To:
Faisal D'Souza
Office of Science and Technology Policy
NCO, 2415 Eisenhower Avenue
Alexandria, VA 22314

From:
Amina Fazlullah, Head of Tech Policy Advocacy
Ariel Fox Johnson, Senior Advisor, Data Privacy
Common Sense Media
699 8th St, Suite C150
San Francisco, CA 94103

Common Sense Media advocates to improve young people's experiences with technology. Common Sense Media is dedicated to helping kids and families thrive in a rapidly changing digital world. Since launching in 2003, Common Sense has helped millions of families and kids think critically and make smart choices about the media they create and consume, offering age-appropriate family media ratings and reviews that reach over 110 million users across the country, a digital citizenship curriculum for schools, and research reports that fuel discussions of how media and tech impact kids today. Common Sense also educates legislators across the country about children's unique vulnerabilities online.

In addition to the recommendations[1] below, we wanted to share the resources Common Sense Media has created in partnership with industry stakeholders to respond to the needs of educators, parents, and kids through our Common Sense AI Initiatives.

We write to share recommendations regarding high-priority policy actions for the National AI Action Plan. We believe a high priority of the Trump Administration's in this Action Plan should be making responsible policy on AI and children, addressing privacy,

[1] This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing the AI Action Plan and associated documents without attribution.

safety, and educational efficacy. Our recommendations below are based on ideas first presented in a policy memo published by the Federation of American Scientists at https://fas.org/publication/ensuring-child-safety-ai-era/.

To ensure the safe and effective use of AI serves to secure our nation's future global competitiveness, to that end we recommend the administration: build a coordinated framework for AI Safety; champion legislation to support youth privacy and online safety in AI; and ensure every child can benefit from the promise of AI. The federal government should develop clear prohibitions, enforce them, and serve as a national clearinghouse for AI K-12 educational policy. It should also support comprehensive digital literacy related to AI to ensure today's youth can effectively harness AI tools.

AI is transforming how children learn and live, and policymakers, industry, and educators owe it to the next generation to set in place a responsible policy that embraces this new technology while at the same time ensuring all children's well-being, privacy, and safety are respected.

In terms of building a coordinated framework for AI Safety, the administration should: ensure parity with existing child data protections; develop safety guidance for developers, including specific prohibitions to limit harmful designs and inappropriate uses; and direct the National Institute of Standards and Technology (NIST) to serve as the lead organizer for federal efforts on AI safety for children. When championing legislation to support youth privacy and online safety in AI, the administration should support the passage of online safety laws that address harmful design features that can lead to medically recognized mental health disorders and patterns of use indicating addiction-like behavior, and modernize federal children's privacy laws including updating Children's Online Privacy Protection Act and passing education privacy laws to explicitly address AI data use issues, including prohibiting developing commercial models from students' educational information, with strong enforcement mechanisms. And, in order to speed safe and effective use of AI for every child, the next administration should support comprehensive digital literacy efforts.

Importantly, policies and frameworks need to have teeth and need to take the burden off of individual states, school districts, or local stakeholders to assess AI tools for children. Enforcement should be tailored to specific laws but should include, as appropriate, private rights of action, and well-funded government enforcers. Companies should feel incentivized to act. The framework cannot be voluntary, enabling companies to pick and choose whether or not to follow recommendations. We've seen what happens when we do not put in place guardrails for tech, such as increased risk of child addiction, depression,

and self-harm–and it should not happen again. We cannot say that this is merely a nascent technology and that we can delay the development of protections. We already know AI will critically impact our lives. We've watched tech critically impact lives and AI-enabled tech is both faster and potentially more extreme.

Background

AI is already embedded in children's lives and education. According to Common Sense Media research, seven in ten teens have used generative AI, and the most common use is for help with homework. The research also found most parents are in the dark about their child's generative AI use–only a third of parents whose children reported using generative AI were aware of such use. Beyond generative AI, machine learning systems are embedded in just about every application kids use at school and at home. Further, most teens and parents say schools have either no AI policy or have not communicated one.

The U.S. has developed a risk management framework, but the U.S. has not yet articulated risk levels or developed a specific educational or youth profile using NIST's Risk Management Framework. There is still a deep need to ensure that AI systems likely to be used by children or in education, are assessed in terms of risk management and impact on youth.

It is well established that children and teenagers are vulnerable to manipulation by technology. Youths report struggling to set boundaries from technology, and according to a U.S. Surgeon General report, almost a third of teens say they are on social media almost constantly. Almost half of youth say social media has reduced their attention span and takes time away from other activities they care about. They are unequipped to assess sophisticated and targeted advertising, as most children cannot distinguish ads from content until they are at least eight years old, and most children do not realize ads can be customized. Additionally, social media design features lead, in addition to addiction, to teens suffering other mental or physical harm: from unattainable beauty filters to friend comparison to recommendation systems that promote harmful content, such as the algorithmic promotion of viral "challenges" that can lead to death. AI technology is particularly concerning given its novelness, the speed and autonomy at which the technology can operate, and the frequent opacity even to developers of AI systems about how inputs and outputs may be used or exposed.

Particularly problematic uses of AI in products used in education and/or by children so far include products that use emotion detection, biometric data, facial recognition (built from scraping online images that include children), AI companions, automated education decisions, and social scoring. This list will continue to grow as AI is further adopted.

Recommendations

There are numerous useful frameworks and toolkits from expert organizations like EdSafe, and TeachAI, and from government organizations like NIST, the National Telecommunications and Information Administration (NTIA), and the Department of Education (Dept of Ed). However, we need the next administration to (1) encourage Congress to pass clear rules regarding AI products used with children, (2) have NIST develop risk management frameworks specifically addressing the use of AI in education and by children more broadly, and serve as a clearinghouse function so individual actors and states do not bear that responsibility, and (3) ensure frameworks are required and prohibitions are enforced. This is also reflected in the lack of updated federal privacy and safety laws that protect children and teens.

The AI Action Plan should consider innovative policy ideas bubbling up at the state level. For example, there is legislation and proposals in Colorado, California, and Texas, and detailed guidance in over 20 states, including Ohio, Alabama, and Oregon.

Policymakers should take a multi-pronged approach to address AI for children and learning, recognizing they are higher risk and therefore additional layers of protection should apply:

Recommendation 1: Build a coordinated framework for an AI Safety and Kids Initiative at NIST

As the federal government further details the risk associated with AI use, common uses of AI by kids should be designated or managed as high risk. This is a foundational step to support the creation of guardrails or ensure protections for children as they use AI systems. The administration should clearly categorize education and use by children within a risk-level framework. If the risk framework includes education and AI systems that are likely to be used by children, it provides a strong signal to policymakers at the state and federal level that these are uses that require protections (audits, transparency, or enforcement) to prevent or address potential harm.

NIST, in partnership with others, should develop risk management profiles for platform developers building AI products for use in education and for products likely to be used by children. Emphasis should be on safety and efficacy before technology products come to market, with audits throughout development. NIST should:

- Periodically update the risk management framework (RMF) profiles, including benchmarking standards related to safety.
- Refine risk levels and RMFs relevant to education, working in partnership across federal and state government and through an open call to stakeholders.

Work in partnership with NTIA, FTC, CPSC, Dept of Ed, and HHS to refine risk levels and risk management profiles for AI systems likely to be used by children.

The administration should task NIST's Safety Institute to provide clarity on how safety should be considered for the use of AI in education and for AI systems likely to be used by children. This is accomplished through:

- Developer guidance: Promulgate safety guidance for developers of AI systems likely to be used by children or used in education
- Procurement guidance: In collaboration with the Dept of Education as needed, to provide guidance on safety, efficacy, and privacy to support educational procurement of AI systems
- Information clearinghouse: To support state bodies and other entities developing guidance on the use of AI systems by serving as a clearinghouse for information on the state of AI systems, developments in efficacy and safety, and to highlight through periodic reporting the concerns of and needs of users.

Recommendation 2: Safe and effective use of AI to ensure every child benefits from the promise of AI innovations

The administration should support comprehensive digital literacy and support expanded access to the necessary technology for effective use.

- Highlighting Meaningful Use: Provide periodically updated guidance on the best uses available for schools, teachers, students, and caregivers to support their use of AI technology for education.
- Support Professional Development: Dept of Ed and NSF can collaborate on Professional Development guidelines, flag new areas for teacher training, and administer funding to support educator professional development.
- Comprehensive Digital Literacy: NTIA and the he Dept of Ed should collaborate to administer funds for digital literacy efforts that support both students and caregivers. Digital literacy guidance should support both use and dynamically address concerns around current risks or safety issues as they arise. This can help ensure individuals can effectively and responsibly use AI tools in the future, which will be important for global competitiveness.

- Clearinghouse for AI Developments: In addition to funding this work, experts in government at NIST, NTIA, FTC, FCC, and Dept of Ed can work collaboratively to periodically alert and inform consumers, educators, digital literacy organizations, and other stakeholders about developments with AI systems. The federal government can serve as a resource to alert stakeholders downstream on both positive and negative developments, for example, the FCC Consumer Advisory Committee was tasked with developing recommendations with a consumer education outreach plan regarding AI-generated robocalls.
- Support access to technology: In 2021, Common Sense Media, in collaboration with Boston Consulting Group, identified that an estimated 16 million students were part of the persistent digital divide, lacking access to the home broadband connectivity and devices necessary to succeed in education. Further, our analysis estimated an annual loss of $33 billion to the GDP, if those students were left in the digital divide. To ensure rapid and meaningful use of AI technology by our nation's students, the administration should ensure there is support for affordable broadband and devices. The administration should direct the FCC and NTIA to ensure that any federal broadband service or device affordability support for students is capable of meeting the needs of students as they make greater use of AI for education.

Recommendation 3: Encourage Congress to pass clear, enforceable rules regarding privacy and safety for AI products used by children

Champion Congressional updates to privacy laws like COPPA and FERPA to address use (especially for training) and sharing of personal information (PI) by AI tools. These laws can work in tandem, see for example recent proposed COPPA updates that would address use of technology in educational settings by children.

- Consumer Protections: In the consumer space, consider requirements generally prohibiting use of children's PI for training AI models, unless deidentified or aggregated and with consent (see CA AB 1064).
- Education Protections: In education settings, it may be unclear when information about students shared with AI systems is subject to FERPA. In order to be most effective in protecting student privacy with AI systems, FERPA could be updated to explicitly cover personal information collected by and shared with LLMs: covered education records must include this data; sharing of directory information for all purposes including AI should be limited; the statute should address when ed tech vendors operate as "school officials" and generally prohibit training AI models on student personal information.

Push for Congress to pass AI-specific legislation addressing the development and deployment of AI systems for use by children

- Address High Risk Uses: Support legislation to prohibit the use of AI systems in high-risk educational contexts, or when likely to be used by children, unless committee-identified benchmarks are met. Use of AI in educational contexts and when used by children should, by default, be deemed high risk unless it can be demonstrated otherwise. Specific examples of high risks uses by children or in education include AI for threat detection and disciplinary uses, exam proctoring, automated grading and admissions, and companion AI use by minors.
- Require Third-Party Audits: Support legislation to require third-party audits at the application, model, and governance level, considering functionality, performance, robustness, security and privacy, safety, educational efficacy (as appropriate), accessibility, risks, and mitigation strategies.
- Require Transparency: Support legislation to require transparency if incident reporting by AI developers. This will enable parents, and education procurement officials, to make their own informed choices with regard to what is best for their children and students.

One final recommendation for the AI Action Plan is that standards and requirements need teeth. Frameworks should require that companies comply with legal requirements or face effective enforcement (such as by a well-funded expert regulator, or private lawsuits), with tools such as fines and injunctions.