



May 9, 2024

The Honorable John Hickenlooper
Chairman
Subcommittee on Consumer Protection,
Product Safety & Data Security
United States Senate

The Honorable Marsha Blackburn
Ranking Member
Subcommittee on Consumer Protection,
Production Safety & Data Security
United States Senate

Dear Chairman Hickenlooper and Ranking Member Blackburn:

Thank you for the opportunity for the U.S. Chamber of Commerce (“Chamber”) to share our views regarding data minimization issues and our opposition to the draft American Privacy Rights Act (“APRA”) in the Subcommittee’s “Strengthening Data Security to Protect Consumers” hearing.

In its current form, APRA is deeply flawed and unworkable because it would fail to create a single national data privacy and security standard, would rely on the private trial bar for enforcement through private right of action provisions, and would impose unnecessary restrictions on goods and services that consumers enjoy.

In the absence of such federal privacy legislation, we have supported harmonized and workable proposals like the bipartisan Consensus Privacy Approach¹ in states like Virginia,² Texas,³ and Tennessee⁴ where more than 100 million Americans now enjoy privacy protections under a common framework.⁵

As drafted, APRA would reject full preemption and empower states to regulate beyond federal standards.

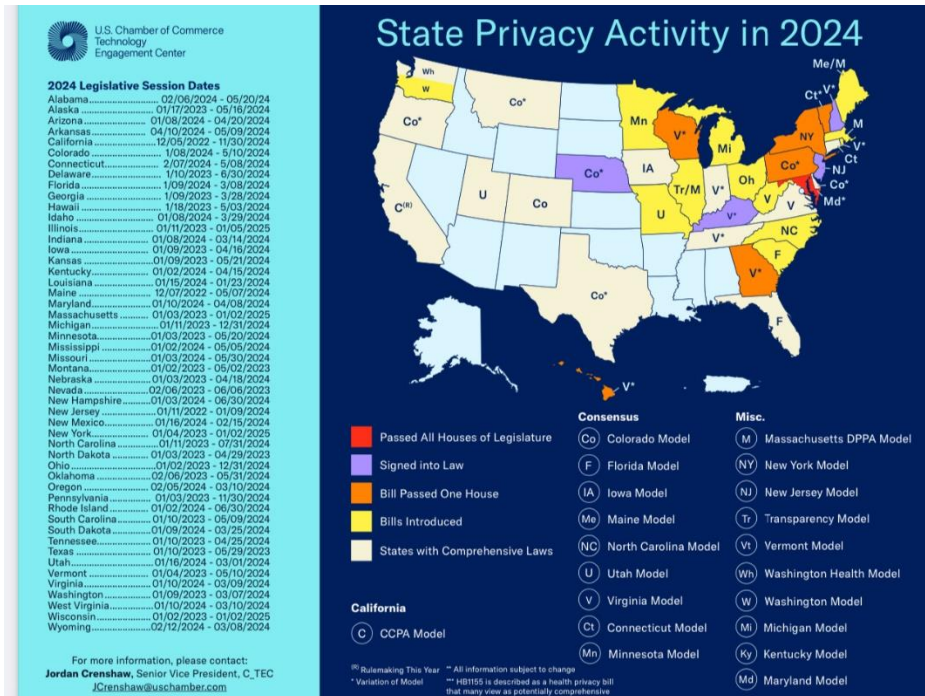
¹ U.S. Chamber Model Privacy Legislation (February 13, 2019) *available at* https://www.uschamber.com/assets/documents/uscc_dataprivacymodellegislation.pdf.

² Letter to Governor Northam *available at* <https://americaninnovators.com/wp-content/uploads/2022/08/Virginia-Data-Privacy-Act-Letter.pdf>.

³ Letter to Texas House *available at* https://americaninnovators.com/wp-content/uploads/2023/04/State_HB4_TexasDataPrivacyandSecurityAct_TXHouse.pdf.

⁴ Letter to Tennessee Senate *available at* https://americaninnovators.com/wp-content/uploads/2023/04/230417_State_BS73_TNPrivacy_TNSenate.pdf.

⁵ Jordan Crenshaw, “What Congress Can Learn from the States on Data Privacy,” Real Clear Policy (January 2024) *available at* https://www.realclearpolicy.com/2024/01/30/what_congress_can_learn_from_the_states_on_data_privacy_1008521.html.



I. Data Minimization

The Chamber recommends that APRA be revised to follow the Consensus Privacy Approach to data minimization to effectively protect consumers. Data minimization can be an important component of regulation to ensure the privacy and security of individuals, but overly broad, unnecessarily strict, or poorly crafted data minimization standards would impede innovation.

States that incorporated the Consensus Privacy Approach in law have enacted a balanced and workable data minimization standard. For example, states like Colorado, Tennessee, and Texas mandate that companies limit data collection to what is “adequate, relevant, and reasonably necessary” related to a disclosed or specified purpose.⁶

By contrast, APRA as drafted would limit all data collection and processing to “necessary, proportionate, and limit[ed] to provide or maintain” a specific product or service or consumer or anticipated communications.⁷ Although both the Consensus Privacy Approach and APRA have exceptions for certain practices like security, APRA would limit companies from collecting data that may be necessary for providing a service but can also have a societally beneficial purpose utilized by other companies. These secondary purposes include anti-fraud protections, Know Your Customer, and

⁶ See, e.g. Colo. Rev. Stat. § 6-1-1308(3); Tenn. Code Ann § 47-18-3208(a)(1); Tex. Bus. & Com. Code Ann § 541.101(1).

⁷ American Privacy Rights Act Discussion Draft § 3(a).

other web-based security applications, including those used by federal programs to reduce theft of benefits and identity fraud. Secondary data sets have also enabled law enforcement to intervene and stop incidents of violence, human trafficking, and organized crime.⁸

II. APRA Fails to Create a Single National Privacy Standard

Congress should include in any federal privacy legislation full preemption of state standards. A national privacy law without strong preemption would enable a state patchwork of laws that would be confusing to consumers and would potentially make it impossible for small businesses to comply.

A recent report 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.⁹ Many small businesses are worried that a patchwork of state laws will increase litigation and compliance costs.¹⁰

The APRA draft does not address concerns of the Chamber and other groups regarding of APRA's predecessor from the 117th Congress, the American Data Privacy and Protection Act. Although APRA's advocates express an intention to create "uniform national data privacy and security standard," the actual provisions of the draft provide only limited preemption and would allow states to pass more restrictive privacy laws. APRA only preempts "any law, regulation, rule, or requirement *covered by* [emphasis added] the provisions of this Act or a rule, regulation, or requirement promulgated under this Act."

According to a Congressional Research Service report, to provide the strongest preemption, Congress should use clearer and more forceful terms than "covering" or "covered by."¹¹ Congress should avoid merely preempting what a proposed bill is "covering" or "covered by," because such clauses are considered by the Supreme Court to be less restrictive on states than phrases like "related to."¹² According to the

⁸ Chamber Technology Engagement Center, "Data For Good: Promoting Safety, Health and Inclusion," (January 2020) available at https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf.

⁹ ITIF, "The Looming Cost of a Patchwork of State Privacy Laws," (January 2022) available at <https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/>.

¹⁰ U.S. Chamber "Empowering Small Business: The Impact of Technology on U.S. Small Business," (September 2023) available at <https://americaninnovators.com/wp-content/uploads/2023/09/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf>.

¹¹ Congressional Research Service "Federal Preemption: A Legal Primer," (May 2023) available at <https://crsreports.congress.gov/product/pdf/R/R45825>.

¹² *Id.* at 10.

Supreme Court, “[c]overing’ is a more restrictive term which indicates that preemption will lie only if the federal regulations substantially subsume the subject matter of the relevant state law.”¹³ 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 would also create exceptions to preemption in the areas of consumer protection, health data, and remedies based on California’s Consumer Privacy Act and highly abused lawsuits under the Illinois Biometric Privacy Law. These exceptions could easily be exploited in lawsuits and state legislatures to circumvent preemption in APRA.

There are better models. In recent years, legislation has been authored by both Republicans and Democrats that would provide strong preemption, including:

- H.R. 3388, the “SELF DRIVE Act,” from the 115th Congress, which preempted broad categories of activities and passed the House by unanimous consent.
- H.R. 1816, the Information Transparency and Personal Data Control Act, from the 117th Congress, that provided: “No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard *related to* [emphasis added] the data privacy or associated activities of covered entities.”¹⁴
- Financial Services Committee Chairman Patrick McHenry’s “Data Privacy Act of 2023” draft from the current Congress, which provides that federal legislation “supersedes any statute or rule of a State.”¹⁵

III. APRA Fails by Providing a Private Right of Action

Comprehensive privacy legislation should leave enforcement to agencies like the Federal Trade Commission and state attorneys general, not the private trial bar. Such private rights of action would invite unwarranted lawsuits that would ultimately hamstring innovation and the viability of some innovators. Frivolous, non-harm-based litigation has been used in the past to extract costly settlements from companies,

¹³ *CSX Transportation, Inc. v. Easterwood*, 507 U.S. 663 (1993).

¹⁴ <https://www.congress.gov/bill/117th-congress/house-bill/1816/text> (emphasis added).

¹⁵ https://financialservices.house.gov/uploadedfiles/glb_2023_xml_2.24_934.pdf.

including small businesses. Private rights of action are ill-suited in privacy laws because they:¹⁶

- Undermine appropriate agency enforcement and allow plaintiffs' lawyers to set policy nationwide. By contrast, statutes enforced exclusively by agencies are appropriately guided by experts in the field who are best positioned to understand the complexities of compliance, promote innovation, and prevent and remediate harms.
- Entail 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.
- Are, when combined with the power handed to the plaintiffs' bar in Federal Rule of Civil Procedure 23, routinely abused by plaintiffs' attorneys, leading to grossly expensive litigation and staggeringly high settlements that disproportionately benefit plaintiffs' lawyers.
- Hinder innovation and consumer choice by the uncertain and pervasive threat of lawsuits, particularly for companies 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 passing their own laws, but individual judicial district precedent could also create further confusion and conflict.

IV. Substantive Concerns with APRA

- **Artificial Intelligence & Algorithms**—As drafted, Sections 13 and 14 of APRA would significantly impair America's lead in 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, which could severely limit consumers' access to things like insurance, credit, employment opportunities, and other apps and services.
- **Small Business Impacts**—Small businesses would have to meet three elements of a vague test to determine if are exempt under the bill. Given

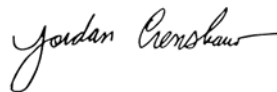
¹⁶ U.S. Chamber Institute for Legal Reform, "Ill-Suited: Private Rights of Action and Privacy Claims," (July 2019) available at https://instituteforlegalreform.com/wp-content/uploads/2020/10/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf.

APRA's private right of action provisions, small businesses would likely have to bear high litigation costs 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 would inhibit such important and beneficial uses as fraud prevention, small business marketing, healthcare, charitable contributions, and commercial credit and financing services.
- **Loyalty Program**—We are concerned that the APRA draft's prohibition on price and service discrimination could impair customer loyalty programs. 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. Such a requirement would have a chilling effect on offering loyalty programs like hotel, restaurant, and retail programs consumers enjoy.

The Chamber opposes APRA in its current form. We stand ready with the Subcommittee and other members of Congress to enact meaningful and workable national privacy legislation.

Sincerely,



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

cc: Committee on Commerce, Science, and Transportation