



March 11, 2024

Federal Trade Commission, Office of the Secretary
600 Pennsylvania Avenue NW, Suite CC-5610 (Annex E)
Washington, DC 20580

COPPA Rule Review, Project No. P195404

Introduction

The Family Online Safety Institute (FOSI) appreciates the opportunity to contribute to the Federal Trade Commission (FTC) Request for Comment (RFC) on the COPPA Rule proposed modifications, [16 CFR Part 312, Federal Register Number 2023-28569](#).

[FOSI](#) is an international, non-profit, membership organization working to make the online world a safer place for children and their families. We achieve this by identifying and promoting best practices, tools, and solutions in the field of online safety. FOSI convenes leaders in industry, government, academia, and the non-profit sectors to collaborate and innovate new solutions and policies that ensure a safer, more rewarding digital experience for all. Through research, resources, events, and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all.

FOSI defines online safety as *acknowledging the risks and mitigating the harms in order to reap the rewards of digital life*. We believe that online safety and data privacy are complementary parts to protecting young people online, and we are glad to see the FTC thoughtfully approach these issues as it seeks to update guidance for the most significant federal children's privacy law.

What Congress can do

First and foremost, as an online safety organization, we believe that COPPA is and should remain a children's privacy law. While privacy protections can be an important precursor to safety regulation, as discussed below, the best way to improve online safety is to pass a law specifically focused on safety, rather than adapt a notice and consent privacy law into a safety one.

We understand that this request for comment is focused on the COPPA Rule and the FTC is limited in how much it can do without additional action in Congress, but we want to take a moment to acknowledge the essential role that Congress plays in keeping young people and their data safe and secure.

In the 26 years since COPPA was passed into law there have been significant changes both in technology and in how people use online platforms and services. FOSI believes that a federal comprehensive data privacy law is long overdue. If additional protections for young people are not addressed in a comprehensive law, COPPA must be significantly updated and expanded to better protect young people online. All Americans, especially children and teenagers, need data privacy protections.

While the FTC has taken significant action to protect children online, it is limited to working within the confines of the statutory text. New privacy legislation would better equip the FTC to improve online experiences for children, teens, and adults. Until legislative updates occur, the FTC will be disadvantaged compared to its international regulatory cousins that are armed with modern and comprehensive direction and authority.

The FTC certainly retains important powers and has demonstrated its strong enforcement abilities in recent years. However, as online safety and privacy become priorities for lawmakers around the world, other regulatory agencies have seen significantly increased investment. Congress must work with the FTC to ensure the Commission has the resources, personnel, and expertise needed to continue to be a top investigative and enforcement agency on the global scale.

While Congress has stalled, states have begun passing their own data privacy laws, with [more than a dozen](#) already enacted across the country. With baseline privacy protections long overdue, individual state actions exacerbate the need for a federal comprehensive law. The developing state by state patchwork of privacy laws makes it difficult for consumers to know their rights, and also presents new compliance challenges for industry. A federal law would give clarity and confidence to people exercising their online rights and to businesses working to comply with the law.

Questions in the RFC

[Questions 9 and 15](#) in the RFC stood out to us as they focus on using personal identifiers to increase a child's time on a service, and whether the FTC should prohibit such use. Prolonged engagement appears to verge into the categories of online safety and harm prevention, as opposed to only the collection of data. FOSI certainly opposes using children's data to manipulate them into prolonged engagement, including related dark patterns that could expose children to additional risks. We would like to direct the FTC to the work that the [UK Information Commissioner's Office](#) (ICO) has done on this topic with its development and implementation of the [Age Appropriate Design Code](#) (UK AADC).

Built on top of a national data privacy law, the UK AADC takes a considered approach to minimize harms to young people online. [Standard 13: Nudge Techniques](#) may be of particular interest to the FTC in that it provides recommendations for online platforms to nudge young users toward taking breaks and using design features like pausing and saving progress. These nudges are one way to discourage prolonged engagement and direct young users towards “wellbeing enhancing behaviors”. We encourage the FTC to learn from its peers in the UK who have spent years navigating the difficult tradeoffs in pursuit of an age appropriate internet.

[Question 11](#) in the RFC addresses the importance of operators knowing the age of their users. While utilizing age assurance processes is not a silver bullet that will solve all online safety problems, it does hold considerable promise in improving online safety for many young users by offering age appropriate online experiences.

FOSI would like to highlight the important nuance between age assurance and age verification by starting with definitions. FOSI uses “age assurance” as a broad term that describes various methods to discern the age or age-range of an online user, including age verification, age estimation, and age gating. This distinction is well-documented in the [guidance produced by the UK ICO](#). The ICO describes a risk-based approach, where certain age assurance processes are more appropriate than others depending on the level of risk posed to a young user. A self-declaration pop-up or age gate may be appropriate for services or products that present minimal levels of risk, whereas a form of age verification that offers a higher level of accuracy and certainty makes sense in order to gain access to more dangerous experiences such as violent content and products, online gambling, and purchasing alcohol or tobacco. A considerable benefit of establishing such a risk-based system is that online platforms have multiple options to present to users.

This topic is another area where state legislatures have acted, as multiple states have passed their own age verification laws. Unfortunately, they do not approach this complicated issue with the nuance necessary to balance safety and privacy. As the ICO has documented, risk-based systems with more flexibility and choices for consumers are better than overly-prescriptive regulation. Anyone looking to regulate age assurance processes, including the FTC, Congress, and state legislatures, should look to the ICO to learn from its work and thorough guidance.

Another lesson we have learned from the UK is the importance of guidance and communication with industry. The ICO has produced substantial [guidance and resources](#) to help industry understand how to comply with the AADC. The ICO understands that with widespread compliance comes an increase in safer online experiences for young users. A collaborative regulatory approach between regulators and industry has made the UK’s risk-based age assurance model successful in increasing online safety and privacy.

FOSI released [original research from 2022](#) about age assurance that highlights important family perspectives that should be taken into account by policymakers. FOSI also produced a [white paper](#) after a year-long working group that outlines some of the key tradeoffs of implementing age assurance processes, especially discussing the balance between invasiveness and effectiveness.

The Future of Privacy Forum created an [informative infographic](#) demonstrating the age assurance process with specific examples. The University of North Carolina and the Center for Growth and Opportunity at Utah State University produced another [particularly helpful paper](#) that clearly lays out tradeoffs and recommendations for regulators considering age assurance. For additional resources on age assurance and thoughtful perspectives across the world, please see the [Age Verification Provider's Association](#) and Europe's [euCONSENT](#) work.

There is near unanimous agreement that simple age gates to protect children and their data are not good enough. But improvements must be made by thoughtfully considering the tradeoffs of different age assurance approaches and finding the balance between privacy and safety.

Conclusion

FOSI commends the FTC for taking such a thoughtful and considered approach to the COPPA Rule proposed modifications process. It is clear that the FTC is using every available resource to make important regulatory updates to the foundational data privacy law in the US. However, despite its best efforts, the FTC cannot fully improve online privacy and safety on its own. Congress must act to establish data privacy protections for all Americans, whether through a comprehensive law or significant updates to COPPA. While the FTC needs a considerable investment in resources and personnel to effectively carry out its mission, it can also learn from its regulatory cousins around the world who have produced thoughtful and well-researched guidance and resources, especially the ICO.

Thank you for the opportunity to comment. FOSI looks forward to working with the FTC on these important online privacy and safety issues.

Respectfully submitted,

Andrew Zack
Policy Manager
Family Online Safety Institute