April 16, 2024

The Honorable Cathy McMorris Rodgers
Chair, House Energy and Commerce Committee
United States House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone, Jr.
Ranking Member, House Energy and Commerce Committee
United States House of Representatives
2322A Rayburn House Office Building
Washington, D.C. 20515

Re: Innovation, Data and Commerce Subcommittee Hearing on "Legislative Solutions to Protect Kids Online and Ensure Americans Data Privacy Rights"

Dear Chair McMorris Rodgers and Ranking Member Pallone,

We write today to add our voice to the chorus that are expressing views on the proposed legislation being heard tomorrow. Our members appreciate the efforts to continue to find consensus to pass preemptive consumer privacy legislation. We wanted to take the opportunity to provide our feedback on three of the bills under consideration during this hearing: **American Privacy Rights Act of 2024 (APRA), Children's Online Privacy Protection Act (COPPA 2.0) and Kids Online Safety Act (KOSA).** We remain hopeful that Congress will work together to move comprehensive legislation across the finish line.

SIIA is the principal trade association for those in the business of information. Our nearly 400 member 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. On behalf of our members, we view it as our mission to ensure a healthy information ecosystem: one that fosters its creation, dissemination and productive use.

Privacy is essential to the health of that ecosystem. Our members believe that a comprehensive privacy law is critical to address concerns about the lack of accountability and transparency with how consumer data is collected, processed,

and used. We released a set of principles[1] earlier this year that reflect major areas that need the attention of Congress to effectively protect the privacy and safety of children and teens online. We are gratified to see that many of these principles are reflected in the proposals and applaud the sponsors and cosponsors for their leadership.

American Privacy Rights Act of 2024

We view this as a thoughtful draft and a positive step towards comprehensive federal privacy legislation, as we are pleased to see various improvements to the 2022 bill.

Exemption of Publicly Available Information – For our members, it is imperative that the legislation respect the bounds of the First Amendment. To that end, the bill exempts publicly available information (PAI), as well as inferences derived solely from PAI. The draft clarifies that inferences that reveal sensitive covered data remain protected under the First Amendment unless combined with sensitive data itself. We were also pleased that the new draft avoids removing PAI's public designation when temporarily combined with covered data.

Embraces Privacy-enhancing Technologies – APRA directs the Federal Trade Commission (FTC) to carry out a pilot program to encourage private sector use of privacy-enhancing technologies (PETs) for the purpose of protecting covered data. SIIA has long advocated in favor of PETs, which have the potential to reduce or eliminate privacy risks for consumers while simultaneously enabling the productive use of valuable data sets.

Strong Preemption – We applaud improvements to preemption that works to avoid a confusing and expensive patchwork of state privacy laws and eliminates the carve outs reserved for states that happened to pass privacy laws pre-introduction. ***We believe that the preemption provision can be further refined so that states may not use common law or existing statutory law to evade Congress's stated intent. That evasion is of particular concern because of the private right of action provision.***

The following outlines areas of concerns with APRA as currently drafted.

Expanded Definition of Sensitive Data – Rather than addressing the risks of data dissemination according to its uses, the bill expands the definition of sensitive data to include new inflexible categories that are overinclusive of data that may pose little risk, but also under include high-risk uses of data that the definition does not cover.

[1] https://www.siia.net/wp-content/uploads/2024/03/SIIA-Child-Privacy-and-Safety-Principles-.pdf

In our view, the term "sensitive data" should be limited to that information which, by its nature, is intrinsically subject to abuse or the release of which would be offensive to a reasonable person.

- For example, the APRA defines "sensitive data" to include "information *about* a minor under the age of 17." There are two implications of this that we find concerning. First, it places the bill at odds with laws at the federal level and in the states designed to protect children's privacy, wrapping children's data into the "sensitive data" regulatory framework. Second, the word "about" would render this provision seriously overbroad (e.g., a picture of a child).

Application of Data Minimization – The bill imposes a presumption of illegality around a significant amount of productive commercial publishing activity, with little corresponding privacy benefits for consumers. It is also unclear whether the data minimization standards apply even in cases of affirmative opt-in consent, which is required around, for example, "sensitive data."

Private Right of Action – We oppose the inclusion of a private right of action. With that said, we appreciate the efforts made to narrow it and reduce the risk of "sue and settle" lawsuits that have become all too common.

Broad AI Provisions – The definition of "covered algorithms" addresses artificial intelligence tools, defined as a computational process that makes a decision or *facilitates* human decision-making by using covered data. The term "facilitates" dramatically broadens the scope of covered algorithms to include even those that pose minimal risk – rather than only those that pose a risk of consequential harm – and exist well outside the realm of AI as commonly understood. The APRA also applies its AI provisions to "entities," not "covered entities," confusingly expanding the scope of its AI requirements beyond those entities covered by the privacy provisions in the bill.

COPPA 2.0

This legislation is an encouraging step on protecting the privacy and safety of children and teens online while ensuring they are able to connect, learn, and access information online.

We are pleased that COPPA 2.0 includes language that clarifies how COPPA works in public schools. The lack of clarity on how to protect student data subject to protections under both the Family Educational Rights and Privacy Act (FERPA) and COPPA has been unclear since the passage of COPPA over two decades ago. The proposed changes in this legislation will ensure student data is protected without

creating conflicting legal obligations for schools and vendors or rights for students and parents.

The text of COPPA 2.0 also codifies internal operations language that was included in the 2013 rulemaking and has been incorporated into many business practices over the past decade. We are pleased this will allow businesses some predictability in their compliance work going forward.

The legislation also includes language that establishes data minimization rules to prohibit the excessive collection of children and teens' data. This aligns with the Child and Teen Privacy and Safety Principles that SIIA released in late March.

The following outlines areas of concerns with COPPA 2.0 as currently drafted.

Age Verification Requirement – We are concerned that COPPA 2.0 about the change to the existing COPPA knowledge standard from "actual knowledge" to a new standard of "knowledge fairly implied on the basis of objective circumstances." This change could lead operators to require age verification for all visitors, not just children, to an operator's website. This would increase the amount of information collected from visitors, increasing privacy and cybersecurity risks.

Treatment of Contextual Advertising – We are concerned that COPPA 2.0 would, even if unintentionally, prohibit contextual advertising, which could lead operators to charge for access or cut off services. Contextual advertising has played an important role in supporting the creation of free high-quality content for kids. Without the support of contextual advertising revenues, this content may no longer exist. This would have a notable impact on the digital divide.

No Preemption – Lastly, the bill does not offer effective preemption which will lead to a difficult patchwork of laws to comply with leading to different protections and experiences for consumers across the U.S.

Kids Online Safety Act

We are extremely concerned about the introduction of the Kids Online Safety Act. We believe this bill will require extensive modifications in order to protect the privacy and safety of young Americans. As written, it will require companies to censor content for users, which raises First Amendment concerns. A negligence standard for "duty of care" would create a burdensome risk of liability, leaving online platforms with virtually no choice but to restrict content.

The current text also requires companies to offer different services to users of different ages, effectively requiring age verification, which could be invasive to

privacy. Experts have noted this could require companies to collect more information than necessary on all users, not just kids.

We urge Congress to consider further improvement to KOSA that would meaningfully strengthen privacy protections and uphold Constitutional rights for all Americans.

We stand ready to continue to work with the Committee to ensure the proposals represent balanced and comprehensive federal standards to protect the privacy of all Americans. Thank you for considering our views.

Respectfully,

Christopher A. Mohr

President