

## Memo to the Presidential Transition Team Regarding Priorities for Helping Children Lead Healthy Digital Lives

November 2024

**Children and Screens: Institute of Digital Media and Child Development** is pleased to offer these recommendations to guide the first 100 days of the Trump-Vance administration.

Children live in a distinct ecosystem relative to previous generations. While they face some of the same risks, they are exposed to new or heightened threats and opportunities online. Addressing the specific challenges and leveraging the benefits of their evolving environment calls for innovative policy approaches and decisive action.

Digital technology offers immense opportunities, but also brings new and often unintended harms. Evidence shows that tech companies are frequently aware of the harms their products pose, yet many fail to implement necessary safeguards. Protections that exist in the offline world have not yet been translated to the online space, leaving children vulnerable in ways they were once protected. We failed to adequately protect children with the advent of the internet, during the rise of social media, and again as smart devices became commonplace. We must now act to both retroactively protect children and to proactively defend them from emerging digital threats.

Government regulations and policymakers have not kept pace with the rapid evolution of technology and digital media, and there remains a need for enduring, innovative policy solutions. Yet, as so much of our communication and expression has moved online, attempting to regulate tech companies can be fraught with risks to civil liberties and unintended consequences.

Despite this, these challenges are far from insurmountable.

## Recommendation 1: Advance strong online protections for kids

Health, privacy, and safety should be the default priorities of all technology and digital media platforms, especially those with child-facing features. This goal should be baked into the design, from the product's inception to the development of the user interface. Designs should empower users to make healthy choices, allowing for the realization of the opportunities technology can provide instead of its harms. There is already legislation in play that addresses this need. If left unaddressed when the 118th Congress adjourns sine die, the Trump-Vance administration should immediately work with legislators to pass reintroduced versions of the following bills during the 119th Congress.

### 1.1 Sign into law the [Kids Online Safety Act \(KOSA\)](#) and the [Children and Teens' Online Privacy Protection Act \(COPPA 2.0\)](#), or similar legislation.

KOSA and COPPA 2.0 are currently being considered by Congress. Should either bill fail to pass this year, the Trump-Vance administration should prioritize continued work on these vitally important measures.

### 1.2 Elevate and strengthen key components of KOSA and COPPA 2.0.

KOSA's platform design focus should be maintained and elevated. From a website's or online service's design stage, the technology should prioritize safety and respect users' rights.

The following design features must be addressed:

- Dark patterns (design features that subvert user autonomy, like making it hard to find the "decline" option for cookies) should be prohibited.
- Personalized recommendation systems, partially or fully automated based on personal user data, should be limited or prohibited for children.
- Users should have control over whether or not to use these systems. For children, some of these systems should not be available at all.
  - KOSA and New York's [S. 7694A](#), Stop Addictive Feeds Exploitation (SAFE) for Kids Act, provide examples of how to define personalized recommendation systems that include account recommendations, and approaches to restricting these systems for children.
  - Notifications and other nudge techniques should be limited or prohibited, particularly for children, and especially at night.

- Platform designs must prioritize children's privacy. Specifically, tracking, including persistent identifiers, account visibility, and the ability for strangers to contact children, should be severely limited, if not outright prohibited.

COPPA 2.0 provides strong privacy and data protections that must be enacted.

- COPPA 2.0 extends the [Children's Online Privacy Protection Act's](#) (COPPA) longstanding and effective protections to teenagers. Every American deserves privacy protections, but it is an absolute necessity for children and teens.
- COPPA 2.0 sets a high bar for permissible data collection from children. Only the minimal amount necessary to provide a service is permissible.
- When applying privacy and data protections, companies would be required to satisfy a "constructive knowledge standard" of age assurance, as opposed to the current, less rigorous "actual knowledge standard" to which they are held.

**There is overlap in some components of KOSA and COPPA 2.0. The most important of these should be preserved in any new online safety legislation.**

**These include:**

- Prohibiting targeted advertising to children.
- Require companies to provide ways for children to delete their information.
  - COPPA 2.0 specifies the child should be able to easily erase their data from a service, and KOSA specifies the child should be able to easily delete their account and accompanying data. COPPA 2.0's data deletion rights are preferable, however KOSA's account deletion requirement is a bar that should not be lowered.
- By nature, both KOSA and COPPA 2.0 will require some form of age assurance. Robust age assurance should be developed, yet should respect privacy and should not limit free speech. To ensure appropriate age assurance methods are available, research into optimal age assurance approaches could be conducted, as detailed in KOSA.

**KOSA and COPPA 2.0 are not end solutions on their own. We encourage the new administration to call on Congress to also address:**

- Artificial intelligence (AI) – any company deploying AI in a manner in which children are likely to interact with it must take the developmental and other needs of children into account. Children should not have access to AI that is not developmentally appropriate or that may subvert their developmental needs. Children should always consent to the use of, and interaction with, AI. AI must support, not replace, fundamental cognitive skills.
- Image and video filters should be limited. Some filters should not be accessible to children. Users should always be aware when filters are used.

- Profiling of children should be limited to only what is necessary for the operation of the service.
- Data ownership – children should have ownership over their data. This goes beyond requiring companies to delete it. It extends to every use of the child's data, including giving the child the ability to download it or transfer it to other platforms.

**User safety and privacy must be the default; provisions within KOSA and COPPA 2.0 apply these standards, and should remain a top priority in all online safety legislation.**

- All feature restrictions and privacy settings should be the strongest by default for children. Allowances for only the minimal necessary use of features or personal information to provide the service.
- Additional restrictions should be considered for any feature or design that is intended to maximize user engagement. This includes, but is not limited to, notifications and algorithmic personalization.
  - There must be clear, strong cybersecurity standards for children's data. These are noted in the [Children's Online Privacy Protection Rule](#), and reiterated again in COPPA 2.0. It is vital that cybersecurity standards be enforced.
- The level of control should be developmentally appropriate – older adolescents should have greater control over settings, whereas it may be more appropriate to limit feature and privacy controls for younger adolescents. Children below a certain age should require parental consent to change all of these settings.

### **1.3 Notification of features – users should be notified of their rights and the protective features described above.**

- If any of the listed features are used, children should be aware whenever they engage with them.
- Children should be aware of all privacy settings, how to change them, and what changing them means.
- Children should be notified at the point at which a feature or privacy setting is activated.
- Notifications must be age-appropriate and presented in an understandable way that takes into consideration literacy, native language, and disabilities. If children of a certain age are likely to use a platform, notifications must be presented at a level they will understand.

## 1.4 Tools – children and their parents should have reasonable, easily accessible tools to enact these rights and support healthy online experiences.

- KOSA and COPPA 2.0 both address these areas to some extent, but they should be much more expressly and broadly required.
- Tools that address known harms must be provided. These include, but are not limited to user control of content they engage with, and erasing personal data.
  - Tools must be meaningful. They must be effective, accurately represented by the platforms, and easy to access and use. Accessibility and utility should be evaluated with direct input from users.

## Recommendation 2: Require transparency and invest in public interest research

Many tech companies hide dangers associated with their products and services. Regulators need more accurate information to protect children and other consumers. Furthermore, informed policies require evidence. Funding should be increased for objective, scientific research. Validated data and research will require complex designs and following studies over time, which can be expensive and require structural support.

## 2.1 Transparency – companies must be compelled to be transparent. Transparency is required to build more effective legislation and to enforce any regulations.

Companies must divulge to regulators the information necessary to enforce regulations. This could include, but is not limited to:

- Advertising data
- Number and age of users
- The use of personalization algorithms
- Any uses of AI
- Content and account moderation practices
- Revenue - how much and where it comes from
- Data handling practices
- Derived user data

Companies must provide information that enables consumers to make informed decisions.

- Consumers require the same transparency provided to regulators. Insights about advertising and moderation are particularly important.
- This transparency is not only important for user agency, but also supports competitive markets.

Require Data Protection Impact Assessments (DPIA) for services likely to be accessed by children.

- This requirement is the core of many Age-Appropriate Design Codes (i.e. Kids Codes) in the United States.
- [Maryland \(H.B. 603\)](#), [California \(A.B. 2273\)](#), and [Vermont \(S. 289\)](#) all passed Kids Codes and offer examples of different DPIA requirements.
- Components of a DPIA that do not contain proprietary information should be publicly available.
- DPIAs can be a vehicle to communicate the transparency data needed by regulators and consumers.
- DPIAs should not require companies to speculate on the harms of their products. However, any evidence of product impacts should be included. The administration should consider compelling companies to perform safety testing on their products and include those findings.

## 2.2 Invest in and support public interest research – we need to better understand the impacts of technology and digital media. Effective legislation and regulation requires information and research.

Platforms should not interfere with research studies, and should be responsive when they are made aware that product updates and/or features inhibit data collection.

- If paired with regulations, investments in research will yield significantly greater benefits.
- The administration should refer to legislation such as [S. 1876](#), Platform Accountability and Transparency Act, for potential mechanisms and systems for research.
- Companies should be compelled to comply with approved research studies.
- Approved researchers should have access to the information given to regulators, even if that information is not publicly available.
- Safeguards must be in place to protect sensitive and proprietary information.
- Researchers should be protected from liability, except when they act with malice.

## 2.3 The Trump-Vance administration’s budget could help advance both of the above goals.

- Legislation is necessary to compel significantly greater transparency, but additional investment is also needed.
- Research lacks funding, and simply investing in it would promote our understanding of online platforms.
- The findings of publicly funded research promote transparency, even when platforms do not divulge their own data and practices.

**Researchers now understand the urgency for online safety regulations in spite of the limited funding to date. With more funding, we could refine research.**

- The Trump-Vance administration should prioritize funding and disseminating diverse research.
- There is still a need for comprehensive studies on the impacts of technology and digital media on youth mental health, cognition, and well-being.
- There is also a need to study the effects of technology in early childhood development, education technology, AI, diverse youth, and how technology can undermine cognitive development, among many other areas.
- Funding should prioritize robust research designs such as longitudinal studies, naturalistic studies, and randomized controlled trials.
- Developmentally appropriate guidance for parents, children, clinicians, educators, and industry should be promulgated from this research. Recommendations could include, but are not limited to:
  - Appropriate screen and device use
  - Healthy, safe, and appropriate use of AI
  - Support for device-free times and zones
  - Special attention to technology in education settings

**Resources and programs should be established to disseminate this guidance to key stakeholders. These should prioritize parental empowerment and support, helping families build digital literacy, and ameliorating the harms of technology and digital media.**

## Recommendation 3: Develop clear governance and enforcement systems

The problems caused by digital media are embedded structural issues and interact with the other environments children experience. Solutions to online safety should recognize that children's well-being hinges on more than social media, and the Trump-Vance administration's approach to governance should reflect this. Policies should empower enforcers to be responsive to technological trends and account for the individual and developmental needs of children.

### 3.1 Establish a Children's Council – the council should consider the entire ecosystem that affects children's well-being, including the digital world.

- The White House should appoint a Chief Technology Officer who will convene the Children's Council to advise them.
- The Council should promote, develop, and implement domestic child well-being policies that address the unique ecosystem children live in today.
- The Council will work with other councils (e.g., [Domestic Policy](#)) across federal agencies to drive holistic, intersectional approaches to child well-being.
- The Council must be bipartisan.
- The Council should engage with youth, caregivers, educators, researchers, clinicians, and industry.

### 3.2 The Federal Trade Commission (FTC) must be established as a fair, nonpartisan agency empowered to hold companies accountable, with the ability to adapt to the ever-evolving digital ecosystem.

- The United States must assume the lead in protecting children online. Considering the globalized nature of the internet, American youth will feel the impact of regulation in the United Kingdom and European Union, potentially leaving safeguarding the well-being of our children in the hands of foreign regulators and profit-motivated digital media companies.
- As we've seen with foreign and domestic regulatory attempts, regulatory approaches should avoid being overly prescriptive. Enforcers need room to react to evolving technology and adjust rules as scientific evidence is updated, but must be nonpartisan and trustworthy to do so.

### 3.3 Expanding enforcement efforts – this moment calls for swift, preemptive measures that protect against risks and anticipate future developments in emerging technologies. Agencies cannot effectively enforce new child online safety and privacy regulations without additional expert staff and dedicated resources.

Expand the FTC's children's privacy protection capacity:

- The FTC's enforcement staff for privacy violations is exceedingly small. For example, they currently do not even have the capacity to properly implement COPPA. The new administration should make expanding this enforcement a priority.
  - Expand enforcement outside of the FTC. The FTC has limited resources to enforce regulations against some of the largest companies in the world. Enforcement efforts should be distributed more broadly, for instance, to the Department of Justice.

- Establish dedicated expertise to review technologies for children’s use, enhancing accountability in child digital safety, health, and development. This need not be housed within the FTC.
- The administration should work closely with Congress to determine the best methods for protecting children online, consistent with the Constitution.

**These actions would reflect a strong commitment to supporting children and families in a balanced, safe, and empowering digital world. By addressing mental and cognitive health and development, privacy, and cybersecurity, these steps lay a foundation for both immediate and long-term improvements in how children and families navigate the digital landscape. This approach empowers children to benefit from technology while minimizing the risks of misuse and over-reliance on it. In addition, all policies should abide by the following key principles to ensure reasonable and lasting regulation:**

- 1. Center the well-being of youth.** Policies should protect young people’s rights to express themselves, seek information, and explore, without undue interference and influence from laws or private companies. By focusing on building fundamental safeguards and rights into how we regulate technology and digital media, we can ensure youth have safe spaces to thrive online, while maintaining their rights and those of all users.
- 2. Prioritize age and developmental stage.** Policies must take into account the age and developmental needs of children accessing a website or online service. Protections should be tailored to their cognitive and emotional abilities, ensuring that regulations appropriately safeguard users based on their age.
- 3. Adopt content-neutral regulations.** Rather than attempting to regulate legally protected content, which poses risks to constitutionally protected speech, policies should focus on platform design, data practices, privacy protections, transparency, and investing in public interest research. This approach will encourage corporate responsibility and ensure that websites and online services are safe and respect the rights of children.
- 4. Ensure policy endurance.** Technology is constantly evolving and the impacts vary across individuals and communities. Policies must accommodate new technology. While certain fundamental platform designs and practices should be regulated, there must be room to address new developments and changing needs.

## About Children and Screens

Children and Screens: Institute for Digital Media and Child Development is an independent, bipartisan, 501(c)3 organization working to help children lead healthy lives in a digital world. The Institute is committed to evidence-based, interdisciplinary, nonpartisan efforts, free from technology industry funding.

Rapidly changing media technology is outstripping our power to create a healthy environment for children, their development, and future—creating a host of detrimental effects on learning, physical and mental health, personal skills and relationships with others. Collaborating with a full range of diverse child advocates and experts, Children and Screens addresses technology and culture change to deliver evidence-based recommendations that equip families and policymakers with the confidence to act in the best interests of children and their development. Research, evidence-based recommendations, communications and policy advocacy — it’s how we create a world of good for children in the digital age.