

At the federal level, some policymakers have called for a repeal of Section 230 of the Communications Decency Act, a law passed in 1996 stating that online services and their users are not liable for third-party content or for good faith efforts to remove objectionable third-party content.[59] Section 230 was at the center of debate during and after the 2020 election, with both Trump and Biden expressing a desire to repeal the law, though for different reasons.[60] Among critics' reasons for opposing Section 230 is the argument that because of Section 230's protections, online services do not do enough to remove harmful content or may even encourage certain forms of harmful content to increase engagement—a claim that lacks evidence.[61]

While age-appropriate design provides a useful set of guiding principles for online services with underaged users, enforcing these standards the way California does would cause more harm than good.

The legal landscape prior to Section 230's passage reveals how repealing the law would be detrimental. Section 230 arose out of a pair of court cases in the 1990s: *Cubby v. CompuServe* (1991) and *Stratton Oakmont v. Prodigy* (1995).[62] These cases established a counterintuitive precedent for websites that rely on third-party content: Websites that exercised no control over what was posted on their platforms and allowed all content would not be liable for third-party content, while websites that exercised good faith efforts to moderate content would face liability. This is the legal landscape America would return to if Congress repealed Section 230.

To solve this, Congress could repeal the clause of Section 230 that protects online services from liability when they fail to remove content but maintain Section 230's protections for good faith content moderation. But even under these circumstances, repealing Section 230's liability shield would still have negative consequences for innovation, free speech, and competition. Large online services would adapt to a world without Section 230, while smaller ones may not have the resources, which would consolidate the market share of large platforms and impose high barriers of entry on start-ups. Moreover, to protect themselves from facing liability, online services would likely turn to overly restrictive content moderation practices, removing any potentially objectionable content, which may include valuable forms of expression such as political speech and marginalized speech.[63]

More recent proposals to protect children from inappropriate or harmful content online have left Section 230 alone. The leading example of this, at the federal level, is the Kids Online Safety Act (KOSA). Sens. Richard Blumenthal (D-CT) and Marsha Blackburn (R-TN) originally introduced KOSA in 2022 and reintroduced it in 2023.[64] In its current form, KOSA would require online services reasonably likely to be used by minors to provide certain parental controls and optional safeguards for minors, including the ability to restrict who can message them and view their profiles, monitor screen time and establish limits, control or opt out of personalized recommendation systems, restrict purchases, manage privacy settings, and report harms that occur. Online services would also have to default minors' accounts to the strictest privacy and safety settings.

KOSA also contains transparency requirements, including requiring online services to provide information for minors and their parents about safeguards, personalized recommendation systems, and advertising. Online services with at least 10 million monthly active users in the United States would also have to publish public reports on both potential risks to minors, according to an independent third-party audit, and steps the online service takes to mitigate these risks. KOSA would also establish requirements for online services to respond to reports of potential harm to minors, giving online services with at least 10 million active monthly users 10 days to respond and smaller platforms 21 days.

Finally, KOSA would establish a "duty of care" for any online service that is reasonably likely to be used by a minor. Specifically, these online services would have a duty to ensure their design features prevent and mitigate harm to minors. This provision has caused the most controversy of any part of the bill, with critics arguing that the language is vague and undefined by existing case law, which would complicate compliance. Online services may overcorrect and make it more difficult for minors, or potentially all users, to access helpful content related to mental health, suicide, addiction, eating disorders, sexuality, and more. The duty of care provision may even violate the First Amendment, as the government cannot dictate an online service's editorial decisions, which could include design features.[65]

KOSA's other provisions are less controversial. The bill's approach to parental controls, for example, would allow children and their parents to tailor their online experience in a way that is best suited to each child's individual needs, striking a good balance between government involvement, platform responsibility, and parental choice. However, requiring online services to default to the strictest settings for minors' accounts strips away some of this choice and would likely result in many minors missing out on potentially beneficial design features—such as algorithmic recommendation systems—if they, like many users, stick with the default options rather than personalize their account settings.[66] It would be more beneficial for certain features that are most important for safety, such as restricting who can message minors and view their profiles, to be left on by default while other features, such as screen-time limits and personalized recommendation systems, are left in the hands of parents.

KOSA's transparency requirements for online services are also beneficial, as they would allow children and their parents to make more informed decisions about their safety and personal information. Meanwhile, impact assessments would benefit the general public by making certain safety information widely available, although this would only be the case for large online services, as those with fewer than 10 million monthly active users would not face this requirement.

This is not the only flaw in KOSA's size-based approach, which also affects online services of different sizes when it comes to responding to reports of potential harm. Seemingly the logic behind giving larger online services less time to respond is that these online services have more resources to respond to reports quickly. However, larger online services are also likely to receive more reports because they have more users making those reports and more content for users to report. Moreover, harmful content is not less harmful simply because it takes place on a smaller platform. A uniform set of rules for all online services would more effectively protect children.

CHILD SEXUAL ABUSE

One of the most serious forms of harm facing children is sexual abuse and exploitation. Child sexual abuse includes both contact and noncontact abuse. Examples of contact abuse include rape and inappropriate or unwanted touching, while examples of noncontact abuse include voyeurism (exposing a child's body), exhibitionism (exposing one's own body to a child), exposure to pornography, verbal sexual harassment, and distribution of CSAM. Contact and noncontact abuse can both lead to negative mental health and quality-of-life outcomes.[67]

While the nature of digital interaction does not allow for contact abuse, in many ways, it makes noncontact abuse easier to perpetrate. Digital spaces enable users to connect with one another and with content in new and unprecedented ways. Unfortunately, this includes connecting perpetrators of child sexual abuse with potential victims or with abusive content, such as CSAM. Perpetrators can also use digital interaction to groom children for abuse.[68]

Online services employ many different strategies to detect and remove CSAM and other abusive content. In addition to features that allow users to report abusive content, online services may use AI to scan for CSAM and hire content moderators to go through content a user or AI system has identified as potentially abusive.[69] In addition to operating the CyberTipline for CSAM reports, NCMEC operates hash-sharing platforms. These platforms assign hash values to CSAM content, including content reported by online services, and when online services scan for CSAM, they can scan for these hash values to detect known CSAM content.[70]

A point of contention when it comes to online services scanning for CSAM content is whether they should break encryption in order to do so. On one side of the debate, law enforcement, government officials, and children's safety advocates argue that end-to-end encryption prevents online services from scanning for CSAM and makes it difficult or impossible for law enforcement to access perpetrators' communications. On the other side, data privacy and security advocates argue that encryption is an important tool that many users—including members of vulnerable populations such as abuse victims, the LGBTQ community, journalists and their sources, military service members, and activists living under oppressive regimes—rely on to protect themselves. Unfortunately, there is no way for online services to create a "backdoor" that allows law

enforcement or the services themselves to access encrypted communications without creating a vulnerability that hackers could exploit.

Congress reignited the debate around encryption in 2020 when Sens. Lindsey Graham (R-SC), Richard Blumenthal (D-CT), Josh Hawley (R-MO), and Dianne Feinstein (D-CA) introduced the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act.[71] The bill's introduction came at a time when Congress was also in the midst of debate surrounding Section 230. In its original form, the EARN IT Act of 2020 required online services to take "reasonable measures" to keep their platforms safe or risk losing Section 230 liability protection. These reasonable measures would include a prescribed list of best practices determined by the National Commission on Online Child Exploitation Prevention and the U.S. Attorney General.

Given bill sponsor Sen. Graham's stance on encryption, as well as the stance of then-Attorney General William Barr—namely, that tech companies should create backdoors for law enforcement to access encrypted data—many privacy and security advocates raised concerns that the EARN IT Act's true goal was to undermine encryption, perhaps by declaring that companies that use end-to-end encryption are not following best practices to prevent child exploitation.[72]

In response, Sen. Patrick Leahy (D-VT) introduced an amendment to the EARN IT Act stating that "cybersecurity protections," including end-to-end and other forms of encryption, "do not give rise to liability."[73] However, even after Sen. Leahy's amendment passed a Judiciary Committee vote, advocates still had concerns. In addition to establishing best practices for preventing child exploitation, the EARN IT Act would allow states to enforce their own child exploitation laws against online services, which could include laws targeting encryption. While it did not pass in 2020, the EARN IT Act was reintroduced in 2022 and 2023.[74]

Digital spaces enable users to connect with one another and with content in new and unprecedented ways. Unfortunately, this includes connecting perpetrators of child sexual abuse with potential victims or with abusive content.

Another anti-CSAM bill, the Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment (STOP CSAM) Act, would also create an exception to Section 230's liability shield in an effort to address child sexual abuse. Sen. Richard Durbin (D-IL) introduced the bill in 2023 with provisions meant to increase transparency and accountability in CSAM reporting such as requiring large online services—those with over 1 million unique monthly visitors and over $50 million in annual revenue—to submit annual reports to the attorney general and chair of the FTC detailing their CSAM policies and reporting systems and other measures to promote a culture of safety for children. The bill also includes increased privacy protections for child victims and witnesses in federal court and would make it easier for states to receive federal funding to establish ICAC task forces.

In addition, the STOP CSAM Act would require online services to report and remove planned or imminent child exploitation, which could encompass a wide range of online content and activities—for example, online communication between two adults to discuss transporting a child across state lines, which could indicate a potential crime, but likely indicates something more innocuous such as a family vacation. The bill would also make it a crime to not only "intentionally" or "knowingly" host or store CSAM or promote or facilitate child exploitation but

also to do so "recklessly" or "negligently."[75] Like the EARN IT Act, this could undermine end-to-end encryption.

The STOP CSAM Act imposes a tight turnaround time of 48 hours for responding to notices, high criminal penalties of $150,000 for an initial violation and $300,000 for subsequent violations, and civil penalties up to $100,000 for failure to report and remove content and up to $1 million for failure to submit an annual report. Moreover, online services would not be able to use Section 230 as a defense for failing to remove content. This would expose online services to a flood of expensive litigation. The threat of legal fees and fines would incentivize online services to remove more content than necessary.[76]

Outside of creating exceptions to Section 230, Congress could increase funding for law enforcement to investigate the millions of CSAM reports online services already submit each year and prosecute the perpetrators responsible for creating, spreading, or enabling child sexual abuse and exploitation. This should include increased funding for ICAC task forces as well as police technology and training to keep up with perpetrators who continually update their methodology to evade detection.

CHILD LABOR

Many social media platforms enable users to make money off of the content they create, as long as those users meet certain requirements and adhere to the platforms' monetization policies.[77] Users with a significant following can also make deals with businesses to promote products and services to their audience, subject to FTC disclosure requirements.[78] These opportunities have created an entire industry of online content creators known as "influencers." According to Allied Market Research, the influencer marketing market generated $16.5 billion in 2022 and is estimated to reach almost $200 billion by 2032.[79]

Within the influencer industry, many accounts create family-oriented or kid-friendly content featuring child creators. Social media platforms typically require users to be at least 18 in order to monetize their content, so child influencers must either appear on a parent's account or have a parent operate their account. These children might appear in all the content made by that account or simply a significant enough portion that the child is a regular feature in a parent's content. The presence of child influencers on social media has generated debate over the ethics of monetizing content that features children. If parents earn money from content that regularly features their children and do not set any of that money aside for their children, are those children being exploited?[80]

This debate mirrors similar debates over child stars of traditional media. Celebrities such as Judy Garland, Shirley Temple, Michael Jackson, Britney Spears, Demi Lovato, and many more have shared their experiences of exploitation and abuse at the hands of their employers or even their

parents.[81] One early case of exploitation in Hollywood—that of child star Jackie Coogan, whose parents spent nearly all his income, leading Jackie to sue for his lost earnings—led California to pass the California Child Actor's Bill, or Coogan Act.[82] The Coogan Act and similar laws passed in nine other states require parents of child performers to set aside a certain amount of the child's earnings—15 percent in California—in a trust that the child gains access to upon reaching adulthood.[83]

Illinois became the first state to extend similar protections to child influencers in 2023, amending its child labor laws to require parents whose children under 16 appear in at least 30 percent of their income-generating video content over a 30-day period must set aside a portion of the revenue in a trust.[84] In other words, the law does not affect parents who only occasionally post content featuring their children or who do not monetize their content on social media. Instead, the law will hopefully protect child influencers in Illinois from financial exploitation when parents monetize video content that regularly features their children.

With child influencer legislation existing in just one state and addressing only the threat of financial exploitation, Illinois's new law is unlikely to settle the child influencer debate, just as the Coogan Act and similar laws did not end the debate over how to protect child stars of traditional media.[85] Passing a federal Coogan Act that protects child performers regardless of the type of media they appear in, whether traditional or digital, would be an effective first step to further enshrine protections for child performers nationwide. However, other forms of exploitation and abuse—including sexual abuse and exposure to or involvement in content that is inappropriate for children—remain a threat to child influencers and child stars.

SUMMARY OF PROPOSALS

Table 1: Summary of proposals to address children's online safety

Proposal	Description	Pros	Cons
Children's Privacy			
Amend COPPA	▪ Amends COPPA to cover children ages 13 to 17 and expand the law's scope	▪ Teenagers would benefit from increased privacy protections ▪ Increasing the standard for compliance would protect more children than the current standard does	▪ Online services may stop providing services for teenagers to avoid COPPA requirements ▪ Significantly increases the cost of compliance and risk of liability
Update the COPPA Rule	▪ Updates the COPPA rule to reflect recent technological changes	▪ Less drastic changes than COPPA 2.0 ▪ Maintains COPPA's actual knowledge standard, benefitting online services that comply in good faith ▪ Giving online services the option to conduct an audience composition	▪ Some of the proposed changes go beyond COPPA's scope of protecting children's individually identifying information ▪ Requiring online services to obtain separate consent for third-party sharing is

Proposal	Description	Pros	Cons
		analysis would benefit online services and the FTC	burdensome for parents and businesses
Ban Targeted Advertising to Children	▪ Bans targeted advertising to children under a certain age	▪ Online services would collect less data from children	▪ Online services may stop providing free or low-cost services aimed at children and teenagers ▪ Businesses selling to children would face higher marketing costs
Age Verification			
At the Platform Level	▪ Verifies users' ages on each age-gated online service they access	▪ Protects children from accessing online services that are inappropriate for their age	▪ Burdensome on users who must verify their age many times ▪ Creates privacy and security risks for users' personal information
At the App Store Level	▪ Verifies users' ages in the app store they use, indicating their age to all apps they download	▪ Protects children from downloading apps that are inappropriate for their age ▪ Less burdensome than age verification at the platform level	▪ Does not address age verification for websites ▪ Still creates some privacy and security risk for users' personal information
At the Device Level	▪ Verifies users' ages on each device they use, indicating their age to all websites or apps they access on that device	▪ Protects children from accessing online services that are inappropriate for their age	▪ Does not address age verification on public or shared devices ▪ Still creates some privacy and security risk for users' personal information
For Adult Websites	▪ Requires adult websites to verify users are over age 18	▪ Creates a barrier to children from accessing sexually explicit content online	▪ Does not address sexually explicit content on mainstream websites ▪ Could boost the growth of bad actors over websites that comply with the law ▪ May violate the First Amendment if less-restrictive means of protecting children exist

Proposal	Description	Pros	Cons
For Social Media Platforms	▪ Requires social media platforms to verify users are over age 18	▪ Creates a barrier to children from seeing harmful or inappropriate content ▪ Creates a barrier to children from becoming addicted to social media	▪ May violate the First Amendment by conditioning users' access to social media on turning over their personal information ▪ May violate young people's First Amendment rights
Child Flag	▪ Requires device makers and online services to establish a child flag system that allows online services to assume everyone is an adult unless they have been marked as a child	▪ Does not create privacy risks from sharing government ID ▪ Low-impact approach for users and online services ▪ Voluntary process that gives parents more control	▪ Exposes online services to liability for collecting information from children
Protection From Harmful Content			
Age-Appropriate Design	▪ Requires online services likely to be accessed by children to design products, services, and features in the best interests of children	▪ Incentivizes online services to prioritize children's interests, which may prevent harm and create safer spaces for kids	▪ Broad and ill-defined standard ▪ May violate the First Amendment by dictating online services' editorial decisions
Repeal Section 230	▪ Removes Section 230 liability protection	▪ Incentivizes online services to remove harmful content or risk liability	▪ High legal fees create barriers to innovation, particularly for smaller companies and start-ups ▪ Online services would likely restrict users' speech to avoid liability
Parental Controls	▪ Require online services to create and offer parental controls for minors' accounts	▪ Allow children and their parents to tailor their online experience to their individual needs	▪ Defaulting to the strictest settings would likely result in many minors missing out on potentially beneficial design features ▪ Relying only on parental controls requires parents to be highly involved and technologically literate

Proposal	Description	Pros	Cons
Transparency Requirements	▪ Require online services to provide safety and privacy information prominently and in clear language for children and parents and make certain data available to researchers and government agencies upon request	▪ Allow children and their parents to make more informed decisions about their safety and personal information	▪ Alone, these requirements do not enforce safety requirements, but rather merely make safety information available
Impact Assessments	▪ Require online services to conduct regular impact assessments on potential harm to children and prevention and mitigation	▪ Make certain safety information widely available to the general public	▪ If only large online services face this requirement, smaller platforms will escape public scrutiny
Takedown Requirements	▪ Require online services to respond to reports of potential harm to children within a certain timeframe	▪ Incentivize online services to remove harmful content or put a stop to harmful activity	▪ Setting different response timelines for larger and smaller online services is counterintuitive
Duty of Care	▪ Requires online services to exercise reasonable care to prevent and mitigate certain harms to children	▪ Incentivizes online services to consider the interests of children first when designing and implementing features	▪ May make it more difficult for users of all ages to access helpful content related to controversial topics ▪ May violate the First Amendment by dictating online services' editorial decisions
Child Sexual Abuse			
Backdoors to Encryption	▪ Require companies to create backdoors to end-to-end encryption	▪ Give law enforcement and online services access to perpetrators' communication	▪ Create cybersecurity vulnerabilities that hackers could exploit

Proposal	Description	Pros	Cons
Section 230 Exception	▪ Creates an exception to Section 230 liability protection for CSAM	▪ Incentivizes online services to report and remove CSAM content	▪ Incentivizes online services to remove more content than necessary ▪ Reports do not necessarily translate to enforcement
Client-Side Scanning	▪ Requires online services to scan their users' communications for CSAM	▪ Increases the amount of abusive content and activity that online services report to law enforcement	▪ Law enforcement already does not have enough resources to investigate all reported cases of CSAM ▪ Violates users' privacy ▪ Requires breaking end-to-end encryption
Improve CSAM Enforcement	▪ Increases funding for law enforcement, including ICAC task forces, police technology, and training	▪ Law enforcement has more resources to investigate CSAM and prosecute perpetrators	▪ Does not necessarily prevent child sexual abuse from occurring
Child Labor			
Child Influencer Protections	▪ Establish federal protections for child influencers similar to existing state-level protections for child performers	▪ Protect child influencers from financial exploitation	▪ Do not protect child influencers from other forms of exploitation or abuse

RECOMMENDATIONS

An effective approach to children's online safety needs to strike a balance between protecting kids, protecting user privacy, and protecting free speech, as well as striking a balance between giving responsibility to the government, online services, and parents.

In order to accomplish this:

1. The FTC should update the COPPA rule to reflect technological changes since 2013, including by allowing operators to conduct an analysis of their audience composition to avoid classification as a child-directed service, while maintaining COPPA's actual knowledge standard and remaining within the law's scope of protecting children's individually identifying information.
2. Congress should pass comprehensive federal privacy legislation that addresses actual privacy harms and preempts state laws, creating a single set of protections for all

Americans, including additional protections for children between ages 13 and 17 such as requiring opt-in consent to collect and share teenagers' data while allowing adults to opt out of data collection and sharing.[86]

3. Congress should pass legislation creating a national, interoperable framework for securely issuing and validating digital IDs across all levels of government and directing the Department of Homeland Security to begin issuing those digital IDs upon request, with grants for states to upgrade their systems for issuing driver's licenses and other identity credentials to support digital IDs that can serve as privacy-protective forms of online age verification for adults.[87]
4. Congress should provide more funding for research and testing of photo-based AI age estimation and direct the National Institute of Standards and Technology (NIST) to conduct an up-to-date empirical evaluation of age estimation algorithms and their accuracy.[88]
5. Congress should pass legislation requiring device operating systems to create an opt-in "trustworthy child flag" for user accounts, available when first setting up a device and later in a device's settings, that signals to apps and websites that a user is underage and requiring apps and websites that serve age-restricted content to check for this signal for their users and block underage users from this content.
6. Congress should amend COPPA's actual knowledge standard so that websites directed at a general audience with common features, such as user feedback forms or customer service chatbots, are not required to obtain parental consent to collect information from users indicated as children by a trustworthy child flag.
7. Congress should pass legislation establishing a government-led forum to create a voluntary industry standard for interoperability on cross-platform parental controls, which would enable parents to create universal limits on their children's online behavior across multiple devices.
8. Congress should increase funding for law enforcement to investigate CSAM reports and prosecute perpetrators, including by increasing funding for ICAC task forces, police technology, and police training to keep up with perpetrators' continuously evolving methodology.[89]
9. Congress should pass federal legislation similar to the Coogan Act and Illinois' child influencer legislation that protects child performers in traditional and digital media by requiring parents to set aside a portion of a child's earnings in a trust that the child can access upon reaching adulthood.
10. Finally, Congress should provide funding for digital literacy campaigns that teach children how to stay safe online and parents how to keep their children safe online.

About the Author

Ashley Johnson (@ashleyjnsn) is a senior policy manager at ITIF. She researches and writes about Internet policy issues such as privacy, security, and platform regulation. She was previously at Software.org: the BSA Foundation and holds a master's degree in security policy from the George Washington University and a bachelor's degree in sociology from Brigham Young University.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org/about.

ENDNOTES

1. "Act No. 440," Louisiana State Legislature, accessed April 22, 2024, https://legis.la.gov/legis/ViewDocument.aspx?d=1289498.
2. Brian Stelter, "25 Years After Columbine: Why the Massacre Was a Turning Point for America," *Vanity Fair*, April 18, 2024, https://www.vanityfair.com/news/story/25-years-after-columbine.
3. Alex Leeds Matthews, "School shootings in the US: Fast facts," updated March 7, 2024, https://www.cnn.com/us/school-shootings-fast-facts-dg/index.html.
4. Rebecca H. Bitsko et al., "Epidemiology and Impact of Health Care Provider–Diagnosed Anxiety and Depression Among US Children," *Journal of Developmental & Behavioral Pediatrics* 39, no. 5 (June 2018): 395-403, https://journals.lww.com/jrnldbp/abstract/2018/06000/epidemiology_and_impact_of_health_care.6.aspx.
5. Rebecca H. Bitsko et al., "Mental Health Surveillance Among Children – United States, 2013–2019," *Morbidity and Mortality Weekly Report Supplements* 71, no. 2 (February 2022): 1–42, https://www.cdc.gov/mmwr/volumes/71/su/su7102a1.htm.
6. Daphne van Hoeken and Hans W. Hoek, "Review of the burden of eating disorders: mortality, disability, costs, quality of life, and family burden," *Current Opinion in Psychiatry* 33, no. 6 (November 2020): 521–527, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7575017/.
7. Kathleen Reis Merikangas et al., "Lifetime prevalence of mental disorders in U.S. adolescents: results from the National Comorbidity Survey Replication—Adolescent Supplement (NCS-A)," *Journal of the American Academy of Child and Adolescent Psychiatry* 49, no. 10 (October 2010): 980–989, https://pubmed.ncbi.nlm.nih.gov/20855043/.
8. 18 U.S.C § 2260A.
9. "CyberTipline," NCMEC, accessed March 20, 2024, https://www.missingkids.org/gethelpnow/cybertipline.
10. "CyberTipline 2022 Report," NCMEC, accessed March 20, 2024, https://www.missingkids.org/cybertiplinedata.
11. "Internet Crimes Against Children (ICAC) Task Force Program," ICAC, accessed March 20, 2024, https://www.icactaskforce.org/.

12. "Children's Online Privacy Protection Rule ('COPPA')," FTC, accessed March 21, 2024, https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.
13. 15 U.S.C. § 6501.
14. "FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Privacy Protection Rule," FTC, December 19, 2012, https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over-their-information-amending-childrens.
15. "AB-2273 The California Age-Appropriate Design Code Act," California Legislative Information, accessed March 21, 2024, https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false.
16. Chris Marchese, "NetChoice v. Bonta," NetChoice, March 21, 2023, https://netchoice.org/netchoice-v-bonta/.
17. Tara Suter, "Judge blocks California children's digital privacy law from taking effect," *The Hill*, September 19, 2023, https://thehill.com/regulation/court-battles/4212857-judge-blocks-california-childrens-digital-privacy-law-from-taking-effect/.
18. Jonathan Limehouse and Kayla Jimenez, "Millions blocked from porn sites as free speech, child safety debate rages across US," *USA Today*, March 14, 2024, https://www.usatoday.com/story/news/nation/2024/03/14/porn-texas-shut-down/72976270007/.
19. Ashley Johnson, "Lacking a Federal Standard, States Try and Fail to Solve Problems Faced by Kids Online" (ITIF, November 17, 2023), https://itif.org/publications/2023/11/17/lacking-a-federal-standard-states-try-and-fail-to-solve-problems-faced-by-kids-online/.
20. Chris Marchese, "NetChoice v. Griffin," June 29, 2023, https://netchoice.org/netchoice-v-griffin/; Chris Marchese, "NetChoice v. Yost," January 5, 2024, https://netchoice.org/netchoice-v-yost/; Chris Marchese, "NetChoice v. Reyes," December 18, 2023, https://netchoice.org/netchoice-v-reyes/.
21. Andrea Vittorio, "Porn Industry Sues Louisiana in Latest Age-Check Legal Feud," *Bloomberg Law*, updated June 28, 2023, https://news.bloomberglaw.com/privacy-and-data-security/porn-industry-sues-louisiana-in-latest-challenge-to-age-mandates; Skye Witley, "Porn Groups Sue to Block Texas' Looming Online Age-Checks Law," *Bloomberg Law*, August 7, 2023, https://news.bloomberglaw.com/privacy-and-data-security/porn-groups-sue-to-block-texas-looming-age-verification-law; Andrea Vittorio, "Porn Industry Group Seeks Pause of Utah Online Age Checks Law," *Bloomberg Law*, June 1, 2023, https://news.bloomberglaw.com/privacy-and-data-security/porn-industry-group-seeks-pause-of-utahs-online-age-checks-law.
22. Kate Walter, "Illinois legislation first to protect the children of influencers," *The Daily Northwestern*, September 27, 2023, https://dailynorthwestern.com/2023/09/27/lateststories/illinois-legislation-first-to-protect-the-children-of-influencers/.
23. See, for example, "Proposed Bill to address Online Harms," Government of Canada, updated March 4, 2024, https://www.canada.ca/en/canadian-heritage/services/online-harms.html; Patrîcia Campos Mello, "Bill Forcing Big Techs to Remove Content that Violates Children's Rights Advances in Brazil's Senate," *Folha de S.Paulo*, February 22, 2024, https://www1.folha.uol.com.br/internacional/en/business/2024/02/bill-forcing-big-techs-to-remove-content-that-violates-childrens-rights-advances-in-brazils-senate.shtml; Josh Taylor, "Australia releases new online safety standards to tackle terror and child sexual abuse content," *The Guardian*, November 20, 2023, https://www.theguardian.com/australia-news/2023/nov/20/australia-esafety-standards-new-2023-targets-child-content-terrorism-detection; Kim Min-Wook, "Laws try to help kids with their sharing of info online," *Korea JoongAng Daily*, July 11, 2022, https://koreajoongangdaily.joins.com/2022/07/11/national/socialAffairs/Korea-personal-information-protection/20220711181402414.html.

24. Kir Nuthi, "The Effect of International Proposals for Monitoring Obligations on End-to-End Encryption" (Center for Data Innovation, November 2022), https://www2.datainnovation.org/2022-E2EE-monitoring-obligations.pdf.
25. Peter Guest, "The UK's Controversial Safety Act Is Now Law," *Wired*, October 26, 2023, https://www.wired.com/story/the-uks-controversial-online-safety-act-is-now-law/.
26. "Online Safety Act," Legislation.gov.uk, accessed March 22, 2024, https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted.
27. Ibid.
28. Alex Hern, "WhatsApp and Signal unite against online safety bill amid privacy concerns," *The Guardian*, April 18, 2023, https://www.theguardian.com/technology/2023/apr/18/whatsapp-signal-unite-against-online-safety-bill-privacy-messaging-apps-safety-security-uk.
29. Jason Kelley, "UK Online Safety Bill Will Mandate Dangerous Age Verification for Much of the Web," Electronic Frontier Foundation, September 5, 2023, https://www.eff.org/deeplinks/2023/09/uk-online-safety-bill-will-mandate-dangerous-age-verification-much-web.
30. "S.1628 - Children and Teens' Online Privacy Protection Act," Congress.gov, accessed April 17, 2024, https://www.congress.gov/bill/117th-congress/senate-bill/1628; "S.1418 - Children and Teens' Online Privacy Protection Act," Congress.gov, accessed April 17, 2024, https://www.congress.gov/bill/118th-congress/senate-bill/1418.
31. 15 U.S.C. § 6501.
32. "COPPA 2.0 Bill Text," Office of Senator Ed Markey, published February 15, 2024, https://www.markey.senate.gov/download/coppa-20-bill-text.
33. "Health Advisory on Social Media Use in Adolescence" (American Psychological Association, May 2023), https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use.pdf.
34. Ibid.
35. "FTC Seeks Comments on Children's Online Privacy Protection Act Rule," FTC, published July 25, 2019, https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-seeks-comments-childrens-online-privacy-protection-act-rule.
36. FTC, "Children's Online Privacy Protection Rule," *Federal Register* 89, no. 2034 (January 11, 2024): 2034-2076, https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule.
37. Ashley Johnson and Daniel Castro, "Maintaining a Light-Touch Approach to Data Protection in the United States" (ITIF, August 2022), https://itif.org/publications/2022/08/08/maintaining-a-light-touch-approach-to-data-protection-in-the-united-states/.
38. Ashley Johnson, "Comments Before the Federal Trade Commission Regarding the Children's Online Privacy Protection Rule" (ITIF, March 11, 2024), https://itif.org/publications/2024/03/11/comments-before-federal-trade-commission-regarding-childrens-online-privacy-protection-rule/.
39. "COPPA 2.0 Bill Text," Office of Senator Ed Markey.
40. "Complying with COPPA: Frequently Asked Questions," FTC, edited January 2024, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.
41. Ashley Johnson, "Banning Targeted Ads Would Sink the Internet Economy" (ITIF, January 20, 2022), https://itif.org/publications/2022/01/20/banning-targeted-ads-would-sink-internet-economy/.
42. Daniel Castro, "Congress Needs to Understand How Online Ads Work to Pass Data Privacy Legislation" (ITIF, March 2, 2023), https://itif.org/publications/2023/03/02/congress-needs-to-understand-how-online-ads-work-to-pass-data-privacy-legislation/.

43. Yonder Consulting, "Children's Online User Ages Quantitative Research Study" (Ofcom, October 2022), https://www.ofcom.org.uk/__data/assets/pdf_file/0015/245004/children-user-ages-chart-pack.pdf.
44. "2012 Time Series Study," America National Election Studies, accessed April 26, 2024, https://electionstudies.org/data-center/2012-time-series-study/.
45. "Mobile drivers license & digital ID adoption," IDScan.net, accessed April 4, 2024, https://idscan.net/mobile-drivers-licenses-mdl-state-adoption/.
46. "Yoti Facial Age Estimation White Paper" (Yoti, March 2023), https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-March-2023.pdf.
47. Antigone Davis, "Parenting in a Digital World Is Hard. Congress Can Make It Easier," Meta, November 15, 2023, https://about.fb.com/news/2023/11/online-teen-safety-legislation-is-needed/.
48. *Miller v. California*, 413 U.S. 15, 27 (1973).
49. *Sable Communications of California v. Federal Communications Commission*, 492 U.S. 115, 126 (1989).
50. See, for example, "Challenge to State's Age Verification Law Dismissed," Utah Office of the Attorney General, published August 1, 2023, https://attorneygeneral.utah.gov/challenge-to-states-age-verification-law-dismissed/; "Attorney General Ken Paxton Sues Two More Pornography Companies for Violating Texas Age Verification Law," Texas Office of the Attorney General, published March 21, 2024, https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-two-more-pornography-companies-violating-texas-age-verification-law.
51. Michael B. Robb and Supreet Mann, "2022 Teens and Pornography" (Common Sense, January 2023), https://www.commonsensemedia.org/sites/default/files/research/report/2022-teens-and-pornography-final-web.pdf.
52. Daniel Castro, "Protecting Children Online Does Not Require ID Checks for Everyone" (ITIF, November 21, 2023), https://itif.org/publications/2023/11/21/protecting-children-online-does-not-require-id-checks-for-everyone/.
53. "Pessimists Archive," Pessimists Archive, accessed March 27, 2024, https://pessimistsarchive.org/.
54. "Obscene, Indecent and Profane Broadcasts," FCC, updated January 13, 2021, https://www.fcc.gov/consumers/guides/obscene-indecent-and-profane-broadcasts.
55. "History of Ratings," FilmRatings.com, accessed March 28, 2024, https://www.filmratings.com/History.
56. "Ratings Guide," ESRB, accessed March 28, 2024, https://www.esrb.org/ratings-guide/.
57. "AB-2273," California Legislative Information.
58. Marchese, "NetChoice v. Bonta."
59. 47 U.S.C. § 230.
60. Cristiano Lima, "Trump, Biden both want to repeal tech legal protections – for opposite reasons," *Politico*, May 29, 2020, https://www.politico.com/news/2020/05/29/trump-biden-tech-legal-protections-289306.
61. Ashley Johnson and Daniel Castro, "Fact-Checking the Critiques of Section 230: What Are the Real Problems?" (ITIF, February 2021), https://itif.org/publications/2021/02/22/fact-checking-critiques-section-230-what-are-real-problems/.
62. *Cubby, Inc v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991); *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995).
63. Ashley Johnson and Daniel Castro, "Proposals to Reform Section 230" (ITIF, February 2021), https://itif.org/publications/2021/02/22/proposals-reform-section-230/.

64. "S.3663 - Kids Online Safety Act," Congress.gov, accessed April 2, 2024, https://www.congress.gov/bill/117th-congress/senate-bill/3663/text; "S.1409 - Kids Online Safety Act," Congress.gov, accessed April 2, 2024, https://www.congress.gov/bill/118th-congress/senate-bill/1409.

65. Ashley Johnson, "Updated Children's Safety Bills Still Contain Serious Flaws" (ITIF, March 6, 2024), https://itif.org/publications/2024/03/06/updated-childrens-safety-bills-still-contain-serious-flaws/.

66. Alan McQuinn, "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules" (ITIF, October 6, 2017), https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules/.

67. Markus A. Landolt et al., "The Harm of Contact and Non-Contact Sexual Abuse: Health-Related Quality of Life and Mental Health in a Population Sample of Swiss Adolescents," *Psychotherapy and* Psychosomatics 85, no. 5 (2016): 320-322, https://doi.org/10.1159/000446810.

68. "Online Enticement," NCMEC, accessed March 26, 2024, https://www.missingkids.org/theissues/onlineenticement.

69. See, for example, Susan Jasper, "How we detect, remove and report child sexual abuse material," Google, October 28, 2022, https://blog.google/technology/safety-security/how-we-detect-remove-and-report-child-sexual-abuse-material/.

70. "NCMEC, Google and Image Hashing Technology," Google Safety Center, accessed March 27, 2024, https://safety.google/stories/hash-matching-to-help-ncmec/.

71. "S.3398 - EARN IT Act of 2020," Congress.gov, accessed April 2, 2024, https://www.congress.gov/bill/116th-congress/senate-bill/3398.

72. Ashley Johnson, "A Backdoor Attempt to Require Backdoors to Encryption," *Morning Consult*, March 11, 2020, https://morningconsult.com/opinions/a-backdoor-attempt-to-require-backdoors-to-encryption/.

73. Ashley Johnson and Daniel Castro, "The EARN IT Act Is a Threat to Privacy, Free Speech, and the Internet Economy" (ITIF, July 10, 2020), https://itif.org/publications/2020/07/10/earn-it-act-threat-privacy-free-speech-and-internet-economy/.

74. "S.3538 - EARN IT Act of 2022," Congress.gov, accessed April 2, 2024, https://www.congress.gov/bill/117th-congress/senate-bill/3538; "S.1207 - EARN IT Act of 2023," Congress.gov, accessed April 2, 2024, https://www.congress.gov/bill/118th-congress/senate-bill/1207.

75. "S.1199 - STOP CSAM Act of 2023," Congress.gov, accessed April 2, 2024, https://www.congress.gov/bill/118th-congress/senate-bill/1199/text.

76. Ashley Johnson, "Stopping Child Sexual Abuse Online Should Start With Law Enforcement" (ITIF, May 10, 2023), https://itif.org/publications/2023/05/10/stopping-child-sexual-abuse-online-should-start-with-law-enforcement/.

77. See, for example, "Monetization Policies," YouTube, accessed March 25, 2024, https://www.youtube.com/howyoutubeworks/policies/monetization-policies/; "Monetize on TikTok," TikTok, accessed March 25, 2024, https://support.tiktok.com/en/business-and-creator; "How to request monetization support for creators," Instagram, accessed March 25, 2024, https://help.instagram.com/167414052020731.

78. "Disclosures 101 for Social Media Influencers," FTC, November 2019, https://www.ftc.gov/system/files/documents/plain-language/1001a-influencer-guide-508_1.pdf.

79. Allied Market Research, "Influencer Marketing Market to Reach $199.6 Billion, Globally, by 2032 at 28.6% CAGR: Allied Market Research," *PR Newswire*, November 14, 2023, https://www.prnewswire.com/news-releases/influencer-marketing-market-to-reach-199-6-billion-globally-by-2032-at-28-6-cagr-allied-market-research-301987451.html.

80. See, for example, Valeriya Safronova, "Child Influencers Make Big Money. Who Gets It?", *The New York Times*, October 13, 2023, https://www.nytimes.com/2023/10/10/style/children-influencers-money.html.
81. Michael S. Rosenwald, "'I'll ruin you': Judy Garland on being groped and harassed by powerful Hollywood men," *The Washington Post*, November 14, 2017, https://www.washingtonpost.com/news/retropolis/wp/2017/11/14/ill-ruin-you-judy-garland-on-being-groped-and-harassed-by-powerful-hollywood-men/; Spencer Kornhaber, "Shirley Temple, the child Star Who Wasn't a Cautionary Tale," *The Atlantic*, February 11, 2014, https://www.theatlantic.com/entertainment/archive/2014/02/shirley-temple-the-child-star-who-wasnt-a-cautionary-tale/283747/; Alexis Petridis, "Joe Jackson was one of the most monstrous fathers in pop," *The Guardian*, June 27, 2018, https://www.theguardian.com/music/2018/jun/27/joe-jackson-one-of-the-most-monstrous-fathers-in-pop; Julia Jacobs and Joe Coscarelli, "'I Had Been Exploited:' Takeaways From Britney Spears's Memoir," *The New York Times*, October 19, 2023, https://www.nytimes.com/2023/10/19/arts/music/britney-spears-memoir-takeaways.html; Adrian Horton, "Demi Lovato says she was raped as a teenager by someone she knew," *The Guardian*, March 16, 2021, https://www.theguardian.com/music/2021/mar/16/demi-lovato-rape-youtube-docuseries-dancing-with-the-devil.
82. Maham Javaid, "Before child influencers, a 1920s movie star sued his mother for wages," *The Washington Post*, August 25, 2023, https://www.washingtonpost.com/history/2023/08/25/illinois-child-influencer-earnings-law-history-jackie-coogan/.
83. "Coogan Accounts: Protecting Your Child Star's Earnings," Morgan Stanley, October 18, 2023, https://www.morganstanley.com/articles/trust-account-for-child-performer.
84. Alex Ambrose, "Kidfluencers Recast Spotlight on Children's Rights in Digital Entertainment" (ITIF, September 5, 2023), https://itif.org/publications/2023/09/05/kidfluencers-recast-spotlight-on-children-s-rights-in-digital-entertainment/.
85. See, for example, Anne Branigin and Samantha Chery, "'Quiet on Set' alleges a 'dark underbelly' at Nickelodeon," *The Washington Times*, updated March 25, 2024, https://www.washingtonpost.com/style/2024/03/23/quiet-on-set-nickelodeon-dan-schneider-drake-bell/.
86. Johnson and Castro, "Maintaining a Light-Touch."
87. Daniel Castro, "Absent Federal IDs, Digital Driver's Licenses a Good Start," *Government Technology*, July 1, 2021, https://www.govtech.com/opinion/absent-federal-ids-digital-drivers-licenses-a-good-start.
88. Ashley Johnson, "AI Could Make Age Verification More Accurate and Less Invasive" (ITIF, April 5, 2023), https://itif.org/publications/2023/04/05/ai-could-make-age-verification-more-accurate-and-less-invasive/.
89. Ashley Johnson, "Stopping Child Sexual Abuse Online Should Start With Law Enforcement" (ITIF, May 10, 2023), https://itif.org/publications/2023/05/10/stopping-child-sexual-abuse-online-should-start-with-law-enforcement/.