Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

CDIAONLINE.ORG

The Honorable Gus Bilirakis, Chair
The Honorable Jan Schakowsky, Ranking Member
Subcommittee on Innovation, Data, and Commerce of the
House Committee on Energy & Commerce
2123 Rayburn House Office Building
Washington, DC 20515

Re: American Privacy Rights Act

Dear Chair Bilirakis and Ranking Member Schakowsky:

The Consumer Data Industry Association (CDIA)[1] applauds the committee's effort to reach consensus on a national, comprehensive, preemptive privacy law. The American Privacy Rights Act does, however, pose some concerns for CDIA and its members and we write today to detail those points and offer our assistance in crafting a bill that both protects consumers and promotes commerce.

The CDIA's members are consumer reporting agencies that provide information services to and for the American economy. The federal Fair Credit Reporting Act (FCRA) is the nation's first national privacy law, passed in 1970, and our comments reflect our deep history of privacy regulation and our members' role in connecting consumers to the American economy.

Our thoughts around the APRA relate to four areas:

1. An overly broad scope and limited preemption interferes with existing privacy laws without clear exemptions for entities regulated by existing privacy laws.
2. The bill's data broker requirements are not necessary and potentially harmful to consumers, businesses, governments, and nonprofits.
3. The APRA's opt-out for algorithms may unintentionally create harm for consumers by restricting the ability of businesses to provide services, including credit, and offer solutions to prevent fraud.
4. The private right of action doesn't accurately depict the business transactions between third parties and consumers.

1. An overly broad scope and limited preemption (Sec. 20) interferes with existing privacy laws.

A. The Section 20(b) "in compliance with" creates an uncertain regulatory structure.

Congress has created a myriad of national sectoral privacy laws, including the FCRA in 1970, the Gramm-Leach-Bliley Act (GLBA) and the Drivers Privacy Protection Act (DPPA) and we note that the APRA considers these other privacy laws (Sec. 20(b)(3)(B)). However, as drafted, the APRA only applies to persons who are "in compliance with" such laws (Sec. 20(b)(3)(A)) and we ask that APRA follow the approach of every state's comprehensive privacy law that excludes from application the transactions, entities, and information *regulated by* (rather than *in compliance with*) the FCRA.

[1] The Consumer Data Industry Association (CDIA) is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals, and to help businesses, governments and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition and expanding consumers' access to financial and other products suited to their unique needs.

The "in compliance with" language raises the stakes for violating the FCRA while providing little consumer protection. Specifically, the limited exemption creates a double jeopardy situation wherein FCRA, GLBA, and DPPA violations also become APRA violations. There is already substantial enforcement in place of existing laws: The FCRA is rigorously enforced by the CFPB, state attorneys general, and the Federal Trade Commission. Private FCRA litigation is rampant and consumers have the ability to obtain damages, even where a consumer may not actually be harmed. In many respects, the FCRA can be viewed as a strict liability statute where technical violations can be actionable.

The result of all the enforcement available is that a CRA found to have violated the FCRA might face penalties for violating all provisions of the APRA, even if the FCRA violation was technical (without real harm to the consumer) and the penalties imposed for violating the FCRA were small. In its current form, the APRA preemption language permits one case to open the door to other cases, with a plaintiff able to allege that the CRA or other entity potentially violated state privacy law as well as the APRA.

B. The Section 20(a) preemption language is incomplete.

The APRA's limited preemption (Sec. 20) interferes with existing privacy laws. Preemption is unnecessarily limited by terms like "general applicability" (Sec. 20(a)(3)(A)), and "sector specific laws unrelated to data privacy...provided such laws do not directly conflict..." with the APRA (Sec. 20(a)(3)(I). We would ask that the committee clarify and define the specific comprehensive privacy, data broker, and deletion laws ripe for preemption.

2. The bill's data broker requirements (Sec. 12) are not necessary and potentially harmful to consumers, businesses, governments, and nonprofits.

There are many types of data brokers and consideration of each should be part of a fulsome debate. Information services companies, considered "data brokers" under the bill's definitions, are integral to American commerce in verifying identities, authenticating consumers and preventing fraud and identity theft.

These companies help prevent fraud against government agencies, nonprofits, businesses, and the consumer while also aiding with law enforcement investigations, risk management, and insurance beneficiary location. The national benefits provided by these companies would be harmed by the APRA's "do not collect" requirement for data brokers, substantially harming commerce and interfering with the socially beneficial uses noted above.

When the subcommittee considers the APRA this week, it will also consider H.R. 4311, the Data Elimination and Limiting Extensive Tracking and Exchange Act (DELETE Act). The APRA would limit data flows on the front end with its "do not collect" while the "delete my data" provisions in the DELETE Act remove data on the back end. The two bills, in tandem, create threats to critical data flows for consumers, governments, businesses, and nonprofits.

We are pleased the APRA recognizes the value of fraud prevention with the exemption for nonprofits "whose primary mission is to prevent, investigate, or deter fraud or to train anti-fraud professionals, or educate the public about fraud, including insurance fraud, securities fraud, and financial fraud..." Sec. 2(10)(C)(v). Fraud prevention protects American consumers, but many would be unprotected by this exemption since the bulk of fraud prevention in the U.S. is done by for-profit companies. To fully protect consumers, the bill should exempt fraud prevention as seen in all state comprehensive privacy laws.

3. The APRA's opt-out for algorithms (Sec. 14) may unintentionally create harm for consumers by restricting the ability of businesses to provide services and offer solutions to prevent fraud.

Businesses use algorithms for many socially beneficial purposes, including matching consumers with the appropriate financial services, aligning government benefits with those eligible, and connecting consumers with healthcare subsidies and assistance. The algorithms contemplated by the APRA could include credit scores, thereby limiting how credit scores function to measure risk. The inability of companies to see credit scores will likely put smaller businesses – with less data

to view – at a competitive disadvantage. Fraud scores and identity verification scores will also be limited by the APRA, as well as scores that match consumers to private and public benefits. The consequences to consumers for opting out of these algorithms will be significant, as will the costs for businesses, governments, and nonprofits that cannot adequately conduct critical risk management to maintain the viability and applicability of their programs and benefits.

4. **The private right of action (Sec. 19) doesn't accurately depict the business transactions between third parties and consumers.**

CDIA's members are third parties and do not have direct relationships with consumers. While Section 20 offers a safe harbor like a cure period for certain businesses, no such safe harbor is available for third parties who do not have direct consumer contact and the CDIA cannot endorse a private right of action.

Summary

Thank you for your time and attention on these important matters and I am happy to discuss our concerns in greater detail with you, your staff, and Chair Rodgers and Ranking Member Pallone.

Sincerely,

Dan Smith
President & CEO

cc: The Honorable Cathy McMorris Rodgers, Chair, House Committee on Energy & Commerce
The Honorable Frank Pallone, Jr., Ranking Member, House Committee on Energy & Commerce