TRUSTED FUTURE

AGE VERIFICATION

TECHNOLOGICAL OPTIONS, PARENTS, AND PROGRESS

MARCH, 2026

PROTECTING KIDS ONLINE SAFETY AND PRIVACY

WHILE GIVING FAMILIES THE TOOLS THEY NEED TO NAVIGATE TODAY'S DIGITAL WORLD WITH CONFIDENCE

HISTORICAL CHALLENGES & SILVER BULLET SOLUTIONS

1. How to protect kids online has historically been one of the hardest and most important set of policy issues facing policymakers, innovators and parents. Parents and their kids deserve comprehensive solutions that are not only effective, but that protect their safety, privacy, and constitutional rights.

2. We've been grappling with these issues for more than 30 years. And while technology has changed dramatically over that time, the basic challenges have not.

3. Policymakers still are looking for simple silver bullet solutions to what is a complex, multi-faceted set of issues. And the simple solutions are often:

    - Ineffective and unworkable,
    - can create substantial new privacy risks for all users – but especially kids,
    - raise important constitutional and legal concerns,
    - sometimes without effectively addressing the fundamental issues of how we create safer spaces for children online.

AGE VERIFICATION: A CURRENT FOCUS

About half of states have adopted laws mandating age verification in some form for accessing adult content or social media platforms. Some states are also proposing laws requiring parental consent when downloading apps. However, in many of these cases, courts have blocked the laws seeking to impose age-verification gates on apps, social media or the Internet.

OPPORTUNITIES FOR PROGRESS

Key opportunities exist for making major progress. Progress involves action from policymakers, innovators, and parents alike, and it can create a more positive digital environment for our kids.
In this brief, we explore:

1. How parents view these critical issues
2. The effectiveness of different age verification technological approaches
3. And look at some of the other tools in the policy toolbox that can produce progress

PARENTS ARE CONCERNED ABOUT ONLINE SAFETY & PRIVACY

WANT THEIR KIDS CONNECTED AND PROTECTED

Trusted Future (TF), the Family Online Safety Institute (FOSI) and others conducted national surveys to better understand the opportunities and challenges that parents are confronting today.

TO TACKLE THESE ISSUES, PARENTS ARE USING A VARIETY OF TOOLS

87% of parents → use some form of parental control tools to manage their children's digital lives.(FOSI)

3/4 of parents → set app restrictions on their children's devices (FOSI)

2/3rds of parents → have instituted restrictions on screen time (FOSI)

4 in 5 parents → find parental controls effective (FOSI)

But parental controls are underutilized on desktops **(46%)**, laptops **(43%)**, SmartTVs **(38%)** and game consoles **(35%)** compared to phones and tablets (FOSI) – suggesting areas of weaknesses.

PARENTS ARE ALSO ENGAGING DIRECTLY WITH THEIR KIDS

9 in 10 parents → (86%) believe talking with their kids about their family's rules and expectations is one of the most effective strategies for helping them establish good online habits. (TF)

89% of kids → say they feel comfortable turning to their parents if something online makes them feel unsafe (FOSI)

BUT PARENTS WANT MORE ACTION FROM COMPANIES AND POLICY-MAKERS: ESPECIALLY AROUND PRIVACY & SOCIAL MEDIA

90% of Americans → are concerned about social media platforms having the personal information of children. (Pew)

63% of parents → say their top priority from policymakers is adopting strong baseline privacy protections for children. (TF)

Almost all adults → (87%), including 90% of parents, agree that social media platforms have a responsibility to prevent kids from seeing inappropriate content. (Morning Consult/PPI)

TECHNICAL FEASIBILITY:

THE ADVANTAGE AND CHALLENGES OF DIFFERENT APPROACHES

NO AGE VERIFICATION TECHNOLOGY IS PERFECT, OR WITHOUT LIMITATIONS

01.

Basic Age-Gating Asking The User to Self-Attest

Its non-invasive and simple. The user is asked to check a box or enter their birthdate.

However, it relies on users being truthful about their age, and it's easy to lie.

Nearly **40% of children ages 8-12** use social media (US Surgeon General) even though 13 is the minimum age (COPPA)

1/3 of children lied about their age to social media companies (2022 Ofcom study)

Interestingly, only **5.4% of the kids** said they were keeping it secret from their parents.

Ofcom found that **2/3rds of those** below the age of thirteen on social media **had direct help from a parent** or guardian getting onto the platform.

So while **kids are lying to social media companies** about their age, they aren't lying to their parents about the accounts, and the parents are engaging with the teens as they sign up and engage.

02.

Age Estimation/ Prediction By Analyzing On-line Activity/Data

- Results in an estimated or approximate age.
- Often done **invisibly** to the user – **so it's a less intrusive approach.**
- Major social media platforms now often use a variety of techniques to infer your age – like analyzing the content of posts, looking for "happy birthday" messages, analyzing users viewing habits, or whether the e-mail is associated with a mortgage or utility bill.

- But it requires platforms to hoover up vast amounts of information & build intrusive digital dossiers about kids.
- Leads more intrusive monitoring of online activities – one of the primary concerns that parents have about social media companies.

90% → of AMERICANS are concerned about social media platforms having the personal information of children.(Pew)

42% → of PARENTS feel they have little or no control over the information social media platforms collect about their children (ICO)

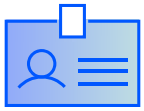
73% → of PARENTS are concerned about personal data being collected by third parties, without their consent. (TF)

These solutions are **designed for identifying underage** kids already on platforms – and because they rely on AI, they will likely get better with time.

03.

Age Estimation/ Through Facial Recognition

- This is a popular approach with some third-party age verification providers – but it's still early days.
- The National Institute of Standards and Technology (NIST) evaluated several provider's technology and found there were **over and under estimation errors of 3.1 years** which varies significantly based on **skin color, gender, and region of birth.**
- **In some cases, one-year age** estimation accuracy incredibly low for 13-year-olds: just **7.2% to 34.5%** of 13-year-olds were correctly estimated within one year of their actual age.
- The Federal Trade Commission (FTC) denied use of facial recognition age estimation technology for COPPA in 2024.
- Because its accuracy varies significantly based on skin color, **gender, and region of birth, or for people with** disabilities, it can also lead to discriminatory outcomes and exacerbate harms to already marginalized groups.
- **Like other AI enabled tools, facial recognition tools are likely get more accurate with time.**



04.

Age Verification Using Government Issued ID

Provides specific and reliable age and identity – but intrusive, and exclusionary

Intrusive: People are Reluctant to Provide IDs

- **2 out of 3 Americans** → are not comfortable sharing their identification document with social media companies.(CGO)
- **7 in 1 parents** → are uncomfortable sharing their child's government documents with social media companies.(CGO)

Exclusionary: Many (adults and teens) don't have acceptable IDs (The ID Divide)

- **21 million Americans** → lack driver's licenses. Another 28.6 million have licenses that aren't current. (UofM research)

- **60% of teens** → (15-19) lack drivers' licenses. (FHWA) 41% of 18–24-year-olds lack current license.
- **Over 25% of Black and Hispanic adult citizens** → don' have a current driver's license (UofM research)
- **2.6 million Americans** → lack govt photo ID—including homeless, recent immigrants.

Creates Major New Privacy Risks:
Often few specific limits on how companies collect, store, and protect sensitive data.
Introduces significant new privacy risks including data breaches, and chances for misuse.

05.

Age Estimation using credit card

Exclusionary: Same challenges as IDs

- About **1 in 6 households** (15.7%) → don't have access to a credit card (FDIC).
- **Kids under 18** → don't have credit cards.

Not always effective: Same challenges as IDs
Minors often use parents' cards with permission

06.

App Store Based Age Verification Policy Proposals

App Store Accountability Act (ASAA)

Unworkable and unconstitutional proposals

- Popular in Principle, Unworkable in Practice, Unconstitutional in law
- Shifts burden from social media apps to app stores.
- Parents must set up child accounts.
- Requires phones to share every user's age (including your child's) with every app developer, for every download -to pizza chains, retailers, etc.
- Every app developer must redesign their app to accept age data.
- Necessitates the widespread collection, storage, and dissemination of sensitive personal information, even when users are simply accessing lawful, general-purpose apps on their own devices.
- Adults need to surrender sensitive personal data as a condition of participating in the digital economy – a government ID or credit card.
- For example, if a 60-year-old wants to download a weather or news app, they'd still have to verify their age first, have it sent to the app, despite posing no age risk.
- Applies changes to **ALL 4 million apps**, by contrast Australia's social media age restrictions applies to just 10 targeted social media apps.

Major privacy risks for all

- It broadly expands potential privacy risks for adults and children
- **First**, takes away parents' existing choice to protect children's data from being shared with strangers.

- **Second**, it places few limits on how shared data can be used.
- **Third**, **85% of parents** are specifically concerned about protecting the privacy of data about their children's age. (TF Survey)
- **Fourth**, it creates a plethora of high-value "honey pots" of data stored by each developer filled with sensitive personal age data.
  - These honey pots are valuable targets for bad actors.
  - Data can be breached, misused, and exploited.
  - It's not hypothetical. Past breaches of age info has exposed millions of users to fraud, identity theft, and harassment.
  - Last July, Tea, a women's dating safety app which required a selfie and government ID breached exposing 72,000 women .
  - Discord breach exposed nearly 70,000 drivers' licenses and passports used for age verification.

Provides false sense of effectiveness

- **Clever kids can easily circumvent these restrictions** – simply by opening a browser on a laptop, computer or game console to access the same age-inappropriate content via the web version instead of trying to access the content through an app.
- **It also creates a shared use dichotomy** – for example sharing devices among multiple children is common. One tablet might be shared between a parent, a 14-year-old, and 10-year-old –who are in two different regulated age ranges but use the same device.

Shifts burden & Huge economic cost

- **Burden Shifting:** App Store Accountability Act (ASAA) (UT, TX, LA) is backed by META as a way to shift its burden from those hosting age-inappropriate content, to the entire mobile ecosystem.
- **Impact on Small Business: 90% of the 4 million apps** covered are small businesses (e.g. a local restaurant, bike shop, or retailer) that don't host age-inappropriate content yet are now burdened by requirements to update apps and comply.
- **Huge Economic Costs:** TF estimates **$20–80K per small developer** to comply. **$70 billion in total** compliance costs for the 3.5 million small app developers covered. (TF analysis)

Parents don't think it keeps kids safe

- **Ineffective:** Only **1 in 3 parents** think that this strategy keeps kids fully safe online.
- **Can't Let Social Media off the Hook: 90% of parents** agree that social media platforms have the responsibility to prevent kids from seeing inappropriate content like pornography or violence.
- **Lacks Continuous Protection: 70% of parents** want constant safety, not just a one-time check at moment of download.
- **Privacy Concerns: Over half (54%) of adults** say they do not trust apps to keep kids' age information secure from hackers or other bad actors. (Morning Consult/PPI)

Better alternatives exist

- **Knowledge of Content:** Apps and websites that host both adult and children's content know their content best and are generally better suited than app stores to design age-appropriate experiences and implement safety features that reflect the specific risks, content, and use cases of their services.
- **Movie Theatre Metaphor:** It's the movie theater in a shopping mall that is responsible for checking IDs for adult-rated films, and the mall restaurant who verifies age before serving alcohol, rather every person's ID checked when entering

the mall, even if someone is just going to the food court. Same should be true for app marketplace.

- **Create Better Age-Appropriate Experience**: Apps like HBO and Netflix host both adult and children's content and are better positioned to create age-appropriate experiences for their users.

Faces constitutional challenges

- **Violates Free Speech Protections of Adults and Minors:** Texas App Store Accountability Act (SB 2420) first to come into effect, and immediately enjoined by district court Judge Robert Pitman for failing to pass constitutional muster.
- **Unconstitutional:** In his decision, he likened app store age verification as "akin to a law that would require every bookstore to verify the age of every customer at the door and, for minors, require parental consent before the child or teen could enter and again when they try to purchase a book" and declared the law **"unconstitutional in the vast majority of its applications."**
- **Parents Already Have Control:** The judge said "This is the state doing it under the guise of parental control when the parents already have control."

07.

Age Range Solutions — Like Bipartisan Parents Over Platforms Act (HR 6333)

Avoids key weaknesses apparent in other proposals

THE FOUNDATION: Privacy, safety & parental control

- **Builds on new age range technologies** developed by Apple and Google to protect **BOTH privacy AND safety.**
- **Keeps parents in charge** with provisions that give parents a central toolkit to manage their child's online activities through the app store.
- **Equips parents with tools** that ensures their children can only download age-appropriate apps through app stores.
- **Allows apps to turn on safety features,** limit adult-only content, and block personalized ads to minors without collecting extra personal information or requiring intrusive age checks.

THE FRAMEWORK: Focused & privacy preserving

- **Utilizes privacy preserving age ranges** (child, teen, adult) – not specific birthdates.
- **Child's age signal is only shared with parental consent.**
- **Focused on limited number of high-risk apps** that host the age-inappropriate content.
- **Does not burden developers** that have no age-inappropriate content.
- **Shares responsibilities among players,** while strengthening protections for kids.

THE BENEFITS: Accountability & a national standard

- **Creates a national age assurance framework** for consistency across the country.
- **Strict limits on use of data** – imposes penalties on developers who misuse users' age information.
- **Prohibits data for targeted advertising** to children.
- Ensures developers of **high-risk social media apps are held fully accountable.**
- Strengthens protections and safety.

Courts have ruled that when less restrictive alternatives exist, governments must make use of them.

OTHER TOOLS IN THE POLICY TOOLBOX

Because there is more to making the Internet a good place for children than just protecting them from objectionable content.

EMPOWERING PARENTS WITH TOOLS TO PROTECT KIDS' PRIVACY AND SAFETY

FURTHER EMPOWER PARENTS WHO WANT TO BE ENGAGED

FOSI survey: Parents see themselves as having the most responsibility for managing access to age-appropriate content – more than developers or government. But they often lack information on tools and strategies that best meet their family's needs.

Promoting a Safe Internet for Minors Act (H.R.6289) would create resources and a national campaign for parents, educators, communities and kids to promote the safe use of the Internet.

ADVANCE RESEARCH ON AGE VERIFICATION TECHNOLOGIES

Because age verification technologies all have limitations, the Kids Online Safety Act (S. 1748) directs federal agencies to study their technology feasibility including their privacy risks – so we can better understand limitations and improve their effectives.

BOOST ONLINE SAFETY BY IMPROVING DIGITAL LITERACY SKILLS

And at least half of U.S. states have now enacted laws to improve media literacy education for kids. Federal efforts are also aimed at boosting online safety through curriculum developed by education experts to help kids learn about the online world in a way that helps them become productive digital citizens.

IMPROVE NATIONAL BASELINE PRIVACY PROTECTIONS FOR CHILDREN

90% of parents are concerned about protecting the privacy of their children online, and 4 out of 5 parents (85%) are specifically concerned about protecting the privacy of their children's age.

Bipartisan Children and Teens' Online Privacy Protection Act (COPPA 2.0) strengthens privacy and bans targeted ads to children and teens.

PUSH INNOVATORS TO ADOPT BETTER SAFETY MEASURES AND CREATE AGE-APPROPRIATE EXPERIENCES

In the absence of legislation, developers today can already begin taking advantage of smartphone provided age-range signals (if parents choose to share) to create age-appropriate experiences, and new tools that put parents in control.


TRUSTED
FUTURE
.org