Testimony before the Subcommittee on Commerce, Manufacturing, and Trade of the Committee on Energy and Commerce, U.S. House of Representatives

"Legislative Solutions to Protect Children and Teens Online"

December 2, 2025

Paul Lekas
Executive Vice President, Global Public Policy & Government Affairs
Software & Information Industry Association

I. Introduction

Thank you, Chairman Bilirakis, Ranking Member Schakowsky, and members of the Subcommittee, for the opportunity to appear before you today. My name is Paul Lekas, and I serve as Executive Vice President of Global Public Policy and Government Affairs for the Software & Information Industry Association (SIIA). SIIA shares the goals of this Subcommittee in making the internet a safer place for all. It is a privilege to join with you to urge Congress to pass bipartisan legislation to protect the privacy and safety of children and teens online.

SIIA represents nearly 400 organizations at the forefront of innovation in the United States around the world. For over forty years, we have advocated for the health of the information lifecycle, advancing favorable conditions for its creation, dissemination, and productive use. Our members range from start-up firms to some of the largest and most recognizable corporations in the world. They include the nation's leading publishers and innovative developers of digital products and services for K-20 education, global leaders in AI models and applications and in cloud computing, companies specializing in data analytics and information services, academic and scientific publishers, creators of legal research and financial databases, and the global financial information and market data community.

Whether in the workplace or the classroom, our members are dedicated to responsible data use. SIIA has made it a priority to work with industry to raise the bar on responsible practices. In addition to our *Child and Teen Privacy and Safety Principles*, discussed below, in the past two years we have collaborated with industry and policymakers to launch the *Principles for the Future of AI in Education*[1] and the *Data Stewardship Best Practices for Data and Analytics*

[1] SIIA, *Principles for the Future of AI in Education* (2023), available at https://edtechprinciples.com/wp-content/uploads/2023/11/Education-Technology-Industrys-Principles-for-the-Future-of-AI-in-Education-3.pdf; *see also* https://edtechprinciples.com/.

Companies.[2] These initiatives reflect industry's interest in promoting practices that advance the interests of those who rely on their services – students and educators, the financial markets and consumers – while taking care to protect individuals' privacy and data security and mitigate the risk of data and software misuse.

The pace of technological change surrounding the internet, and in particular the way that our kids and teens interact with that technology, has created new risks. The same technology that enables close contact with friends, for example, can exacerbate bullying. Thanks to the pressure from employees, families, children, advocates, and policymakers, companies are working to build guardrails and features into their products to address those risks and build a more robust and safe space for youth online.[3]

II. The Industry's Commitment: The SIIA Child and Teen Privacy and Safety Principles

In 2024, SIIA released our *Child and Teen Privacy and Safety Principles* calling on federal policymakers to pass legislation to keep kids safe and connected while holding technology companies accountable for doing just that.[4] Many of the themes in the principles are reflected in provisions of the bills under consideration today. Our principles seek to advance youth online privacy and safety through legislation that requires companies and other stakeholders to do the following:

Minimize collection and use of youth data. Companies must minimize the collection of personal data from children and teens and restrict the ways that data is used. Data minimization is widely recognized and required by many state privacy laws for processing data of children and teens. It is especially important for those populations because children and teens are generally more trusting and less aware of the risks related to sharing personal information.

Adopt tools that empower children, teens, and families. Companies should implement easy-to-use and easy-to-access tools that empower youth and families to maintain control of their data and mitigate potential online harms. Legislation can incentivize companies to provide these sorts of tools without engaging in content-based regulation.

Foster transparency. Families and youth should have access to clear information about how data is being used and the ability to control settings. The internet is a tool that families and youth can use to support learning and connection. Companies should provide information about privacy and safety provided to children, teens, and families in a manner that is concise, prominent, accessible, and use clear and plain language. Transparency is an essential mechanism to build trust and

---

[2] SIIA, *Data Stewardship Best Practices for Data and Analytics Companies* (2025), available at https://www.siia.net/wp-content/uploads/2025/06/Best-Practices-in-Data-Stewardship-for-Data-and-Analytics-Companies.pdf; *see also* https://www.siia.net/data-stewardship-best-practices/.

[3] This testimony uses the term "youth" to cover both children (under 13 years of age) and teens (under 18 years of age).

[4] SIIA, *Child and Teen Privacy and Safety Principles* (2024), available at https://www.siia.net/wp-content/uploads/2024/03/SIIA-Child-Privacy-and-Safety-Principles-.pdf.

demystify what can seem a complicated online landscape. Many state laws require transparency for online services. The goal is to ensure parents and youth can make informed decisions about their activities online.

Restrict advertising. Companies should not advertise to youth based on their online behavior or activity and should not create profiles of youth for the purpose of targeted advertising. Companies should be permitted to serve contextual ads; this is important to ensure that children are being served age-appropriate and location-appropriate content.

Protect personal information. Protecting user data, especially the data of children and teens, is a central tenet of the principles. Companies should implement strong security safeguards appropriate to the level of personal information that may be collected, used, or shared.

Enable access to educational material. The internet is a part of children's lives. News, educational materials, information about sports and hobbies as well as other entertainment can be online. Youth should be afforded access to information online without the threat that companies will over-moderate and prevent access to useful, legal content.

Support K-12 media and digital literacy. Legislation and new policies must be accompanied by support for resources in K-12 schools to implement programs for media and digital literacy. Children and teens are growing up in a digital world, and it is critical that we prepare them to be responsible digital citizens. Platforms should also support those digital literacy efforts.

Require risk assessments. Written risk-based impact assessments keep companies accountable for their practices. Several existing legal regimes already require these assessments, and a federal requirement should align with existing regimes and encourage adoption of best practices in risk-based evaluation and assessment preparation.

Empower enforcement. Effective enforcement requires clarity about which government agencies at the federal or state level have enforcement authority and should be designed to improve privacy and safety practices. Enforcement should not be watered down with private rights of action that can lead to frivolous, excessive lawsuits based on mere statutory violations. For example, enforcement under Unfair and Deceptive Acts and Practices laws provide clear paths for enforcement action without providing private rights of action that create cottage industries of litigation.

Provide consistent rules across the U.S. Federal law should be strong, preemptive, and provide the same protections to all children and teens across the U.S. The emerging patchwork regulations create confusion among both platforms and consumers. They also create gaps, because the internet is not cleanly partitioned along state lines. A national framework would allow companies to put consistent programs in place.

III. Specific Legislative Issues

SIIA appreciates the thoughtful approach that the Subcommittee has taken for today's hearing, recognizing that there is no single solution to the concerns that have been raised involving youth privacy and safety. Our goal is to ensure kids remain safe online and retain access to information and the virtual tools critical in keeping them connected in their communities. Families must also be empowered to decide what is best for their own family online and to teach kids and teens best practices for protecting themselves while navigating the internet. And companies should be encouraged to be proactive in addressing challenges faced on their platforms, apps, or websites in a manner that recognizes the need for context-specific solutions and the varying risk profiles that each corner of the internet presents.

In short, we support efforts to pass laws that improve youth privacy and safety. Many provisions in today's legislative package achieve that. As the Subcommittee considers these bills in greater detail, we urge members to take care to avoid unintended consequences and to advance legislation that meaningfully addresses the challenge at hand.

We are providing preliminary input to key issues raised by the legislation under consideration in this hearing. As the Subcommittee refines these bills, we look forward to continuing to work with all members.

First Amendment and Free Expression

SIIA recognizes youth safety as one of the most important of government interests. At the same time, there are other values that must be balanced against the desire to protect kids online: most notably those involving free speech. The First Amendment requires that Congress calibrate its desire to legislate comprehensive youth online safety measures against the need to foster protected speech.

That is a difficult, but not impossible balance. Most online safety laws are inherently content-based regulations—they require private businesses to make decisions about speech based on its subject matter (e.g., whether it is "harmful" or "detrimental" to minors), thus triggering strict scrutiny from the courts. While the government's interest in protecting children is compelling, courts have historically struck down federal efforts, like the Child Online Protection Act (COPA), because they were overbroad, restricting a substantial amount of constitutionally protected adult speech to shield minors.[5] This scrutiny forces Congress toward less restrictive means, such as regulating design or privacy conduct, rather than content.

This already challenging landscape has been both clarified and complicated by recent judicial decisions. The Supreme Court's 2025 decision in *Free Speech Coalition v. Paxton*[6] provides a

[5] *See Ashcroft v. Am. Civil Liberties Union*, 542 U.S. 656 (2004) (holding COPA unconstitutional); *Reno v. Am. Civil Liberties Union*, 521 U.S. 844 (1997) (holding portions of the Communications Decency Act unconstitutional).

[6] *Free Speech Coalition, Inc. v. Paxton,* 606 U.S. ___ (2025), available at https://www.supremecourt.gov/opinions/24pdf/23-1122_3e04.pdf.

narrow pathway for federal regulation by upholding Texas's age-verification requirement for commercial sites hosting unprotected, sexually explicit material, essentially confirming that regulation targeting content *unprotected as to minors* may withstand intermediate scrutiny. However, the logic of this decision is unlikely to extend to general-purpose social media platforms containing vast amounts of protected, non-sexual speech.

Conversely, the Ninth Circuit's 2024 decision in *NetChoice v. Bonta*[7] (regarding the California AADC) is a major constraint on federal legislation aimed at platform design. The court found that requiring platforms to assess and mitigate the risk of "harm" to children transforms a design regulation into a content regulation, subject to strict scrutiny and thus likely unconstitutional. It found that California had less restrictive means to achieve its goals – for example, incentivizing companies to offer content filters, educating children and families, and enforcing existing criminal laws. The Ninth Circuit also highlighted concerns raised by the ACLU that vague and expansive language would likely prevent youth from accessing content such as mental health resources, information about school shootings, and content reflective of minors' own religious or political speech.

A divided three-judge panel of the Eleventh Circuit recently issued an opinion that *may* provide additional guidance to lawmakers but is still the subject of active litigation.[8] In a 2-1 decision, the panel stayed a preliminary injunction that prevented Florida from enforcing a law that would prohibit users under the age of 14 maintaining or creating accounts on social media platforms and permit users aged 14 or 15 to maintain accounts only with parental consent. The majority held that by targeting platforms with "addictive features," the law was content neutral and subject to intermediate scrutiny.

In a vigorous dissent, Judge Rosenbaum argued that the Florida law "is not just 'likely' unconstitutional; it's plainly unconstitutional on its face." He described how the law "directly regulates both expressive activity itself and conduct with an expressive element," and noted–with some force–that the prohibitions not only impermissibly allow the state to control the ideas that minors can access but prohibit parents from exposing them to those ideas. In that circumstance, he found the burden on the speech rights of both minors and adults to far outweigh the government's interest under either strict or intermediate scrutiny. We think the dissent has the better of this argument, as this case remains a minority position and would caution the Subcommittee against putting too much weight on it. That said, if the panel majority's position holds, it will support the view that legislation addressing content-neutral design features rather than content itself stands on stronger constitutional footing.[9]

These decisions provide important guidance to Congress as it develops legislation to address a range of issues involving youth online privacy and safety. Legislation such as the Senate version of the Kids Online Safety Act (KOSA), which would impose a vague, expansive "duty of care"

---

[7] *NetChoice, LLC v. Bonta*, No. 23-2969 (9th Cir. Aug 16, 2024), available at https://netchoice.org/wp-content/uploads/2024/08/Ninth-Circuit-Ruling_NetChoice-v.-Bonta.pdf.

[8] *Comp. & Comm. Indus. Assoc. v. Uthmeier*, No. 25-11881 (11th Cir. Nov. 25, 2025).

[9] SIIA filed an amicus brief with the Ninth Circuit supporting the appellee in this matter.

that requires platforms to filter content based on subjective harm, would be likely to run afoul of the First Amendment.

We are encouraged that several bills the Subcommittee is considering have taken to heart the fundamental tension between free expression and the interests of youth online privacy and safety. We encourage the Subcommittee to see the evolving case law in this area not as an impediment but as a roadmap to identify legislative solutions that address legitimate concerns about online safety and privacy while also adhering to core American values. Legislation should avoid broad measures that amount to content filtering while focusing on ways to regulate non-expressive conduct, narrowly target explicit sexual content, incentivize companies to address gaps in their privacy and safety protocol, and leverage non-technical tools such as consumer education and criminal laws.

Modernizing COPPA

The Children's Online Privacy Protection Act of 1998 (COPPA) has served as a critical baseline for protecting the personal information of children, defined in COPPA as people under the age of 13. Most important is COPPA's requirement that operators obtain verifiable parental consent prior to collecting information from a child unless the information is used for internal operations. The FTC administers COPPA and earlier this year issued long-awaited amendments to regulations.

The new FTC regulations,[10] approved by the Commission on a bipartisan basis, represent the latest iteration of an ongoing effort to modernize COPPA. Among other things, the new regulations recognize the need to make verifiable parental consent reflective of modern technologies. Whereas a signed consent form sent in via fax was appropriate two decades ago, the FTC approved newer methods like a knowledge-based authentication process or the use of facial recognition technologies. The FTC has also updated the definition of personal information to include biometric identifiers and government-issued identifiers, reflecting the variety of information on children that could be collected online.

In recent years, the FTC has focused on COPPA enforcement. This year alone, the FTC has settled a number of matters involving alleged COPPA violations based on enabling a third party in China to collect geolocation information about American children without parental consent,[11]

[10] 16 CFR Part 312, available at https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312.

[11] FTC, Online docket for *United States v. Apitor Tech. Co., Ltd.* (Oct. 1, 2025), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/apitor.

unlawfully collecting information from children,[12] and deceiving children about the real costs of in-game transactions.[13]

We believe there are further updates that can be made to bring COPPA into the 21st century, including codifying recent updates into statute. Such updates include aligning to the regulatory requirements and industry best practices of data minimization and ensuring that platforms only gather data essential to preserving child safety. Under the current law, companies may engage in targeted advertising, among other things, with parental consent. As reflected in the SIIA Principles, we believe targeted advertising – as opposed to contextual advertising – should not be allowed for youth.

Perhaps most important, given our longstanding work with the educational community, we believe COPPA needs to be updated to reflect a conflict with the Family Educational Rights and Privacy Act (FERPA). There has long been a lack of clear line between FERPA and COPPA despite overlapping requirements. When a school contracts with an operator, the operator should not be able to use student information for any purpose other than for the educational purpose for which it was disclosed. This educational purpose limitation is required by FERPA but not COPPA. Clarifying this by statute would strictly limit operators' use of personal information. The updates in COPPA 2.0 clarify that educational data may only be used for educational purposes when technology is used at the direction of the school.

Age Assurance Methods

Age assurance covers a variety of methods used to determine a user's age or age range online, encompassing age verification, age estimation, and age declaration. Across the spectrum there are additional approaches that can be adopted – for example, requiring parental consent, estimating age with facial recognition technology or machine-learning models, or using government-issued identification. The choice of method depends on the required level of confidence, privacy concerns, cybersecurity risk, the risk associated with the content or service, technological availability, and other factors such as access and accessibility. Each method inevitably involves tradeoffs of important policy goals.

A principal challenge associated with more precise age assurance methods, such as age verification, is that they require gathering data from *all* users – not just those who fall within an age range or below an age threshold.[14] That collection creates outsized security risks and works

[12] FTC, Online docket for *United States v. Iconic Hearts Holdings, Inc.* (Sept. 29, 2025), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/232-3029-iconic-hearts-holdings-inc-us-v; FTC, Online docket for *United States v. Disney Worldwide Servcs., Inc.* (Sept. 2, 2025), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/disney.

[13]FTC, Online docket for *United States v. Cognosphere, LLC* (Jan. 17, 2025), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/222-3152-cognosphere-llc-us-v.

[14] A recent study by the Center for Democracy and Technology (CDT) found that while "[t]he majority of participants were not against the concept of online age verification…when discussed in more detail and in practical terms, most conversations pertaining to the widespread implementation of age verification raised concerns - including concerns about privacy, security of collected and stored data, their limited trust in

against privacy best practices around data minimization. Age verification requires robust data collection, making it exceedingly difficult to minimize the sensitive data collected from youth users. Websites or platforms holding a rich array of sensitive data are more attractive targets for malicious actors, dramatically increasing the likelihood that a data breach will harm young people. Requiring technology companies to gather and store that information creates the opportunity for bad actors to attack and access that information. This vulnerability is more pronounced for small- and medium-sized companies that may have less robust tools and resources than larger firms.

The most significant privacy and cybersecurity risk associated with robust age verification methods—particularly those requiring the submission of government-issued identification or biometric scans—is the potential for mass data breaches and the creation of centralized identity dossiers. When platforms or their third-party vendors collect and store highly sensitive PII to prove age, this data becomes a high-value target for cybercriminals, raising the risk of identity theft, phishing, and blackmail for all users who comply. Recently, for example, a breach of a third-party service provider used by Discord to perform age verification led to the exposure of 70,000 government-issued IDs.[15]

Furthermore, as discussed by the dissent in the *Uthmeier* case, mandating verification systems fundamentally undermines anonymity and can lead to surveillance creep, as the act of linking a verified identity to online activity transforms the internet experience into a less private space, potentially chilling the protected speech of both adults and minors who value their right to anonymous expression.[16]

Several other age assurance technologies exist that significantly minimize these privacy and cybersecurity risks. For example, age estimation, which uses machine learning to predict a user's age range based on non-identifiable facial characteristics or aggregated behavioral data, is a far less invasive method. While less certain than verification and prone to bias (especially for certain demographics), it could be suitable for low-risk contexts and for triggering a higher level of

---

platforms, and the lack of user agency - all of which left participants uneasy." Michal Luria and Aliya Bhatia, "What Parents Want: Policy Insights for Social Media Safety Features," CDT (Nov. 2025), at 11, available at https://cdt.org/wp-content/uploads/2025/11/2025-11-24-CDT-Research-Social-Media-Report-final-1.pdf.

[15] Discord, "Update on a Security Incident Involving Third-Party Customer Service" (Oct. 9, 2025), available at https://discord.com/press-releases/update-on-security-incident-involving-third-party-customer-service.

[16] *See, e.g.*, Alice Marwick, et al., *Child Online Safety Legislation: A Primer*, Princeton Center for Information Technology Policy, Duke Sanford School of Public Policy, UNC Center for Information Technology, and Public Life (2024), available at https://assets.pubpub.org/bujb2qf1/COSL-06.04-11717506843758.pdf; Shoshanna Weissman, "Current age-verification methods threaten our First Amendment rights beyond anonymity," R Street Institute (June 22, 2023), available at https://www.rstreet.org/commentary/current-age-verification-methods-threaten-our-first-amendment-rights-beyond-anonymity/; Sara Forland, et al., "Age Verification: The Complicated Effort to Protect Youth Online, New America Open Technology Institute" (Apr. 23, 2024), available at https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/.

scrutiny only when a user's age is uncertain. At the same time, it does not create the same privacy risks as using hard identity documents.

Following the Supreme Court's opinion in *Paxton*, age verification requirements are appropriate for websites with a significant amount of sexually explicit material. Half the states have laws that require verification to access sites with one-third sexually explicit material. Outside of that context, however, legislation that requires age verification is likely to raise First Amendment challenges on behalf of adult users who believe such requirements limit their ability to access legal content. Congress would need to establish that the age assurance method required serves a compelling government interest and is the least restrictive means of advancing that interest.

Congress should look to different methods to incentivize the creation of more age-appropriate experiences and protect young people online. Creating tools that empower parents and youth with control over their data and their online experience, using signals to estimate ages and trigger additional guardrails based on company policies, and creating parental monitoring tools can help to limit young people's exposure to harmful content and interactions.[17]

Parental Controls

Parental controls are an essential part of youth online safety and privacy. We believe it is important to empower families as well as youth to manage their online safety and privacy. Every family is different, as are families' views on what content and experiences are appropriate for youth in the online world.

While we support strong privacy standards and giving families tools to exercise appropriate oversight over their children, there are inevitable challenges. One challenge is age-old: children and teens are smart and resourceful, and the ability to implement controls requires being aware of how they can circumvent these controls. This is a challenge that is hard to address through legislation as opposed to education and improving communication within a family.

Making tools for controlling security and safety features easier for parents to access, understand, and use, as well as fostering digital literacy among parents and youth is also important. Creating effective tools and enabling by default is a good start, and ensures that the environment is set up as best it can be from the start, but we also want parents to be able to exercise their own agency based on their own judgment about what's best for their children, and making sure they understand and can use the tools is essential to that work.

[17] *See, e.g.,* Shane Tews, "Age Verification Laws vs. Parental Controls: Why the Legislatures, Courts, and Tech Aren't on the Same Page," American Enterprise Inst. (Feb. 5, 2025), available at https://www.aei.org/technology-and-innovation/age-verification-laws-vs-parental-controls-why-the-legislatures-courts-and-tech-arent-on-the-same-page/; Amanda Reid, et al., "Nerd Harder: A Typology of Techno-Legal Solutionist Logics in Child Online Safety Laws," *Policy & Internet* (Sept. 2025), available at https://onlinelibrary.wiley.com/doi/epdf/10.1002/poi3.70012.

Legislation can set and enforce standards, both for the tools themselves and for the information made available by platforms to parents. It can also leverage social resources to ensure that parents are provided with information in their communities.

Emerging Trends and AI Chatbots

As lawmakers consider risks associated with emerging technologies such as AI chatbots, we recommend a focus on clear, evidence-based, and risk-proportionate requirements rather than broad restrictions that could unintentionally limit access to beneficial technologies including educational tools, accessibility features, or other creative learning and age-appropriate content.

Building on the SIIA's existing principles on children and teen privacy and safety, we have been working closely with our members to develop a comprehensive set of AI chatbot principles, the *SIIA CHAT SAFE Principles*, that simultaneously encourages the development of emerging AI tools while protecting the privacy, safety and security of all Americans. These principles outline guidance for clear disclosures, harm mitigation, accountability, trust and reliability, security and privacy, and adaptability.

Extensive legal frameworks exist in regulated spaces. Developers building tools for use in these spaces and deployers implementing tools in these spaces should ensure that tools align with the goals of CHAT SAFE as well as other privacy, safety, security, and civil rights requirements.

As Congress considers legislation in this space, we encourage policymakers to align with this balanced framework that supports innovation and encourages meaningful protections for children and teens.

Third Party Data Collection and Use

The use of data by third parties has also raised attention. As the Subcommittee considers potential restrictions on third-party data collection and use, we would urge members to consider the possibility for unintended consequences. Data providers come in many stripes and in addition to those data brokers who may engage in practices that undermine youth privacy and safety, many providers engage in responsible practices that both maintain data security and further the interests of youth and are in fact essential to their wellbeing.

SIIA has adopted principles for responsible data use earlier this year: *Data Stewardship Best Practices for Data and Analytics Companies*.[18] Currently, some SIIA members enable the limited, but mission-critical use of minors' data by a range of institutions – colleges and universities, insurance companies, financial institutions, government agencies, foundations, and non-governmental organizations (NGOs) – that rely on that data to provide services that minors and their families rely on. Those include:

[18] SIIA, *Data Stewardship Best Practices for Data and Analytics Companies* (2025), available at https://www.siia.net/wp-content/uploads/2025/06/Best-Practices-in-Data-Stewardship-for-Data-and-Analytics-Companies.pdf; *see also* https://www.siia.net/data-stewardship-best-practices/.

- Extending auto insurance for teen drivers;
- Building minors' credit history;
- Targeting colleges' recruitment efforts to underserved student communities;
- Protecting minors against identity theft and fraud;
- Identifying candidates for scholarships
- Providing financial aid for college;
- Assisting in military recruitment;
- Suppressing the data of minors who are children of judges and law enforcement officials protected by *Daniel's Law*-style legislation;
- Maintaining data and whitelists to enable age verification where required; and
- Tracking exploitation of minors in connection with human trafficking efforts by NGOs and financial institutions.

We do not believe that it is the intent of the Subcommittee to disrupt these kinds of everyday activities. This list demonstrates, however, that too broad of a legislative brush will prevent valuable uses of this data that many people rely on and take for granted. Successful legislation in this sphere will both target "black hat" data brokers and preserve the essential uses that society relies on. We encourage the Subcommittee to use the best practices we developed as a tool to guide policymaking: raising the bar for industry by identifying the characteristics of responsible data providers, and enabling the pro-social data uses described above.

IV. Conclusion

Building a safer, healthier, and more useful internet for youth and families requires everybody's input and all of us to work together. Our members have taken important steps to provide better resources and tools for parents and improve protections for youth safety and privacy. We support legislation that will help to make the internet safer while avoiding unintended consequences by erecting barriers that expose sensitive data, restricting access to content that ignores children's curiosity and ability to work around safeguards, and encouraging youth to seek out darker, harder-to-regulate spaces.

We hear those who have concerns about the impact of technology on today's youth. But we believe the approach must be holistic. Child abuse, CSAM, bullying, and eating disorders existed long before social media. These are old problems with complicated causes. We believe there is a role for government to play and there is more that industry can be doing. There is also a need to focus on non-technical solutions. Education, community building, and support for families are part of that equation. Our kids should be safe. They should be safe in schools and at home. They should be safe in youth sports and in their houses of worship. And they should be safe on the

internet. Developing these environments requires all of us to work together on solutions that acknowledge the constant changes in these problems. There are no silver bullets.

The SIIA *Child and Teen Privacy and Safety Principles* demonstrate industry's readiness to act, and eagerness for Congress to pass legislation designed to advance these goals. We stand ready to work with the Subcommittee to turn these principles into law and provide our best counsel as the Subcommittee considers the legislation assembled today.