



HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON INNOVATION, DATA, AND COMMERCE

“Legislative Solutions to Protect Kids Online and Ensure Americans’ Data Privacy Rights”

April 17, 2024 – 10:00 AM

OVERVIEW

On Tuesday, April 17, the House Energy and Commerce Subcommittee on Innovation, Data, and Commerce held a hearing titled, “Legislative Solutions to Protect Kids Online and Ensure Americans’ Data Privacy Rights.” During the hearing, Members and witnesses discussed data minimization, targeted advertising and safe product design, enforcement, preemption, transparency and algorithmic accountability, data brokers and third-party transfers, and national security.

OPENING STATEMENTS

- [Subcommittee Chair Gus Bilirakis \(R-FL\)](#)
- [Subcommittee Ranking Member Jan Schakowsky \(D-IL\)](#)
- [Committee Chair Cathy McMorris Rodgers \(R-WA\)](#)
- [Committee Ranking Member Frank Pallone \(D-NJ\)](#)

WITNESS PANEL

- [Ms. Ava Smithing](#) – Director of Advocacy, Young People’s Alliance
- [The Honorable Maureen K. Ohlhausen](#) – Co-chair, 21st Century Privacy Coalition; former Commissioner, Federal Trade Commission
- [Ms. Katherine Kuehn](#) – Member, Board of Directors and CISO-in-Residence, National Technology Security Coalition
- [Ms. Kara Frederick](#) – Director, Tech Policy Center, The Heritage Foundation
- [Mr. Samir C. Jain](#) – Vice President of Policy, Center for Democracy and Technology
- [Mr. David Brody](#) – Managing Attorney, Digital Justice Initiative, Lawyers’ Committee for Civil Rights Under Law

LEGISLATION

- [H.R. ____](#), American Privacy Rights Act (APRA)
- [H.R. 7891](#), Kids Online Safety Act (KOSA)
- [H.R. 7890](#), Children and Teens' Online Privacy Protection Act (COPPA 2.0)
- [H.R. 5628](#), Algorithmic Accountability Act of 2023
- [H.R. 4311](#), DELETE Act
- [H.R. 4568](#), TLDR Act
- [H.R. 5534](#), Banning Surveillance Advertising Act of 2023
- [H.R. 5778](#), Sammy's Law of 2023
- [H.R. 6149](#), Protecting Kids on Social Media Act
- [H.R. 6429](#), SCREEN Act

QUESTION AND ANSWER SUMMARY

Data Minimization

Chair Rodgers asked how the APRA would complement KOSA and limit the collection and exploitation of children's data. Ms. Smithing commended the APRA's data minimization provisions to limit the amount of data collected on children. She also advocated for provisions to allow consumers to opt out of targeted advertising and suggested requiring platforms to turn off targeted advertising to children by default.

Ranking Member Schakowsky asked about the importance of specific privacy protections for biometric information. Mr. Brody explained biometric and genetic information is particularly sensitive because it cannot be changed after a data compromise. He also noted this information is often used in discriminatory ways, highlighting the increasing use of flawed facial recognition technologies.

Ranking Member Schakowsky noted scammers can buy lists of people more vulnerable to scams and fraud from data brokers and asked how the APRA would address this issue. Mr. Jain argued data minimization requirements would help limit the availability of data on vulnerable populations, reining in scams and fraud.

Ranking Member Pallone asked if the data minimization requirements in COPPA 2.0 are sufficient to protect children online. Mr. Jain argued COPPA 2.0's minimization provisions only focus on the collection of information, while APRA more broadly applies to the collection, processing, transfer, and use of data. He added the standard is stronger in APRA because it more specifically limits collection to what is necessary to provide the product or service or other permissible purposes.

Rep. Larry Bucshon (R-IN) stressed the need to balance privacy protections for sensitive personal information without stifling biomedical research and innovation. He asked if the APRA should include exceptions for this type of research. Ms. Kuehn argued the existing opt-in mechanisms are sufficient to protect consumer privacy and prevent stifling innovation.

Rep. Debbie Dingell (D-MI) asked if the APRA sufficiently addresses data minimization. Mr. Jain agreed the basic standard is strong, but suggested examining the permissible purposes section to ensure they are appropriately narrow. For example, he warned that allowing the collection of data to prevent fraud could be broadly interpreted by data brokers, offering a loophole to these minimization provisions.

Rep. John James (R-MI) asked how the APRA would establish stronger data security standards and better protect seniors from exploitation and fraud. Ms. Kuehn argued the data minimization and consumer control provisions of the bill are strong steps to better protect consumer data. She added measures to require simplified privacy policies are critical, especially for seniors.

Rep. Kat Cammack (R-FL) asked if the APRA's opt-out mechanism should be altered to an opt-in, raising concerns consumers will not utilize the opt-out. Ms. Frederick agreed default privacy settings should be the most stringent. Mr. Jain noted there are some settings where an opt-out would be appropriate and stressed the need to strike the right balance in these default settings. Ms. Kuehn suggested looking at lessons learned from international counterparts' privacy laws, such as the General Data Protection Regulation (GDPR), to inform the opt-out vs. opt-in debate.

Targeted Advertising and Safe Product Design

Chair Bilirakis asked how design obligations could prevent harm to children online. Ms. Smithing argued design-specific legislation is critical because while data minimization can reduce the amount of information collected on users, features such as like counts and beauty filters cause negative mental health impacts on children and teens.

Ranking Member Pallone asked if specific protections for children should be added to the APRA. Mr. Jain explained children need additional protections because it is more difficult for them to distinguish between advertising content and provide meaningful consent. He recommended banning targeted advertising to kids, prohibiting data transfers without parental consent, and creating a specific Youth Marketing Division at the Federal Trade Commission (FTC) to examine unique harms to children online. Ranking Member Pallone asked if a comprehensive privacy bill would better protect children online than a kids-specific bill. Mr. Jain argued beginning with a comprehensive privacy bill could help shed light on what additional children-specific protections are needed.

Ranking Member Pallone questioned whether notice and consent mechanisms are effective in protecting children's privacy. Mr. Brody argued notice and consent are insufficient and instead advocated for product safety requirements.

Rep. Bucshon stressed the need to ensure children are safe online without restricting their access to the digital world, especially as digital literacy is necessary to succeed in the modern economy. He asked if KOSA and COPPA 2.0 strike the right balance. Ms. Frederick responded affirmatively. Ms. Smithing agreed companies should be required to ensure safe product design, rather than placing the burden of safety on children and parents.

Rep. Kathy Castor (D-FL) asked why both privacy and design safety measures are necessary to protect kids online. Ms. Smithing argued KOSA's provisions to address design safety concerns will be bolstered by privacy legislation limiting data collection, ensuring platforms have less data to support their targeted advertising mechanisms.

Rep. Tim Walberg (R-MI) asked why targeted advertising is particularly harmful to children. Ms. Smithing explained advertising is predicated on insecurity, heightened by data allowing ads to be targeted to specific insecurities, such as weight loss.

Rep. Walberg raised concerns Big Tech platforms are seeking to expand children's engagement online and asked why legislation to prevent this behavior is necessary. Ms. Frederick explained tech companies recognize the revenue that can be earned from children on their platforms and emphasized the need for transparency to expose this behavior. She also warned that children are uniquely vulnerable to addictive design features.

Rep. Dingell asked about the importance of privacy-by-design requirements. Ms. Frederick explained requiring privacy proactively will help regulations keep pace with technological advancements.

Rep. Russ Fulcher (R-ID) noted the APRA would place limits on covered entities' ability to target advertising. He asked where the line should be drawn on the level of tailoring for ads. Mr. Jain noted while mass data collection has allowed companies to target advertisements in extremely harmful ways, there is a role for more reasonable tailored advertising, such as contextual tailored advertising or first-party tailored advertising. He argued lawmakers need to enable an economically viable advertising system with appropriate privacy protections and commended APRA's efforts to find this balance.

Rep. Kim Schrier (D-WA) inquired about the addictive nature of social media platforms' design features and their impact on children. Ms. Smithing argued data minimization provisions and opt-out mechanisms for targeted ads are essential to address addictive product features, limiting the amount of data fed into recommendation algorithms. She noted the cadence in which these posts are delivered is the primary issue, rather than the contents of them.

Enforcement

Chair Bilirakis asked how KOSA and the APRA would give consumers more control over their safety and data online. Ms. Frederick argued these bills would provide for consumer self-governance, transparency, and effective enforcement measures against online harm. She asserted a private right of action is critical to bolster accountability and incentivize better behavior.

Rep. Darren Soto (D-FL) noted Mr. Brody raised concerns the APRA includes a "backtracking" on causes of action for privacy violations in his opening statement and asked him to elaborate on this concern. Mr. Brody explained the APRA's predecessor, the American Data Privacy and Protection Act ([ADPPA](#)), included a privacy right of action for the collection, processing, retention, and transfer of sensitive personal information, while the APRA only includes a private right of action for transfer.

Rep. Fulcher asked what type of liability should rest with service providers for misuse of consumer data. Ms. Ohlhausen commended the APRA's treatment of this issue, placing the responsibility with the party most equipped to protect the data.

Rep. Robin Kelly (D-IL) asked why a private right of action to enforce violations of the APRA's data minimization provisions is necessary. Mr. Jain argued data minimization is a central feature of the APRA, underscoring the need for strong enforcement mechanisms. He explained a private right of action would allow individuals to obtain recovery and deter companies from violating consumers' privacy.

Rep. Diana Harshbarger (R-TN) raised concerns about the FTC's plans to move forward with its proposed data security [regulations](#) and asked about the impact of these rules. Ms. Ohlhausen argued Congress should provide the FTC with additional clarity and authority to address consumer privacy. She added the APRA would allow the FTC to use its expertise in privacy and security more effectively. Ms. Kuehn contended a dual regulatory regime with the FTC's rulemaking and the APRA would help innovation, clarifying federal authority in this space and setting strong guidance, particularly in addressing third and fourth-party risk. Mr. Brody agreed the FTC should have strong authority to regulate common carriers.

Rep. Cammack asked if it makes sense to provide the FTC with broad data security authorities, but leave the Federal Communications Commission (FCC) responsible for data breach notifications for legacy communications. Ms. Ohlhausen argued authority over these issues should be under one unified agency.

Preemption

Chair Rodgers asked about the importance of a uniform federal privacy standard. Ms. Kuehn argued a single national standard is critical to ensure companies can effectively comply with privacy standards, eliminating the patchwork of state standards and bringing the U.S. in parity with its international partners and allies.

Rep. Bucshon asked if there are existing state laws that could inform privacy federal legislation. Ms. Frederick advocated for specific restrictions about third-party data transfers and age verification mechanisms. She noted Florida's social media legislation could provide a strong model for age verification, for example.

Rep. Debbie Lesko (R-AZ) asked if the APRA's preemption language is strong enough. Mr. Jain argued the bill strikes the right balance in establishing a uniform national standard. He noted the Health Insurance Portability and Accountability Act (HIPAA) provides a strong example of success in legislation where state and federal jurisdictions can coexist. Ms. Ohlhausen raised concerns some exceptions to allow state laws, such as tort and common law, could allow states to sidestep the preemption provision.

Rep. Harshbarger asked how the APRA would change the relationship between small businesses and Big Tech companies. Ms. Ohlhausen argued the bill strikes the right balance in allowing certain uses of data and protecting privacy, ensuring small businesses can compete against larger companies. She advocated for a single national standard, which would lower compliance costs for small businesses.

Transparency and Algorithmic Accountability

Chair Rodgers asked if companies should be required to conduct algorithmic impact assessments. Ms. Frederick agreed, emphasizing the importance of transparency.

Rep. Yvette Clarke (D-NY) inquired about the importance of provisions to prohibit algorithmic discrimination and require algorithmic accountability in a comprehensive privacy bill. Mr. Brody explained algorithmic products are increasingly deployed with inadequate testing, often resulting in the exclusion of certain populations from opportunities and the charging of higher rates for goods and services. He stressed the need to require companies to implement safeguards against these types of biases and to test systems before and after deployment to ensure they work as intended. Mr. Jain added greater transparency into AI systems, as outlined in the Algorithmic Accountability Act and APRA, are key aspects in this effort as well.

Rep. Clarke raised concerns about exceptions for targeted advertising based on status as a member of a protected class in the APRA. She asked if this carveout could result in more targeted discrimination. Mr. Brody agreed the provision is concerning. He argued targeted advertising is an important way for consumers to learn of opportunities and warned that minority communities have been specifically redlined from receiving certain ads. He stressed the need to ensure opportunities are not only directed to specific groups.

Rep. Kelly raised concerns about the disparate impacts of flawed facial recognition technologies and asked what safeguards are necessary to ensure a comprehensive privacy bill protects Americans' civil rights. Mr. Brody expressed support for the anti-discrimination protections included in the APRA that prohibit discriminatory uses of personal data in depriving equal opportunity to goods and services. He also advocated for algorithmic impact assessments, consumer rights to data access, correction, and deletion, and strong enforcement mechanisms, including state and private rights of action.

Rep. Lori Trahan (D-MA) asked about the importance of provisions in the TLDR Act to require companies to create standardized terms of service summaries that are understandable for children and parents. Ms. Smithing argued clear and concise language is essential to ensure consumers understand what they are agreeing to, as existing privacy policies are often extremely long and complicated, encouraging users to skip over them.

Rep. Trahan inquired about the importance of providing independent researchers access to social media platforms' data to examine online privacy and safety threats. Mr. Jain agreed increased transparency, especially for researchers, is essential to examine the negative impacts of social media platforms.

Data Brokers and Third-Party Transfers

Ranking Member Pallone asked about the merits of a centralized deletion mechanism for consumers to request all data brokers delete their data. Mr. Jain agreed a centralized mechanism would make it easier for consumers to exercise their data rights and suggested adding this provision to the APRA.

Rep. Lesko noted some stakeholders have raised concerns the APRA's restrictions on third-party data transfers would apply to companies and their subsidiaries. Ms. Frederick argued these restrictions are essential to ensure foreign adversaries are unable to exploit loopholes and access American data.

Rep. Trahan asked how provisions to address data brokers in the APRA differ from those in the DELETE Act. Mr. Jain argued incorporating the DELETE Act's provision to create a centralized mechanism to request deletion of data brokers' information on consumers would strengthen the APRA.

National Security

Rep. Jeff Duncan (R-SC) asked which entities or nations pose the greatest threat to American data. Mr. Frederick argued the Chinese Communist Party (CCP) poses the greatest threat, given the strict national intelligence laws Chinese companies must comply with and China's increasing AI capabilities. Ms. Ohlhausen noted strong privacy laws will provide protections against a wide variety of threats, including foreign adversaries and scammers. Mr. Brody suggested focusing on Big Tech and data brokers, as they have the greatest control over their systems and the greatest abilities to prevent harm.

--

Please click [here](#) for the archived hearing.