Comment of Jennifer Huddleston, Technology Policy Research Fellow, Cato Institute and David Inserra, Fellow for Free Expression and Technology, Cato Institute in response to Initiative to Protect Youth Mental Health, Safety, and Privacy Online

We appreciate the opportunity to provide comments related to the National Telecommunications and Information Administration (NTIA)'s questions on Youth Online Safety and Mental Health. This comment does not represent the views of any particular party or special interest group but is intended to assist regulators in considering the impact of potential actions on young people, parents, innovators, and all internet users.

Many are concerned about the issue of youth mental health and the perception that there is an uptick in problems among children and teens. However, the research to prove a causal link between social media use and such concerns is not currently available[1] and concerning trends around youth mental health pre-date most of the concerns about social media use.[2] The underlying concerns about youth mental health are well intentioned. However, such problems rarely have one-size-fits-all solutions and are much more complicated.

Social media has been beneficial to young people in various ways, such as through the emergence of communities consisting of people that may have been more at risk of suicide or self-harm, or may have experienced fears around lack of acceptance.[3] Particularly during the COVID-19 pandemic, the internet and social media provided ways for people of all ages — including teenagers — to stay connected to friends and family and form new connections while in physical isolation.

A variety of tools are already available for parents at many different points in the internet ecosystem to respond to the wide array of concerns they may have about their child or teen's technology use, ranging from time limits to parental notifications to the ability to block specific types of content. In short, the market continues to respond to the concerns of parents and society by providing more options to personalize and improve experiences online.

With this framing in mind, we would like to highlight two key points:

1. The potential privacy implications of government age-verification requirements.
2. Alternative policy tools that focus on empowerment rather than restriction.

Privacy Implications of Age-Verification Requirements on All Consumers

Many proposals at both the state and federal level treat all young users under 18 the same, advocating for parental oversight through mandatory age verification for all minors; however,

---

[1] Jeffrey A. Singer, "Prosecutors Turn Their Extortion Racket Against Facebook and Instagram," *Reason*, October 26, 2023, https://reason.com/2023/10/26/prosecutors-turn-their-extor9on-racket-against-facebook-and-instagram/.

[2] Taylor Barkley, "The Problems of Teen Suicide and Self-Harm Predate Social Media," *The Center for Growth and Opportunity*, June 8, 2022, https://www.thecgo.org/benchmark/the-problems-of-teen-suicide-and-self-harmpredate-social-media/.

[3] Claire Cain Miller, "For One Group of Teenagers, Social Media Seems a Clear Net Benefit," *New York Times*, May 24, 2023, https://www.ny9mes.com/2023/05/24/upshot/social-media-lgbtq-benefits.html.

this approach has far-reaching implications and goes much further in its requirements than current Children's Online Privacy Protection Act (COPPA) expectations. The proposed age verification methods impact not only the privacy rights of older minors but of all users of the internet.

Even if, in theory, restricting internet access based on age seems to pose no privacy issues, the practical application of these measures could significantly heighten the risk to minors' data and have implications on all internet users. Relying solely on internal mechanisms for age verification is not sufficient under much of the considered legislation, and many of these laws place a higher burden that will be more difficult to assess.

To prove that someone is not a minor, these requirements would apply to adult users as well as those underage. These underlying requirements will result in companies having access to the IDs or biometrics of all internet users, raising concerns about the privacy and data security of such information as well as the potential surveillance risks that comes with government access to such data. Further, it is difficult to understand how such scenarios might work on a shared device such as a gaming console or tablet, for example, that might be passed between family members of multiple ages without separate profiles. The widespread age verification requirements will also negatively impact all users' online experiences, as they are required to verify their identity across each online service or app store. The impact may range from a potentially frustrating DMV-like experience to the nuisance of consenting to website cookies or GDPR-required data notices.[4]

Determining the accurate ages of children online invariably involves assessing the ages of all users, a task where not infringing on everyone's privacy is nearly impossible. Consequently, if businesses opt to avoid the complexity and potential legal ramifications of age verification, they might choose to universally restrict access to content, applying the same standards to adults as to children. This approach effectively reduces the diversity and richness of online content to what is deemed appropriate for the youngest users. Adults, therefore, may find their access to a wide range of content — from news and entertainment to forums for political or social discussion — considerably limited.

Alternatively, businesses that decide to implement age verification for all users create a different set of challenges. This process often requires users to submit personal identification documents or biometric data, which can be intrusive and raise significant privacy concerns. Moreover, this could deter many adults from participating in online spaces due to the fear of their personal information being mishandled, or simply out of a desire to protect their privacy. The result is a chilling effect on free speech, as adults will self-censor or withdraw from online platforms to avoid these privacy invasions.

Alternative Policy Tools: Education and Empowerment over Education

As mentioned earlier, tools are available at every level of the stack, but many parents are often overwhelmed by the pace of today's technology or unaware of the options available to them. Rather than turn to regulation or requirements that presume a market failure, policymakers

[4] Kate Fazzini, "Europe's sweeping privacy rule was supposed to change the internet, but so far it's mostly created frustration for users, companies, and regulators," *CNBC*, May 5, 2019, https://www.cnbc.com/2019/05/04/gdprhas-frustrated-users-and-regulators.html.

should consider how education can improve awareness of what already exists. Education, rather than regulation, can imbue young people and parents with a greater sense of empowerment and agency, enabling them to have more positive experiences with technology and the knowledge of what to do should negative experiences arise.

Government need not invent these resources themselves. For example, recent work by the Competitive Enterprise Institute provides a list of dozens of tools available to parents to improve online safety at every level of the technological experience.[5] Groups like the Family Online Safety Initiative and Connect Safely have various tools available to help parents have difficult conversations around technology with young people. Agencies like the NTIA could help further the reach of available resources by pointing to a wide variety of options from civil society without directly endorsing them. This approach would increase the accessibility of such resources to parents who may feel overwhelmed and not know where to start.

In addition to resources for parents and adults, such conversations should also include the young people themselves so that they can understand both the benefits they find of being online as well as the negative situations they could encounter. Ideally, this approach can give a better understanding of what offline issues might be converging with online scenarios — both good and bad — and place industry, civil society, and parental responses more firmly in the actual experience of young people today. Presumptions of the past should not be used to promote one-size-fits-all solutions today.

Importantly, we would note that government support in the form of education and sharing the best practices and tools of civil society does not mean that the NTIA or other federal agencies should require or inappropriately pressure the private sector into the implementation of certain best practices. Online platforms take many different forms and provide a range of experiences and spaces for various types of users, leading to a range of different tools and resources for users and parents of users. Regulation and jawboning should not compel a platform's speech or ability to provide users with a specific type of experience. Such efforts could also chill the development of new safety-enhancing tools that private actors may develop to further empower young people and parents online.

Conclusion

Most adults want to help keep young people safe on their journey to adulthood, both in their online experiences as well as their offline experiences. However, online experiences — much like offline experiences — vary widely for children, teenagers, and adults. As a result, a one-size-fits all policy approach is likely to have many potential negative tradeoffs, particularly around privacy and speech for all internet users. To help families navigate experiences with technology, policymakers should look at ways to encourage education around available tools and rather than rely on blunt regulation.

[5] "Children Online Safety Tools," Competitive Enterprise Institute, accessed November 16, 2023, https://cei.org/children-online-safety-tools/.