U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

April 17, 2024

The Honorable Gus Bilirakis
Chair
Subcommittee on Innovation, Data & Commerce
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Innovation, Data & Commerce
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

In advance of your Subcommittee's hearing, "Legislative Solutions to Protect Kids Online and Ensure American Data Privacy Rights," the U.S. Chamber of Commerce ("the Chamber") offers the following thoughts and concerns regarding draft legislation titled "American Privacy Rights Act" ("APRA").

The Chamber has supported efforts to pass data privacy legislation that includes strong preemption language. Such an approach is necessary to achieve the goal of a national set of privacy requirements that protects children and consumers, allows businesses, including small businesses and entrepreneurs, to use the latest technology, and continue American global leadership in technology and innovation. In the absence of a national approach, the Chamber supports the bi-partisan consensus privacy approach that has created effective privacy protections in Texas[1], Tennessee[2], Virginia[3] and eleven other states.[4]

Unfortunately, in its current form, the APRA would fail to create a national standard and imposes California-style privacy standards that undermine the consensus privacy approach that protects the privacy rights of almost 100 million Americans.

Our concerns are outlined in more detail below.

I. A Single National Privacy Standard

Congress must pass a fully preemptive privacy law that eliminates a state patchwork of privacy laws and prevents States from drafting laws that survive preemption in the future. A single *preemptive* national privacy standard would allow the United States to reap the benefits of the 21st century digital economy and enable a thriving ecosystem that facilitates small business growth. Simply adopting a national privacy law without strong preemption would enable a state

[1] Letter to Texas House *available at* https://americaninnovators.com/wp-content/uploads/2023/04/State_HB4_TexasDataPrivacyandSecurityAct_TXHouse.pdf
[2] Letter to Tennessee Legislature, *available at* https://americaninnovators.com/wp-content/uploads/2023/04/230417_State_BS73_TNPrivacy_TNSenate.pdf
[3] Letter to Virginia Governor, *available at* https://americaninnovators.com/wp-content/uploads/2022/08/Virginia-Data-Privacy-Act-Letter.pdf
[4] Fourteen states have passed the Consensus Privacy Approach including New Hampshire, Virginia, Florida, Kentucky, Tennessee, Indiana, Iowa, Montana, Texas, Colorado, Utah, Delaware, Connecticut, and Oregon.

patchwork of laws that will be confusing to consumers and potentially impossible for small businesses to comply.

A recent report from ITI highlighted that a national patchwork of privacy laws would cost the United States economy $1 trillion and disproportionately impact small businesses with a $200 billion economic burden.[5] A majority of small businesses are worried a patchwork of state laws will increase litigation and compliance costs.[6]

The APRA draft does not address concerns previously raised with preemption language used in the 117th Congress's American Data Privacy and Protection Act ("ADPPA"). Although APRA states it seeks a "uniform national data privacy and security standard," the operative language APRA uses to preempt state laws is limited and could inadvertently lead to a federal floor and encourage states to pass more restrictive privacy laws. APRA only preempts "any law, regulation, rule, or requirement *covered by* the provisions of this Act or a rule, regulation, or requirement promulgated under this Act."

To provide the strongest preemption, according to a Congressional Research Service report, Congress should avoid merely preempting what a proposed bill is "covering" or "covered by," because such clauses are considered by the United States Supreme Court to be less restrictive on states than phrases like "related to."[7] According to the Supreme Court, "'Covering' is a more restrictive term [on what can be preempted] which indicates that preemption will lie only if the federal regulations substantially subsume the subject matter of the relevant state law."[8] A national privacy law that merely preempts what it "covers" and then provides for exceptions to that preemption would likely be taken by many as evidence that Congress has not intended to "substantially subsume" regulation.

The APRA draft also establishes exceptions to preemption in the areas of consumer protection, health data, and remedies established under California's Consumer Privacy Act and highly abused lawsuits under the Illinois Biometric Privacy Law. These exceptions could easily be exploited in lawsuits and by activist legislatures to get around desired preemption.

We, therefore, encourage the House Energy & Commerce Committee to adopt strong preemption language. In recent years, legislation has been authored by Republican and Democrats that would provide strong preemption concerning broad issues as opposed to only preempting what a law covers:

- In the 115th Congress, H.R. 3388, the unanimously passed "SELF DRIVE Act" which preempted broad categories of safety issues.

- In the 117th Congress, H.R. 1816, the Information Transparency and Personal Data Control Act provided that, "No State or political subdivision of a State may adopt, maintain,

---

[5] https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/.
[6] https://americaninnovators.com/wp-content/uploads/2023/09/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf
[7] *Id.* at 10.
[8] Congressional Research Service, "Federal Preemption: A Legal Primer" (Mary 18, 2023) *available at* https://crsreports.congress.gov/product/pdf/R/R45825. (Citing *CSX Transportation, Inc. v. Easterwood*, 507 U.S. 663 (1993)).

enforce, or continue in effect any law, regulation, rule, requirement, or standard *related to* the data privacy or associated activities of covered entities."[9]

- In the 118th Congress, House Financial Services Committee Chairman Patrick McHenry has proposed the "Data Privacy Act of 2023," which provides that legislation "supersedes any statute or rule of a State."[10]

II. Private Right of Action

Comprehensive privacy legislation should leave enforcement to agencies like the Federal Trade Commission and state attorneys general and not empower the private trial bar at the expense of business innovation and viability. Frivolous, non-harm-based litigation has been used in the past to extract costly settlements from companies, even small businesses, based on privacy law provisions granting a private right of action. Private rights of action are ill-suited in privacy laws because:[11]

- Private rights of action undermine appropriate agency enforcement and allow plaintiffs' lawyers to set policy nationwide, rather than allowing expert regulators to shape and balance policy and protections. By contrast, statutes enforced exclusively by agencies are appropriately guided by experts in the field who can be expected to understand the complexities of encouraging compliance and innovation while preventing and remediating harms.

- They can also lead to a series of inconsistent and dramatically varied, district-by-district court rulings. Agency enforcement can provide constructive, consistent decisions that shape privacy protections for all American consumers and provide structure for companies aiming to align their practices with existing and developing law.

- Combined with the power handed to the plaintiffs' bar in Federal Rule of Civil Procedure 23, private rights of action are routinely abused by plaintiffs' attorneys, leading to grossly expensive litigation and staggeringly high settlements that disproportionally benefit plaintiffs' lawyers rather than individuals whose privacy interests may have been infringed.

- They also hinder innovation and consumer choice by threatening companies with frivolous, excessive, and expensive litigation, particularly if those companies are at the forefront of transformative new technologies.

Private rights of action would be particularly devastating for business under a privacy law that does not have a strong preemptive effect. Not only would states be able to continue

---

[9] https://www.congress.gov/bill/117th-congress/house-bill/1816/text (emphasis added)
[10] https://financialservices.house.gov/uploadedfiles/glb_2023_xml_2.24_934.pdf
[11] U.S. Chamber Institute for Legal Reform, *Ill-Suited: Private Rights of Action and Privacy Claims* (July 2019) *available at* https://instituteforlegalreform.com/wp-content/uploads/2020/10/Ill-Suited_-_Private_RIghts_of_Action_and_Privacy_Claims_Report.pdf.

passing their own laws, but individual judicial district precedent could also create further confusion and conflict.

III. Substantive Concerns

We also note the following substantive concerns with APRA as drafted:

- Artificial Intelligence & Algorithms—As drafted Sections 13 and 14 of APRA would significantly impair America's ability to compete with respect to Artificial Intelligence. APRA as drafted would encourage lawsuits against companies that do not allow individuals to opt out of using basic technologies in any place of public accommodation. This could severely limit access to things like insurance, credit, employment opportunities, and other apps and services consumers enjoy.

- Small Business Impacts—Although the bill exempts small business from the requirements of APRA, as drafted small businesses would have to meet three elements of a vague test to determine if they are identified as a small business. Under this draft, given APRA's inclusion of a private right of action, small businesses will have to bear high litigation costs in court just to prove they are not covered by the bill. Even if a small business is not directly covered by the bill, we are concerned that the digital tools small businesses rely on could be threatened by other elements of APRA.

- Digital Advertising—The online advertising ecosystem is what enables Americans to enjoy the benefits of low-cost access to websites and apps. Unfortunately, as drafted APRA's data minimization, new FTC authorities to define what data is subject to opt-in consent, and universal opt-out for targeted advertising will threaten the contextual and personalized advertising that has driven U.S. internet growth and innovation.

- Data Broker Requirements—While the Chamber does not take issue with a data broker registry, we are concerned that the bill's mass "Do Not Collect" requirements for data brokers will inhibit societally beneficial users of data like fraud prevention, small business marketing, healthcare charitable services, and commercial credit and financing services.

- Loyalty Program— We are concerned that the APRA draft's prohibition on price and service discrimination could negatively impair customer loyalty programs. In particular Section 8(b)(a)(i)(IV) would require companies obtain "affirmative express consent for the transfer of any data collected in connection with a bona fide loyalty program." There is concern this provision would require consent every time data is transferred and would subject companies to private rights of action for inadvertent errors if consent is required every time. This would have a chilling effect on offering loyalty programs like hotel, restaurant, and retail programs consumers enjoy.

The Chamber's goal is to have a national set of privacy requirements that protects children and consumers, allows businesses of all sizes to use the latest technology, and permits

the United States to be the global leader in technology and innovation. We believe that in its current form the APRA fails to meet those goals. The APRA would degrade the privacy protections enjoyed by almost 100 million Americans, would harm small businesses, and would endanger American global innovation leadership.

While the Chamber opposes the APRA in its current form, we stand ready to work with you to address our concerns and provide strong privacy protections for all Americans.

Sincerely,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

cc: Members of the House Committee on Energy & Commerce