CENTER FOR
DEMOCRACY
& TECHNOLOGY

November 16, 2023

To: National Telecommunications and Information Administration
Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230

Re: Initiative To Protect Youth Mental Health, Safety & Privacy Online Request for Comment, NTIA–2023–0008

Introduction

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the National Telecommunications and Information Administration's (NTIA) request for comments regarding efforts to protect youth mental health, safety, and privacy online. CDT is a nonprofit 501(c)(3) organization fighting to advance civil rights and civil liberties in the digital age for all users, including children. For example, CDT advocates for greater privacy protections,[1] protecting users' rights to access information freely,[2] and ensuring online services enable individuals to exercise choice and control over their online experience.[3] CDT has also promoted norms around responsible use of data and technology by education institutions,[4] and written extensively about the implications of student activity monitoring systems.[5]

Protecting children online is a critical priority. But that goal must be pursued in a manner that does not cause more harm than it brings benefits. Some proposals, while well-intentioned, may

[1] Eric Null, *We Should Protect Children's Privacy Through a Comprehensive Federal Privacy and Civil Rights Bill - Center for Democracy and Technology*, (March 22, 2022)
[2] *CDT Comments to the FTC on the 2010 COPPA Rule Review*, (June 30, 2010)
[3] Michal Luria and Carol F. Scott, *More Tools, More Control: Lessons from Young Users on Handling Unwanted Messages Online - Center for Democracy and Technology*, (November 8, 2023)
[4] Kristin Woelfel, *et al.*, *Late Applications: Protecting Students' Civil Rights in the Digital Age - Center for Democracy and Technology* (September 20, 2023); Dhanaraj Thakur and Elizabeth Laird, *Beyond the Screen: Parents' Experiences with Student Activity Monitoring in K-12 Schools - Center for Democracy and Technology*, (July 31, 2023)
[5] Hugh Grant Chapman, *et al.*, *Student Activity Monitoring Software: Research Insights and Recommendations - Center for Democracy and Technology*, (September 21, 2021)

actually jeopardize the safety and well-being of the youth they are intended to protect and undermine their rights, as well as those of adults.[6]

These comments discuss four ways in which initiatives to protect children can undermine the safety, well-being, and rights of all users, adults and children alike, and impede services offered by educational institutions:

- **Approaches to children's safety should not legitimize or facilitate content-based restrictions.** Many approaches to protecting young children rest on the premise that certain types of content are harmful to children. Studies are divided regarding the impacts of online content on children and on the question of what the right solutions to protect children should be. What is certain is that baking this principle into law and imposing a legal obligation on online service providers to filter out potentially harmful content under the threat of liability will create incentives for online services to err on the side of caution and over-filter content, undermining the right to free expression and minors' access to information. In past instances, for example, the use of filtering technology has led to lawful content related to LGBTQ+ identity being over-removed impeding all users' ability to seek important information.

- **Expanding surveillance of young people by parents and through the use of school monitoring systems will undermine young people's rights, particularly teens' right to privacy.** Teenagers, especially older teens aged 15 and 16, have a reasonable need for privacy and private channels through which to access and exchange information. However, mandating the availability of parental surveillance mechanisms and student activity monitoring systems undermine young peoples' ability to seek information securely and lead to decreased teen independence, which researchers say correlate with negative mental health consequences.[7] Additionally, surveys of educators and students conducted by CDT found that overbroad use of student activity monitoring systems led to increased encounters with law enforcement for young people of color and inadvertent outings of LGBTQ+ teens.[8]

[6] Aliya Bhatia, *Senate Commerce Should Reject Bills Jeopardizing Online Safety for Kids and Adults - Center for Democracy and Technology*, (July 25, 2023); See also: Beyond the Bailout: Congress Passes a Flurry of 'Child Safety' Bills - Center for Democracy and Technology (October 6, 2008)

[7] Peter Gray, *et al.* *Decline in Independent Activity as a Cause of Decline in Children's Mental Well-being: Summary of the Evidence - The Journal of Pediatrics* (September 2023); Kathryn Jezer-Morton, *Childhood Independence Is a Mental-Health Issue*, The Cut, (October 29, 2023)

[8] Elizabeth Laird and Aaron Spitler, *Brief – Hidden Harms: Increased Law Enforcement Interactions - Center for Democracy and Technology* (November 17, 2022)

- **Explicit or implicit age verification or assurance requirements to determine which users are children can undermine the privacy of both minors and adults by mandating more data collection, as well as potentially violate the right to speak and access information anonymously**. Approaches to estimate and/or verify the ages of all users in order to identify child users will require further data collection and processing for children and adults alike and eliminate the ability for all users to seek information anonymously. Further, age estimation and identity verification systems can have discriminatory effects. For example, facial analysis methods to estimate age may perform poorer on faces with different morphologies due to cognitive or physical disabilities, trans and non-binary faces, and non-white faces.

- **Efforts to protect children should account for the unique needs for educational institutions.** Schools and other educational institutions, including vendors of education technology, should not be treated the same as commercial actors so as not to inadvertently undermine educational services. Subjecting education providers and local education agencies to certain privacy provisions such as data deletion rights and data minimization protections may inadvertently undermine education service delivery by, for example, enabling parents to delete their children's grades or attendance records.

NTIA should recommend and advance proactive approaches to protecting young people online that avoid these pitfalls. These include:

- Establishing comprehensive federal privacy protections to protect children as well as adults;
- Promoting the development and deployment of user tools that empower young people online and help them shape their online experiences;
- Investing in more research to better understand the harms different groups of minors face online and the causes of those harms; and
- Developing dynamic and age-appropriate education and digital literacy initiatives to equip young users with the knowledge and responsible use practices to help them navigate the digital ecosystem.

I. Important considerations to promote young peoples' rights to privacy, access to information, and safety

A. Approaches to children's safety should not legitimize or facilitate content-based restrictions.

Many efforts to protect children since the rise of the internet have included restrictions on access to lawful content.[9] In fact, childrens' safety is currently being invoked to justify unconstitutional book bans,[10] changes to curriculum,[11] and restrictions on conduct across the nation.[12] Recent approaches to protecting children online often introduce broad restrictions on access to lawful content by introducing vague "duty of care" standards enforceable by State Attorneys General or by requiring platforms to "prevent and mitigate" harms or risks to young peoples' mental health.[13]

Approaches that seek to protect children by restricting content are problematic for several reasons. Broad content-based restrictions hurt young people, particularly teenagers, who need to access important information, particularly as they graduate and enter higher education and the workforce. In some states, teenagers can begin to work, marry, and make their own healthcare decisions starting at the age of 16, requiring unrestricted access to information to inform their decision-making. Children who grow up in highly restricted environments or face parental or domestic abuse in particular have a strong need for access to information and private communications channels to ensure their safety and mental health.[14] According to the American Psychology Association, imposing barriers to accessing reproductive services will lead to a decline in mental health.[15]

Moreover, no consensus exists as to what content should be restricted. Researchers are divided on what type of content and online services are and are not harmful to young people.[16] In practice, this means that those charged with enforcing such laws are left to make often politicized decisions to curtail access to lawful speech they claim leads to adverse mental health

[9] *Transition Memo: Preserving Free Speech on the Internet | Center for Democracy & Technology*, (November 13, 2008)

[10] Eesha Pendharkar, *State Laws Are Behind Many Book Bans, Even Indirectly, Report Finds*, Ed Week (May 19, 2023)

[11] Nicquel Terry Ellis, *Florida's new standards on Black history curriculum are creating outrage | CNN*, (August 17, 2023)

[12] LGBTQMap, *Restrictions on Drag Performances*

[13] Kids Online Safety Act (S. 1409 - 118th Congress); Utah Social Media Regulation Act; Louisiana Measure on Social Media ; Age-Appropriate Design Code Act (New Mexico); California Age Appropriate Design Code Act. See also: Makena Kelly, *Child Safety Bills are Reshaping the Internet for Everyone*, The Verge (August 29, 2023)

[14] Terry Gross, *How Twitter Helped Change The Mind Of A Westboro Baptist Church Member : NPR* (October 10, 2019)

[15] *Restricting access to abortion likely to lead to mental health harms, APA asserts*, American Psychological Association, (May 3, 2022)

[16] Candice L. Odgers and Michaeline R. Jenson, *Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review*, Journal of Child Psychology and Psychiatry, (January 17, 2020)

outcomes or other harms to minors, including information related to reproductive healthcare and LGBTQ+ identity that might be of particular importance to vulnerable youth.[17]

The threat of enforcement action and potential liability, in turn, will lead online services to err on the side of over-filtering content to reduce their risk. That is what has happened in the past in response to overbroad but well-intended laws that imposed content-based restrictions like FOSTA-SESTA (the Allow States and Victims to Fight Online Sex Trafficking Act and Stop Enabling Sex Traffickers Act) or CIPA (the Children's Internet Protection Act).[18] FOSTA prohibited online services from "promoting or facilitating sex trafficking". Several online platforms made changes to their terms of service to restrict content. For example, Craigslist immediately closed its "Personals" page, writing, "US Congress just passed HR 1865, 'FOSTA', seeking to subject websites to criminal and civil liability when third parties (users) misuse online personals unlawfully. Any tool or service can be misused. We can't take such a risk without jeopardizing all our other services, so we are regretfully taking Craigslist personals offline."[19] Schools and libraries have similarly found that content filters used to comply with CIPA have prevented students from accessing content related to LGBTQ+ identity entirely.[20]

In order to proactively comply at scale with obligations to prevent and mitigate harms to youth borne from content, online services are likely to use content filtering techniques to enforce their policies and remove content the platform thinks may put them in the crossfire of a regulator.[21] Content filtering tools are automated systems that detect and evaluate text or multi-modal content using keyword filtering or hash matching techniques.[22] In keyword filtering, the text of a post is evaluated against a set of words or phrases that have been blacklisted. In hash-matching techniques, an online service creates an alpha-numeric string of code (also called a hash) for a new image and checks it against a database which contains hashes for known images that a

[17] Emma Llansó, *CDT, Civil Rights Orgs Urge Congress to Not Advance KOSA, Detailing Continued Risks to Minors and LGBTQ+ Teens*, Center for Democracy & Technology, (December 16, 2022); Bhatia, *Senate Commerce Should Reject Bills Jeopardizing Online Safety for Kids and Adults | Center for Democracy and Technology*, (2023)

[18] Clare Mathias, *What 'Woodhull' Won't Change: Five Years of Chilling Effects Under FOSTA | Center for Democracy & Technology*, (October 27, 2023)

[19] About FOSTA | Craigslist

[20] Hannah Dellinger, *Katy ISD blocks LGBTQ+ resources, suicide prevention websites from students*, Houston Chronicle (November 24, 2021)

[21] Content removal mechanisms may be proactive (a human moderator flags posts prior to publication or a platform uses automated content analysis systems which evaluate or detect content) or reactive (a user or a court order flags a piece of content to an online service's attention for removal).

[22] See: Natasha Duarte and Emma Llansó, *Mixed Messages: The Limits of Automated Social Media Content Analysis | Center for Democracy & Technology*, (November 28, 2017); Dhanaraj Thakur and Emma Llansó, *Do You See What I See | Center for Democracy & Technology,* (May 20, 2021)

platform does not want to host.[23] Increasingly, online services are also using large language models to moderate content.[24]

CDT has conducted research into these automated content analysis systems and found that their use can result in overbroad censorship and biased enforcement of online services' terms of service.[25] Automated content analysis systems are unable to parse the intent of a post, which can result in an enforcement action on a post that does not violate a platform's policy. For example, a keyword filter may be trained on terminology used by proponents of eating disorders like "thinspo" or "thinspiration" to detect and enforce a service's policy against content that promotes eating disorders. However, an academic study conducted of eating disorder communities on Tumblr found that accounts that seek to educate and promote recovery for those suffering from eating disorders also use the same keywords and "linguistic style markers" that pro-eating disorder accounts use in order to reach pro-eating disorder audiences and encourage them to seek support and recovery.[26] As a result, a filter tuned to detect and prevent the spread of content that promotes eating disorders using a set of keywords is likely to remove access to critical information providing care for those suffering from eating disorders.

Attempting to protect minors by restricting access to content also raises significant constitutional concerns. Government restrictions on speech are generally unconstitutional and will harm the free expression rights of online services that publish and host user-generated speech and more importantly, the rights of users who have the right to access constitutionally-protected information. Moreover, effectively mandating the use of content filters may also be unconstitutional as content filters may enact prior restraints on speech. Filtering all user-generated speech at the point of upload bears many of the characteristics of a prior restraint on speech by requiring approval by a gatekeeper, in this case an online intermediary compelled by a state actor, before they are allowed to speak or publish their views.[27]

[23] Thakur and Llanso, *Do You See What I See?*, (2021)

[24] Increasingly, online services are also using large language models to moderate content, see: Lilian Weng, *Using GPT-4 for content moderation*, Open AI, (August 15, 2023); New research by CDT also found that the shortcomings of these automated content analysis methods are likely to be exacerbated when applied to detect and take action on speech in non-English languages. See Gabriel Nicholas and Aliya Bhatia, *Lost in Translation: Large Language Models in Non-English Content Analysis - Center for Democracy and Technology*, (May 23, 2023)

[25] See Mixed Messages and Do you See What I See

[26] Munmun De Choudhury, *Anorexia on Tumblr: A Characterization Study*, ACM (May 18, 2015)

[27] Emma J. Llansó, *No amount of "AI" in content moderation will solve filtering's prior-restraint problem*, Big Data & Society (April 23, 2020)

B. Expanding surveillance of young people by parents and through school devices will undermine the privacy and safety of young people, particularly marginalized young people.

Many recently introduced state and federal online child safety bills would require mandatory parental and/or educator surveillance of children's online activities. Proposed bills require online service providers to enable parents and caregivers to control their children's online activity.[28] For example, they may require online service providers to enable parents and/or caregivers to control who their child can be in contact with and view their child's online activity, which could include anything from their search history, URLs they have accessed, and the contents of their private messages.[29] Some state laws even require teenagers to seek parental consent before accessing online services.[30] Education agencies and edtech vendors have also interpreted some pieces of legislation to require monitoring of students' online activity.[31]

Mandating parental consent and surveillance of online activities often will do more harm than good, particularly for vulnerable teenagers. Young people, particularly older teens, have a reasonable need for privacy especially when seeking sensitive information about their health or identity. In instances where a young person does not have a healthy relationship with their family, for example if they are facing parental abuse[32] or they are questioning their sexual identity in a family of unsupportive caregivers, preserving privacy is critical for young peoples' safety.[33] The Trevor Project writes that nearly a third of LGBTQ+ teens face housing instability because of their identity and 16 percent have run away from home due to unsupportive parents.[34]

In recently released research, CDT spoke with thirty-two teenagers about their use of private messaging services to understand the unwanted encounters they face online and found that overwhelmingly, teenagers want the ability and autonomy to ask for help when they need it, rather than be monitored online 24/7.[35] Only 6% of unwanted messages were shared with

[28] Llansó, CDT, Civil Rights Orgs Urge Congress to Not Advance KOSA, Detailing Continued Risks to Minors and LGBTQ+ Teens, (2022); Bhatia, Senate Commerce Should Reject Bills Jeopardizing Online Safety for Kids and Adults (2023)

[29] Alfred Ng, Where parental snooping is becoming the law | POLITICO, (April 11, 2023)

[30] Ben Goggin, Utah governor signs laws requiring parents' consent for minors to use social media, NBC News (March 23, 2023)

[31] Cody Venzke, CDT Calls for Congress to Clarify the Privacy Impacts of CIPA, Center for Democracy & Technology (September 27, 2023)

[32] Anna Nikupeteri, *et al.*, Coercive control and technology-facilitated parental stalking in children's and young people's lives in, Journal of Gender-Based Violence (October 1, 2021)

[33] Carlos Gutierrez, Legislative Parental Consent Requirements | LGBTTech, (October 11, 2023)

[34] Homelessness and Housing Instability Among LGBTQ Youth | The Trevor Project, (February 3, 2022)

[35] Luria, More Tools, More Control, (2023)

caregivers. In interviews with participants, they explained that they would turn to parents or another trusted adult only in a more severe case that they feel would require adult intervention or support. The vast majority of participants reported taking intentional and calculated steps to prevent unwanted messages from coming into their accounts and wanted to maintain autonomy in managing their response to ones that do, including going to an adult when needed.

CDT conducted polling this summer of teen-aged students, which includes some unreleased figures about student perceptions of parental access to their online content. Our findings reveal that only about 50 percent of students report that they would be comfortable with their parents seeing a report of all of their online activity at school, with that number being significantly lower for LGBTQ+ students at 35 percent.[36] Students express even less support for their parents being able to see a report of all of their online activity, in school and out: 42 percent of all students said they would be comfortable with this, while again, LGBTQ+ students report a much lower number at 24 percent. In line with these views, 67 percent of students said they would be likely to turn off their parents' ability to see their online activity if they could, and LGBTQ+ students would be even more likely at 74 percent.[37]

Psychologists and healthcare professionals agree and note that requiring parental surveillance undermines teen autonomy, which is crucial for their development and mental health. A paper recently released by the Journal of Pediatrics conducted a survey of existing research, which found that increased monitoring by parents is correlated with a decline in independence for young people that can have negative consequences for young peoples' mental health.[38]

Simultaneously, the COVID-19 pandemic and increase in school shootings has also led to an increase in the use of monitoring software in schools, which similarly can do more harm than good. Polling conducted by CDT found that 88 percent of teachers reported that their school uses some kind of monitoring technology on either school-issued or personal devices.[39] Of this 88 percent, two-thirds report that the use of this technology led to a student being disciplined in school, and 38 percent reported that it led to contact with law enforcement. For marginalized students, these numbers are even higher. Licensed special education teachers and teachers in Title I schools reported higher incidences of law enforcement contact, at 46 percent and 42 percent, respectively. In addition to discipline and contact with law enforcement, LGBTQ+

[36] Elizabeth Laird and Maddy Dwyer, *Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI*, Center for Democracy & Technology, (September 20, 2023)

[37] *Ibid*

[38] Gray *et al.* *Decline in Independent Activity as a Cause of Decline in Children's Mental Well-being* (September 2023);

[39] Laird and Dwyer, *Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI*, (2023)

students experience unique harms: 19 percent of students report that they or someone they know was outed as LGBTQ+ as a result of this technology.[40]

C. Laws that require online services to treat adult and child users differently either explicitly or implicitly require the use of age verification or assurance technology, which undermines privacy and chills free expression rights for both young people and adult users.

Many child safety proposals require general audience online services to offer certain protections and safeguards to children and parents of children rather than all users. Examples of this include an online service being required to limit by default a minor's ability to communicate with a user they do not have any mutual connections with or to enable a parent to manage their child's account settings. These sorts of settings would be inappropriate to apply to adult users' accounts, as they would limit key functionality for adult users and put adults' privacy and safety at risk by giving another user the ability to control their communications.[41] Applying these sorts of restrictive settings only to the accounts of minors, and not all users, will require online service providers to distinguish adults from minors.

Such obligations thus either explicitly or implicitly require online service providers to use age assurance technology to determine which of their users are adults and which are children. An online service may employ many methods to estimate or verify a user's age. Age assurance is the umbrella term for a range of methods an online service can use to verify or estimate a users' age. Age declaration is the method most internet users are already aware of, where a user is asked to check a box that affirms they are over 18 or input their date of birth. This approach of age-gating is considered very easy to circumvent.

Online services have begun using a combination of age estimation methods that collect and analyze sensitive personal information and online behavior (like groups a user is a part of or their search history) to estimate a user's age. These methods may use facial scanning or voice recognition technology or other types of machine learning technology to analyze and compare a user's characteristics against features it believes to be a child's features. Approaches that use machine learning systems to predict the ages of all users may raise concerns of bias and error;[42]

[40] *Ibid*

[41] See: Research on instances where equipping an adult control over another adult's user settings could facilitate technology-facilitated abuse. Renee Fiolet, *et al., Exploring the Impact of Technology-Facilitated Abuse and Its Relationship with Domestic Violence: A Qualitative Study on Experts' Perceptions*, Global Qualitative Nursing Research (June 29, 2021).

[42] Zoe Hilton and Helen King, *Age assurance technologies and inclusion considerations*, Praesidio Safeguarding (March 2023)

these systems often perform less accurately when assessing the ages of people with disabilities, nonbinary faces, and non-white faces, specifically those with darker skin tones.[43]

Finally, some online services use (or are even required to use) age verification technology that requires account holders to provide hard identifiers like driver's licenses or other government credentials to verify their age with little uncertainty. These methods can present a host of problems. First, they will impose barriers to access information should a user not have these documents, for example undocumented immigrants or young people. Second, they require collection and processing of personal data that services might not otherwise collect. If high-assurance government-issued credentials became ubiquitous in order to provide for age verification, they could also be used for many more invasive purposes, including both commercial and governmental surveillance, unless strong privacy protections around collection and use of such identification were implemented simultaneously.[44] The privacy gains that have been made in restricting pervasive online tracking could easily be undermined by easier access to high-assurance permanent identifiers like mobile driver's licenses. Third, requiring users to provide identification information threatens their ability to access information and speak anonymously, which could have harmful chilling effects and raises significant First Amendment concerns.[45]

Some online services have also proposed conducting age and/or identity verification at the device, app-store, or ISP level to centralize data collection and processing and limit individual services' access to sensitive information.[46] This approach would work by limiting the collection of government credentials to a single, centralized intermediary to enable it to create an anonymized token indicating a user's age or age range.[47] A user could then grant access to that token to applications or online services without having to provide any further documentation or sensitive information. In this sense, a centralized approach would have some advantages from a privacy perspective since only one entity would obtain access to the personal information necessary to establish age. And it could permit users to access content anonymously. At the same time, this approach would mean the centralized intermediary would bear the burden of

[43] See: *Improvements in Facial Estimation* by Yoti (January 2023); *Gender Shades*, a study of facial scanning technology on faces of different skin tones.

[44] *Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom*, American Civil Liberties Union, (May 17, 2021)

[45] Shoshana Weissman, *Age-verification methods, in their current forms, threaten our First Amendment right to anonymity - R Street Institute* (June 1, 2023); Emma Llansó, *CDT and Rights Groups File Amicus Brief in Texas Online Age Verification Case - Center for Democracy and Technology* (September 28, 2023)

[46] Simone van der Hof, *Age assurance and age appropriate design: what is required? – Parenting for a Digital Future*, London School of Economics*,* (November 17, 2021)

[47] Scott Brennan and Matt Perault, *Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?* Utah State University's Center for Growth & Opportunity (June 21, 2023)

sensitive data collection, security, and liability, and it may provide the intermediary even more power in the online ecosystem (e.g., by refusing to provide token access to a particular service). Moreover, it may fail in situations where a device is used by multiple people, for example a family tablet used by both children and adults.

As a result of these and other issues, studies conducted on age verification technology by French and Australian regulators have concluded that age verification raises far too many privacy and security concerns to be mandated by law.[48] A federal study would go a long way in understanding the privacy and expression risks of age assurance technology and advancing norms around the use of data by age assurance methods.

D. Child safety approaches must account for the unique needs of schools and education agencies

As technology becomes increasingly ubiquitous in schools, online child safety inevitably must address students' use of technology in schools. As discussed above, student activity monitoring and content filtering in the name of child safety presents significant risk of harm, from restricting access to valuable information to discriminatory disciplinary and other practices. Schools and educational institutions and their vendors also have unique roles with respect to student data. For example, although the right of an individual to require deletion of their own personal data is now thought of as a basic right included in many privacy laws, the inclusion of schools and education vendors within the scope of those laws can have unintended consequences on the education sector. If a student or parent can require such deletion by third-party vendors who operate on behalf of educational institutions, that could lead to the deletion or amendment of critical information like grades and disciplinary records.

Likewise, child safety policies sometimes place restrictions on profiling users of a certain age. Schools might use data for things like personalizing student learning and other operational purposes, and prohibitions on profiling under most definitions without exclusions for schools and their vendors would render these systems ineffective, removing a tool that is aimed at improving education. For instance, consider a system that uses data about students such as their stated interests, grades from past assignments and other classes, and teacher observations to develop assignments tailored to address students' academic weak spots while catering to their interests, making it easier for them to approach their trickiest subjects. This analysis of

[48] *Age Verification Report | eSafety Commissioner*, Government of Australia (March 2023); *Online Age Verification: balancing privacy and the protection of minors |* Commission Nationale Informatique & Libertés, Government of France (September 22, 2022). Note: State governments in Utah for example are also grappling with the relatively unregulated space of age assurance service providers by drafting proposed rules for the use of age verification and assurance techniques as part of its recently passed Social Media Regulation Act.

student data could be considered profiling, and thus unallowable under certain child safety policies, limiting schools' ability to address their student's needs effectively.

II. NTIA should support and promote measures to protect children online that are evidence-based and do not lead to inadvertent and disparate impacts on users' right to privacy and access to information.

Although some proposals to advance online child health and safety can create more harm than benefits and undermine rights, others can promote this critical goal. NTIA should recommend and advance these alternative measures.

A. Support passage of comprehensive federal privacy legislation (Q. 16, 17)

The most effective way to protect children's privacy, and in many cases their safety, is to pass a comprehensive privacy law. Such a privacy law could move the U.S. beyond its failed notice-and-consent regime and toward a regime that holds companies, not individuals, accountable for their data practices.[49] The law could limit data collection, use, and transfer overall, including for children, and limit collection and use of particularly sensitive information like geolocation and contents of communications, all of which will reduce privacy- and safety-related harms.

For example, the American Data Privacy and Protection Act (ADPPA), which passed out of the House Energy & Commerce Committee last year with a bipartisan vote of 53-2, would significantly help with keeping minors safe online.[50] Its protections include data minimization, civil rights, algorithmic and AI transparency, and user rights to access, correct, delete, and port their data, among other provisions.[51] Importantly, the bill includes strict protections for children, including a ban on targeted advertising to anyone under 17 years of age, as well as a ban on transfers of children's data without parental consent.[52] It also created a new "Youth Privacy and Marketing Division" within a new privacy bureau at the Federal Trade Commission.[53] Passing these common-sense, bipartisan reforms would move the U.S. much closer to protecting children (and all individuals) online.

[49] Eric Null, *We Should Protect Children's Privacy Through a Comprehensive Federal Privacy and Civil Rights Bill - Center for Democracy and Technology*, (March 22, 2022)

[50] *Overview of the American Data Privacy and Protection Act, H.R. 8152*, Congressional Research Service, (August 31, 2022)

[51] Will Adler, *et al., CDT Comments to the National Telecommunications and Information Administration on AI Accountability*, Center for Democracy & Technology, June 12, 2023

[52] *The American Data Privacy and Protection Act*, Section 205(a)-(b)

[53] *The American Data Privacy and Protection Act*, Section 205(c)

B. Empower all users, including teens and children, with tools and design choices that allow them to shape a positive online environment in accordance with their needs (Q. 5a, 5b, 13, 14)

Equipping users with tools to control their own experience online can make the most significant direct impact on child safety online, particularly for teens. As the American Psychological Association concluded earlier this year, "[u]sing social media is not inherently beneficial or harmful to young people," and "[n]ot all findings apply equally to all youth."[54] As a result, "[a]dolescents' experiences online are affected by both 1) how they shape their own social media experiences (e.g., they choose whom to like and follow); and 2) both visible and unknown features built into social media platforms."[55] It follows from these findings that providing adolescents with tools that they can use to shape their own experiences to best meet their specific needs is a critical component of promoting youth online health and safety.

That focus on youth agency is consistent with a recent study conducted by CDT, in which researchers spoke with over thirty people aged 14-21 about the unwanted messages—defined as unwanted, unpleasant, or concerning messages that came from strangers— they received on direct messaging services and how they dealt with them.[56] Overwhelmingly, they told us, they relied on signals that companies offered like blurring of an inbound potentially sexual image or displaying whether or not a message sender had any mutual friends to gauge the potential intent or impact of an unwanted message. After assessing the unwanted message, teens used reporting or blocking tools to limit similar encounters, deleted messages when it was possible, and set their accounts on "private" mode if they had been previously set to "public" or findable by other users.

Equipping users with tools to navigate potentially harmful encounters or content can empower them to make their own decisions and serve as a more malleable and personalized approach to dynamic issues. Some of the participants we engaged thought that the risk of unwanted messages "was not a big deal," while others reported receiving frequent discriminatory, highly sexual, and otherwise offensive messages. Out of 72 incidents where a participant wrote about an unwanted message, they dealt with 30 incidents by ignoring them, while responding to 20 by reporting the sender. Some participants either deleted the message or expressed an interest in being able to delete unwanted messages when that option was not offered. This range of responses also spoke to another finding, specifically that the risk and frequency of unwanted messages was not equally spread across our participants. Over a three week period, some

[54] *Health advisory on social media use in adolescence*, American Psychological Association
[55] *Ibid*
[56] Luria, *More Tools, More Control*, (2023)

participants in our study received as many as two unwanted interactions per week, while others received only one message, or none at all, during that period.[57] African American boys and men received the highest share of unwanted messages.

NTIA should identify and promote the adoption of tools that all users, including children, can use to enable them to better address negative online experiences. Those could include, for example, the ability of users to easily delete and block unwanted interactions; better methods to report unwanted content, including feedback to users about what action a platform took in response to a report; greater friction or "speed bumps" in interactions with unknown profiles or potential strangers; and more "just-in-time" notices that inform and educate users about potential risks and steps they can take to mitigate them. In addition, users of different ages have expressed interest in accessing voluntary filters, settings, or features on online services that enable them to control the types of ads or content they see,[58] the use of their data to train automated systems, and who can reach out to them. These efforts may not be suitable to require by law, but may inform voluntary guidance or codes of best practices for companies serving mixed audiences. NTIA should explore how tooling can better empower users online in ways that don't undermine user privacy and expression and how to promote the development and use of such tools.

NTIA should also explore whether there is an evidentiary basis for other design choices that can protect users while still giving them agency and not restricting their ability to access content. Such measures could include steps such as restricting autoplay, prohibiting the use of dark patterns, and defaulting accounts upon creation to the most privacy-protective settings (while allowing users to change those settings to suit their preferences) .

C. Conduct more research into the benefits and harms of online services (Q. 19)

More research is needed to understand how social media affects young people over time. Some researchers have found a small negative correlation between well-being and social media use, but this finding is both inconsistent and insufficient to demonstrate a causal relationship.[59] Researchers have called for longitudinal studies that can investigate potential causal

[57] Luria, *More Tools, More Control*, (2023)

[58] See: Research conducting user-polling on sensitive ad categories that conclude with users expressing a desire to control what types of ads they do and do not see. Liza Gak, *et al., The Distressing Ads That Persist: Uncovering The Harms of Targeted Weight-Loss Ads Among Users with Histories of Disordered Eating*, Association for Computing Machinery, (November 2022); Yuxi Wu, *et al., Slow Violence of Surveillance Capitalism: How Online Behavioral Advertising Hurts People*, FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, (June 2023)

[59] Odgers and Michaeline R. Jenson, *Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review*, (January 17, 2020)

relationships between social media and mental health.[60] In the meantime, it is premature to conclude that social media leads to mental illness in adolescents. There is simply not enough evidence to support this claim.

Research should also investigate how different individuals and groups interact with social media. The American Psychological Association concluded that "relatively few studies have been conducted with marginalized populations of youth, including those from marginalized racial, ethnic, sexual, gender, socioeconomic backgrounds, those who are differently abled, and/or youth with chronic developmental or health conditions."[61] Benefits and harms of social media can vary depending on factors such as race, sexual orientation, socioeconomic status, and propensity for mental illness. For example, LGBTQ+ teenagers face heightened risk for online harassment, but they also derive benefits from engaging in online LGBTQ+ communities and the chance to explore their identities.[62] Teenagers of color also face a similar complex online environment, where they find strength in online communities based on their identities while simultaneously facing racial abuse.[63]

D. Invest in more education and digital literacy initiatives

Digital literacy initiatives can be well-suited alternatives to legislation as they can empower young people to access age-appropriate experiences on a range of online services.[64] Digital literacy programs are particularly important for newly connected students, as studies show that students with limited broadband access have lower digital skills.[65] Educators can play a frontline role in equipping children with tools they need for the future. In polls conducted in 2021, only 33 percent discussed data privacy with students as a requirement or part of the curriculum.[66] The FCC has previously played a role in lifting this number by providing resources to schools that receive E-Rate funding as part of its OnGuard Online program to develop digital literacy initiatives for students. Expanding similar programs aimed at educating minors about appropriate online behavior can help in equipping young people to navigate social media and messaging services, avoid and respond to instances of cyberbullying, and secure private information like passwords and personally-identifying information.

[60] Patti M. Valkenburg, *Social Media Use and Well-Being: What We Know and What We Need to Know*, Current Opinion in Psychology 45 (June 1, 2022)

[61] *Health advisory on social media use in adolescence*, American Psychological Association

[62] Linda Charmaraman, et al., *Marginalized and Understudied Populations Using Digital Media*, In Handbook of Adolescent Digital Media Use and Mental Health (2022).

[63] *Ibid*

[64] Cody Venzke and Hannah Quay-de-la-Vallee, *Closing the Homework Gap While Protecting Student Privacy*, Center for Democracy and Technology, (May 26, 2021)

[65] *Broadband and Student Performance Gaps,* Quello Center | Michigan State University, (2022)

[66] *Teacher and Parent Views on EdTech and Student Privacy*, Center for Democracy & Technology, (March 29, 2021)