SIIA CHILD AND TEEN PRIVACY AND SAFETY PRINCIPLES

Our kids deserve access to information and the virtual tools critical in keeping them connected and engrained in their communities without fear of being exploited. Policymakers have the opportunity to prioritize the privacy and safety of kids while empowering parents to be active participants in how their child operates online.

The following are the principles we believe should ground federal policy – including legislation – to keep kids safe and connected while holding platforms accountable for doing just that.

SAFE KIDS

Minimize the collection of personal data from children and teens and restrict the ways in which data is used.

- Covered platforms should only collect personal data from children and teens to the extent reasonably necessary to provide a service in which the child is actively and knowingly engaged.
- Covered platforms should retain personal data of children and teens only for the time that is necessary to fulfill the specified purpose.
- Covered platforms should not be prohibited from using data to provide access to high-quality content, if applicable to the service.
- Covered platforms should be prohibited from selling the personal data of children and teens to third parties without consent.
- Covered platforms should not be prohibited from using safety-enhancing and privacy protective algorithm-based features for minors.
- Covered platforms should not be prohibited from collecting information necessary to facilitate internal operations, including measuring site performance or for cybersecurity, or as required under other laws.

Data minimization, a widely recognized best practice for data processing, is one of the Fair Information Practice Principles [1] and is already required in many state privacy laws.[2] Data minimization is especially important for processing children's data because children are generally more trusting and less aware of the risks related to sharing personal information.

Provide easy-to-use and easy-to-access tools that empower children, teens, and families to customize safety protections and exercise rights over their own data. Offer simple, accessible easy-to-use and easy-to-access tools that empower children and teens to use privacy settings to consider and learn about privacy impacts.

---

[1] See Appendix A of the White House National Strategy for Trusted Identities in Cyberspace, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[2] These include theCalifornia Consumer Privacy Act, Connecticut Data Privacy Act (passed 2022), Colorado Privacy Act (passed 2021), and Virginia Consumer Data Protection Act (passed 2021).

Mandating that covered platforms provide these tools could be a meaningful way to help children and parents prevent and combat these harms.

Require platforms to be more transparent.
Privacy information provided to children, teens, and families, and any other published terms, policies, and community standards, must be concise, prominent, accessible, and use clear and plain language.

Transparency is a widely recognized best practice for data processing and is already required in many state privacy laws.[3] Transparency empowers parents and children to make informed decisions regarding online activities and privacy settings. When privacy information is provided to children in a clear manner that is developmentally appropriate, children are able to make more informed choices about their information and build trust with the platform.

Prohibit advertising based on online behaviors or activity of children and teens.
Covered platforms should be prohibited from creating and maintaining profiles about children for the purpose of targeting advertising to children based on their online behaviors, activities, or gender. Covered platforms should not be prohibited from contextual advertising or using a child's known age or location to show advertisements or prevent advertising from displaying on a child's device.

Children are less aware of business practices and may not understand how covered platforms create profiles for targeted advertising, making them especially susceptible to persuasive techniques.

Protect children's personal information with strong security safeguards that are appropriate to the level of sensitivity of the personal information collected, used, or shared.
Safeguards, which may be part of a company's larger security program, should incorporate protections against such risks as loss, or unauthorized access, destruction, use, modification, or disclosure of data. It should also include precautions against the deliberate abuse or misuse of information and facilitate the detection of any violation of the security system.

Security safeguards are a fundamental principle of privacy protection. A data breach involving children's data can have immense impacts on the futures of affected children, making them vulnerable to exploitation and abuse. Many state laws require covered platforms that handle consumer information to adhere to specific security standards.[4] Where adequate security laws may already exist, an additional child-specific security requirement is not required. Policies should ensure that security safeguards are proportional to the risk of exposure.

---

[3] California Consumer Privacy Act, Connecticut Data Privacy Act (passed 2022), Colorado Privacy Act (passed 2021), Virginia Consumer Data Protection Act (passed 2021), Iowa Consumer Data Protection Act (passed 2023), and Utah Consumer Privacy Act (passed 2022).
[4] Data security requirements exist in U.S. state consumer privacy laws, including the California Consumer Privacy Act, Connecticut Data Privacy Act (passed 2022) Colorado Privacy Act (passed 2021), and Virginia Consumer Data Protection Act (passed 2021).

CONNECTED KIDS

Ensure children and teens have equitable access to educational material on the internet and through other digital applications.
In a digital world, we cannot simply block children from accessing the vast resources available on digital platforms that can power a robust education. We must ensure that any new rules do not harm a child's access to high-quality educational technologies or educational information inside and outside of the classroom. Additionally, we must consider the impact proposals will have on all communities and ensure children and teens have the ability to access information.

Support resourcing to foster media and digital literacy in K-12 schools.
Any child privacy proposal must be accompanied by support for additional resources for America's K-12 schools to implement robust programs for media/digital literacy to prepare children and teens to be responsible digital citizens to ensure children and teens take a mindful approach to their online lives. Covered platforms should undertake efforts to advance K-12 digital literacy programs and support digital literacy efforts by governmental bodies at all levels.

ACCOUNTABLE PLATFORMS

Require risk-based impact assessments to address risks to children and teens.
Covered platforms must complete written risk-based impact assessments to evaluate a product's data practices with special attention to data of children and teens.

Risk-based impact assessments, already required by many legal regimes, will require companies to remain accountable for their practices. Any new requirements for risk-based impact assessments should align to existing requirements in other legal regimes.

Provide additional accountability by empowering enforcement.
Empower an appropriate government authority (e.g., the FTC or state attorneys general) to enforce legislation. Effective enforcement should not be watered down with inclusion of private rights of action leading to frivolous, excessive, and expensive lawsuits.

In order to ensure that covered platforms adhere to the requirements and protections described here, the language should include an enforcement mechanism. For example, enforcement under state Unfair and Deceptive Acts and Practices laws provides flexibility and adapts to existing state legislative processes but should take care to clarify that it does not provide a basis for a "backdoor" private right of action.

Advance consistent rules across the United States.
A federal law must be strong, preemptive, and provide the same protections to all children and teens across the United States.

The emerging patchwork of protections for children at the state level has the potential to create consumer confusion. A strong, preemptive law would ensure that all children were provided with equivalent protections and would foster better understanding of those protections among parents and families. It would also allow companies to operationalize consistent compliance programs.

ABOUT SIIA

SIIA is the principal trade association for the software and digital information industries. Our members include over 450 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services. SIIA is the only association representing both those who develop and deploy AI engines and those who create the information that feeds environments.

To learn more visit www.siia.net/policy/