

Ms. Kara Frederick

May 21, 2024

Jessica Herron  
Legislative Clerk  
Subcommittee on Innovation, Data, and Commerce  
House Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, DC 20515-6115

Re: Kara Frederick's Responses to Additional Questions for the Record

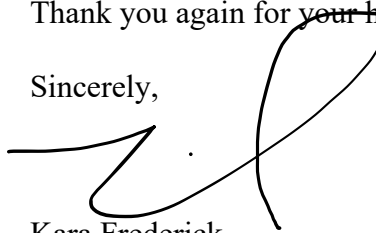
Dear Ms. Herron:

I deeply appreciate the Subcommittee's invitation for me to appear before the Subcommittee on Innovation, Data, and Commerce on Wednesday, April 17, 2024 titled, "Legislative Solutions to Protect Kids Online and Ensure Americans' Data Privacy Rights."

Pursuant to the Rules of the Committee on Energy and Commerce, I am attaching my answers to additional questions for the record, in the required format.

Thank you again for your help, and please let me know if you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to be 'Kara Frederick', written over the word 'help' in the previous paragraph. The signature is fluid and cursive, with a large loop at the end.

Kara Frederick  
Director, Tech Policy Center  
The Heritage Foundation

Ms. Kara Frederick

## **The Honorable Russ Fulcher**

**In response to my question about third-party data providers, a.k.a., “data brokers,” where I noted tailored marketing messages and advertisements to different customers are commonly used through marketing automation and other tools, I asked about where is the line on the level of tailoring of messaging and advertising, given the American Privacy Rights Act (ARPA) strongly keeps the decision ownership with the consumer, the issue of delineating between contextual ads, first-party ads being okay provided they are not behind paywalls, and that ARPA generally strikes the right balance. I want to ensure a company can use a marketing automation tool but is not excessively or intrusively profiling individual customers.**

**1. Does this just come down to disaggregating individual customers into categories and the types and amount of tailoring of a message that can be done under ARPA? When it comes to the categories of ads you mentioned – “contextual, first-party not behind a paywall, etc.” – can you discuss further what should be allowable versus not, fitting within the requirements of ARPA?**

APRA defines targeted advertising as relying on known or predicted preferences or interests associated with an individual or device identified by a unique identifier. The bill requires covered entities that engage in targeted advertising to provide individuals with a clear and conspicuous means to opt out.

The bill’s current exclusions offer a balance between intrusive profiling and harnessing automation for efficiency in the market. These include excluding first-party advertising based on an individual’s use of a website or online service that offers a product or service related to the subject of the advertisement. APRA also excludes contextual advertising, which is based on the content of the webpage on which the advertisement appears. These exceptions allow websites and online services to ensure an ad’s relevance, maintain consistency with their brand/marketing, and avoid consumer confusion without relying on personal or sensitive user data.

However, the draft can go further in requiring data minimization for individuals at a certain age threshold. Targeted advertising at minors and even teenagers should be considered off-limits.

**2. Talk to me about reporting that is both efficient and thorough, without being overly burdensome, when it comes to reporting data privacy and security practices on the issue of transparency?**

APRA’s limitation of reporting requirements to large data holders is a critical provision in ensuring efficient and “not overly burdensome” reporting. Duly, this provision spares new entrants and small competitors from asymmetric demands on their resources. (The bill defines a large data holder as an entity that has an annual gross revenue of \$250 million or more and collects, processes, retains, or transfers data of 5 million or more individuals, 15 million or more portable connected devices, or 35 million or more connected devices.)

Ms. Kara Frederick

APRA encourages transparency from large data holders by requiring them to designate one qualified employee as a privacy officer and one qualified employee to serve as a data security officer, subject to internal reporting structure requirements.

Subsection (a) paragraph (2) subparagraph (C) requires periodic reviews and updates to policies, practices, and procedures, biennial and comprehensive audits to ensure compliance with the bill, and to share the audits with the FTC if requested. It also directs entities to educate and train their employees about the requirements without being overly prescriptive. Large data holders can also include a level of granularity in their privacy and security reporting that strikes a similar balance, including notifications of: attempted data breaches, known probing attempts by foreign adversaries, and other forms of data sharing with third parties.