June 26, 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

cc: House Leadership, Members of the House Committee on Energy and Commerce

Re: American Privacy Rights Act and Kids Online Safety Act

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 national, uniform consumer privacy legislation. We wanted to take the opportunity to provide our feedback on two bills under consideration during this hearing: **American Privacy Rights Act of 2024 (APRA), including the Children's Online Privacy Protection Act 2.0 (COPPA 2.0), and the Kids Online Safety Act (KOSA).** We remain hopeful that Congress will work together to move comprehensive legislation across the finish line. As such, we request that this letter be submitted into the legislative record.

SIIA is the principal trade association for those in the business of information. Our nearly 400 member companies reflect 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. However, we are concerned that the bill could unintentionally hamstring a variety of productive data uses that in turn create far-reaching domestic and international consequences.

Title I of the American Privacy Rights Act of 2024 - American Privacy Rights

Areas of Strength

Title I is a thoughtful draft that improves on the earlier APRA discussion draft and will serve as a positive step towards comprehensive federal privacy legislation.

We applaud the creation of 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.

From our perspective, the private right of action provision has improved, and we applaud the extension of the right to cure for 60 days, along with a 60-day deadline for providing notice before seeking actual damages. We also strongly support the provision to dismiss bad faith actions.

Finally, we strongly support the revised provisions that improve the bill's practical application to commonsense advertising practices. The draft now permits the use of ZIP code-level "coarse geolocation data" for use in contextual advertising. It also clarifies that direct mail and email targeted advertising is permitted, as well as data processing for advertising performance measurement. As we have raised in response to previous discussion drafts, these are critical tools for conducting business and maintaining a healthy online ecosystem.

Areas that Require Further Attention

First, although we are glad to see that the bill exempts PAI and inferences derived solely from PAI, we are concerned that Title I does not exempt data derived from PAI. This feature, set out in Section 101 (47)(B)(iii)(II) would turn PAI into sensitive covered data. This would include, for example, anything to do with a child. Furthermore, the latest discussion draft now specifies that sensitive covered data made available by a data broker is not considered to be "publicly available information." This means that if sensitive covered data appears in a publicly available source, a data broker could be sued for distributing this data unlawfully – even if it was already in the public domain. This would incorrectly attribute liability to entities that may not even have released this data into the public domain. Furthermore, this restriction on further

dissemination of public data cis unlikely to pass constitutional muster under the First Amendment.

Second, APRA imposes a presumption of illegality around benign areas of technological development and use, with minimal or no link to a privacy harm. For example, Section 102 would restrict all covered data collection and processing to a set of predetermined permitted purposes, resulting in unforeseen legal technicalities that would hamstring future technological development. For example, AI development would largely violate APRA's permitted purpose restrictions. Not only is general AI development not included as a permitted purpose, but models' natural application for a variety of purposes would run afoul of this section.

Third, the bill expands the definition of sensitive covered data to include new, inflexible categories that are overinclusive of data that may pose little risk, but also underinclusive of high-risk uses of data that the definition does not cover. The latest draft broadens the categories and now includes a vaguely defined "online activity profile," as well as data "identifying" its subject as a member of the armed forces. The latter is, of course, well-intentioned, but currently so broadly-worded it would capture even clerical data such as street addresses of military installations, or membership in veterans' associations. 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.

This overbreadth also extends to defining sensitive covered 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). This is particularly relevant because the APRA standard for minors' data has been changed to a standard of "actual knowledge or knowledge fairly implied on the basis of objective circumstances," which is impractical for businesses and circular.

Lastly, APRA imposes significant requirements on data brokers, and omits a variety of exemptions we believe would be helpful to permit entities that fall under this definition to engage in societally positive data sharing. The bill also departs from the definition of "data broker" in every U.S. state data broker law, which cover entities that process *and* transfer personal data. Instead, APRA defines data brokers as entities that process *or* transfer personal data they did not collect directly from a consumer. Even with APRA's service provider exemption, this could wrap in a variety of businesses that are neither commonly understood nor appropriately regulated as data brokers. For example, it could capture a social media platform that uses a user-

generated photo of multiple subjects—but where only one subject posts the photo—to inform the user experience and generate personalized content.

Title II of the American Privacy Rights Act of 2024 - COPPA 2.0

Areas of Strength

We see the inclusion of language to update COPPA in APRA as an encouraging step on protecting the privacy and safety of children 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.

Areas that Require Further Attention

We are concerned about the change of the knowledge standard from the discussion draft. The current outlines that knowledge, "means actual knowledge or knowledge fairly implied on the basis of objective circumstances." This effectively establishes a constructive knowledge standard which creates uncertainty from a compliance perspective. Additionally, it requires the FTC to write guidance on the knowledge standard but does not require anyone to follow that guidance

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. We urge the Committee to consider amending the definition to allow contextual advertising as defined under the 2013 Rule's internal operations definition.

Kids Online Safety Act (H.R. 7891)

Areas of Concern

We are extremely concerned about the impact of KOSA on both young people and all Americans. 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 encourage Congress to consider the Child and Teen Privacy and Safety Principles that SIIA released in March as a framework for legislation that avoids the concerns outlined above.

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