

Subcommittee on Innovation, Data, and Commerce
Markup of Three Bills
[May 23, 2024]

Documents for the record

At the conclusion of the meeting, the Chair asked and was given unanimous consent to include the following documents into the record:

1. Letter from the Connected Commerce Council (3C) to Chairs Rodgers and Bilirakis and Ranking Members Pallone and Schakowsky regarding the American Privacy Rights Act, May 23, 2024, submitted by the Majority.
2. Letter to Speaker Johnson, Leader Schumer, Leader McConnell, and Leader Jeffries on the Kids Online Safety Act, May 23, 2024, submitted by the Minority.
3. Letter from America's Credit Unions to Chair Bilirakis and Ranking Member Schakowsky on the American Privacy Rights Act, May 23, 2024, submitted by the Majority.
4. Letter from the Mortgage Bankers Association to Chair Bilirakis and Ranking Member Schakowsky on the American Privacy Rights Act, May 23, 2024, submitted by the Majority.
5. Letter from undersigned associations on the American Privacy Rights Act, May 22, 2024, submitted by the Majority.
6. Coalition letter on the American Privacy Rights Act, May 21, 2024, submitted by the Minority.
7. Letter from the American Property Casualty Insurance Association to Chairs Rodgers and Bilirakis and Ranking Members Schakowsky and Pallone on the American Privacy Rights Act, May 23, 2024, submitted by the Majority.
8. Letter from the Consumer Watchdog to Chairs Rodgers and Bilirakis regarding the American Privacy Rights Act, May 22, 2024, submitted by the Minority.
9. Letter from ATA Action to Chair Bilirakis, Ranking Member Schakowsky, and Vice Chair Walberg on the American Privacy Rights Act, May 23, 2024, submitted by the Majority.
10. Letter from ITI on Chairs Rodgers and Bilirakis and Ranking Members Pallone and Schakowsky on the American Privacy Rights Act, May 22, 2024, submitted by the Minority.
11. Joint trades letter to Chair Bilirakis and Ranking Member Schakowsky on the American Privacy Rights Act, May 23, 2024, submitted by the Majority.
12. Letter from civil society organizations to Chairs Rodgers, Pallone, Latta, Weber, and Ranking Member Matsui on the Kids Online Safety Act, May 23, 2024, submitted by the Minority.
13. Letter from undersigned groups to the Members of the Energy and Commerce Committee on the Kids Online Safety Act, May 23, 2024, submitted by the Minority.
14. Letter to Ranking Member Pallone from LGBT Tech regarding the Kids Online Safety Act, May 22, 2024, submitted by the Minority.
15. Letter from Main Street Privacy Coalition to Chairs Rodgers and Bilirakis and Ranking Members Pallone and Schakowsky on the American Privacy Rights Act, May 22, 2024, submitted by the Majority.
16. Letter from the National Association of Mutual Insurance Companies to Chairs Rodgers and Bilirakis and Ranking Members Pallone and Schakowsky on the American Privacy Rights Act, May 22, 2024, submitted by the Majority.

17. Letter from SIIA to Chair Rodgers and Ranking Member Pallone on the APRA, KOSA, and COPPA 2.0, May 22, 2024, submitted by the Minority.
18. Letter from TechNet to Members of the Innovation, Data, and Commerce Subcommittee regarding the American Privacy Rights Act, May 22, 2024, submitted by the Minority.
19. Letter from Cap 20 to Chairs Rodgers and Cantwell on the American Privacy Rights Act, May 20, 2024, submitted by Rep. Trahan.
20. Letter from undersigned organizations to Chairs Rodgers and Bilirakis and Ranking Members Pallone and Schakowsky, May 17, 2024, submitted by Rep. Trahan.



May 23, 2024

The Honorable Cathy McMorris Rodgers
Chair of the Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member of the Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Gus Bilirakis
Chair of the Subcommittee on Innovation, Data, and Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member of the Subcommittee on Innovation, Data, and Commerce
U.S. House of Representatives
Washington, D.C. 20515

Re: Connected Commerce Council's Comments on the American Privacy Rights Act of 2024

The Connected Commerce Council (3C), which represents digitally empowered small and medium-sized businesses (SMBs), is grateful for the chance to submit our thoughts on the American Privacy Rights Act of 2024 (APRA). We kindly request that this correspondence be included in the records for the forthcoming committee vote in the House Subcommittee on Innovation, Data, and Commerce on May 23, 2024.

The introduction of APRA represents a pivotal moment for businesses and consumers alike, marking a significant step toward establishing a more secure and private digital landscape. As Congress considers a national privacy law, it is critical to achieve the goal of safeguarding consumer data while allowing small businesses to advertise freely and operate without fear. Unfortunately, the American Privacy Rights Act, as written, raises some serious concerns for small businesses:

1. **The small business exemption is a misnomer.** The proposed exemption for small businesses within the APRA framework is misleading and does not provide genuine relief for small enterprises. Rather, it mandates that small businesses adhere to the same stringent requirements imposed on large technology corporations. Specifically, the legislation delineates that any business engaging in data transfer of any "value" shall not be considered a small business. Consequently, entities collaborating with third-party vendors for the enhancement of their website, advertising, and marketing efforts will find themselves subject to the regulations, irrespective of possessing fewer than 200,000 consumer records. The threshold of 200,000 data points also is exceedingly low, inadvertently encompassing millions of small businesses within its scope.
2. **The private right of action escalates legal risk.** APRA introduces a provision for private litigation, significantly increasing the potential for groundless legal actions against businesses, spearheaded by plaintiffs' attorneys. This scenario mirrors the past occurrences with patent infringement and ongoing issues with ADA lawsuits, where small businesses are targeted for allegedly excessive collection or processing of consumer data. Subsequently, these businesses are propositioned with settlement offers, which, while financially burdensome, are less costly than court proceedings, regardless of the businesses' innocence.
3. **The data minimization requirements are too restrictive.** The principle of "data minimization," as outlined, severely restricts small businesses' capacity to understand and interact with their clientele by limiting data collection and processing solely to information deemed "necessary...to provide a specific product or service requested by the individual." This restriction impedes:
 - a. Communication with current customers regarding forthcoming sales, new product launches, or marketing updates.
 - b. Website personalization based on user behavior and preferences.
 - c. Utilization of customer geographical data for strategic expansion decisions.
 - d. Collaboration with marketing partners to collect traffic data essential for website performance optimization.
 - e. Collaboration with advertising partners to gather basic consumer data vital for reaching potential customers.
 - f. Inclusion of images depicting store activities on digital platforms.
4. **There are complex opt-out mechanisms and ambiguous provisions.** The extensive nature of the opt-out provision for targeted advertising effectively nullifies opt-in agreements. Small businesses require clarity that browser-level opt-outs do not override their explicit store-level opt-ins, and consumers deserve a broader spectrum of choices

regarding their online content preferences. Furthermore, APRA's anti-discrimination provisions expose small businesses to an extensive array of enforcement actions and private lawsuits, seeking to delineate the boundaries of these newly introduced, broad standards. This concern could be readily addressed by aligning APRA's anti-discrimination guidelines with existing federal and state laws, rather than establishing a novel, undefined anti-discrimination framework.

5. **The state patchwork of privacy laws will still continue to grow.** APRA's failure to preempt state privacy laws and regulations perpetuates the existing fragmented landscape of state-level regulations. Navigating this complex patchwork imposes considerable burdens in terms of compliance costs and operational complexities on SMBs, placing them at a marked disadvantage relative to their larger counterparts.

In conclusion, we earnestly implore our esteemed lawmakers to closely examine the potential repercussions the American Privacy Rights Act may have on the very foundation of our nation's economy—small businesses. It is crucial to address and rectify these concerns and any unnecessary burdens on small businesses prior to the enactment of a national privacy law. By doing so, we can ensure that legislation not only protects privacy rights but also supports and fosters the growth and sustainability of small businesses across the country. We trust that with thoughtful consideration and amendments, the APRA can achieve its objectives without placing undue burdens on the small enterprises that are integral to our economy's vitality and prosperity. Thank you for your time and consideration.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Rob Retzlaff', with a stylized, cursive script.

Rob Retzlaff
Executive Director
Connected Commerce Council

May 23, 2024

The Honorable Mike Johnson
Speaker of the House
U.S. House of Representatives

The Honorable Chuck Schumer
Majority Leader
U.S. Senate

The Honorable Mitch McConnell
Republican Leader
U.S. Senate

The Honorable Hakeem Jeffries
Democratic Leader
U.S. House of Representatives

Dear Speaker Johnson, Leader Schumer, Leader McConnell, and Leader Jeffries,

On behalf of the millions of taxpayers and consumers, we, the undersigned organizations, write to you in opposition to S. 1409/H.R. 7891, the Kids Online Safety Act (KOSA). While we applaud your efforts to improve children's privacy and online safety, KOSA fails to achieve these laudable goals and, in fact, would create greater risks for America's youth in the technology age.

S. 1409/H.R. 7891, introduced by Sens. Richard Blumenthal (D-Conn.) and Marsha Blackburn (R-Tenn.), alongside Reps. Gus Bilirakis (R-Fla.) and Kathy Castor (D-Fla.), would broadly hold online platforms liable if their design and operation of products and services fails to mitigate wide-ranging societal issues such as mental health, suicide, and addiction. This untenable standard will result in platforms being forced to censor perfectly legal speech, including that of non-minors, fearing the liability repercussions KOSA's Sec. 102 creates.

To ensure platforms' compliance, Sec. 105 of KOSA would require public reporting on age-specific statistics for users under seventeen years old. Statutorily requiring the mass collection of aggregate minor user data stands in stark contrast to what laws intending to protect children's online activity and privacy should do. Moreover, imposing the Sec. 102 Duty of Care standards would also ultimately lead to age verification requirements for platforms, something which the U.S. Court of Appeals for the Third Circuit ruled as having serious First Amendment concerns in *ACLU v. Ashcroft* (2002) and again in *ACLU v. Mukasey* (2008).

Online platforms provide a valuable space where discourse around complex issues that range the political spectrum can occur. KOSA's first version awarded state Attorneys General sweeping powers to subjectively determine the criteria for harms to children. Immediately, interested parties on both sides of the aisle have already floated various ways they could weaponize KOSA (or similar proposals) against speech they dislike, making de facto censorship an almost certain result of the bill's passage. The second, and most recent approach, to this bill awards vast decision-making authority to regulators at the Federal Trade Commission (FTC), an agency under heavy scrutiny for blatant partisanship. The FTC has been the subject of dozens of oversight hearings in the 118th Congress. Simply put, changes to KOSA loosely replace a 50-state regulatory patchwork with a partisan regulatory board at a rogue federal agency.

Regulating the ways children and teens interact with the internet is entirely different, and in many ways opposite, of protecting them. For example, Sec. 103 of KOSA would enact limits on the abilities of minors to communicate with other users. The vague language employed would likely lead to minors being unable to communicate with other minors, as well as adult users, essentially flipping the light switch off on minors' ability to engage on the internet. If enacted, KOSA would also target platform

design infrastructure such as infinite scrolling and autoplay, placing limits on the amount of content – or in more constitutional terms, free speech – individuals can access.

Protecting children online is a complex and noble endeavor and we applaud your members for trying to undertake this effort. However, considering legislation that would undo the last 30 years of internet regulation by placing the responsibility for protecting children on partisan bureaucrats will fail to protect children and strip civil liberties from Americans of all ages. We urge you to reject advancing KOSA, and instead work towards empowering law enforcement to track and catch online predators and protecting the data privacy of all Americans.

Sincerely,

David Williams

President

Taxpayers Protection Alliance

Tirzah Duren

Vice President of Policy & Research

American Consumer Institute

Jessica Melugin

Director, Center for Technology & Innovation

Competitive Enterprise Institute

Yaël Ossowski

Deputy Director

Consumer Choice Center

Mario H. Lopez

President

Hispanic Leadership Fund

Bartlett Cleland

Executive Director

Innovation Economy Institute

Tom Giovanetti

Institute for Policy Innovation*

Douglas Carswell

President & CEO

Mississippi Center for Public Policy

Chris Cargill

President & CEO

Mountain States Policy Center

Pete Sepp

President

National Taxpayers Union

John Tamny

President

Parkview Institute

Daniel J. Erspamer

Chief Executive Officer

Pelican Institute for Public Policy

Josh Withrow

Fellow, Technology & Innovation Policy

R Street Institute

Stacie D. Rumenap

President

Stop Child Predators

Vance Ginn, Ph.D.

Former Chief Economist

White House OMB

Casey Given

President

Young Voices

**Organization Listed for Identification Purposes Only*



**America's
Credit Unions**

Jim Nussle

President & CEO
202-508-6745

jnussle@americascreditunions.org

99 M Street SE
Suite 300

Washington, DC 20003

May 23, 2024

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

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

Re: Today's Markup of the American Privacy Rights Act

Dear Chairman Bilirakis and Ranking Member Schakowsky:

On behalf of America's Credit Unions, I am writing to share our thoughts regarding the draft American Privacy Rights Act (APRA) ahead of today's Subcommittee markup. America's Credit Unions is the voice of consumers' best option for financial services: credit unions. We advocate for policies that allow the industry to effectively meet the needs of their more than 142 million members nationwide.

We applaud the efforts of Chair McMorris Rodgers and Chairwoman Cantwell in crafting comprehensive data privacy legislation and attempting to advance this issue. Credit unions strongly support the idea of a national data security and data privacy regime that includes robust security standards that apply to all who collect or hold personal data, recognizes existing Gramm-Leach-Bliley Act (GLBA) standards, and is preemptive of state laws. We firmly believe that there can be no data privacy until there is strong data security.

Stringent information security and privacy practices have long been a part of the financial services industries' business practices and are necessary as financial services are entrusted with consumers' personal information. This responsibility is reflected in the strong information security and privacy laws that govern data practices for the financial services industry as set forth in the GLBA. The GLBA's protection requirements are strengthened by federal and state regulators' examinations for compliance with the GLBA's requirements and robust enforcement for violations.

There are three key tenets that credit unions believe must be addressed in any new national data privacy law: a recognition of GLBA standards in place for financial institutions and a strong exemption from new burdensome requirements; a strong federal preemption from the myriad of various state laws for those in compliance with national privacy and GLBA standards; and protection from frivolous lawsuits created by a private right of action. While the draft APRA addresses many of these areas, we believe it falls short of addressing credit unions' concerns and we cannot support it as currently drafted.

GLBA Exemption

We are concerned that the bill does not have an entity-level exemption for those in compliance with the GLBA, but instead creates a complex data-level GLBA exemption. While this would provide some exemption for credit unions from a number of the bill's provisions, it may not address certain new requirements that lack any comparable analogue in either the GLBA or the Fair Credit Reporting Act (FCRA), such as data portability provisions in Section 5 of the bill. The data-level exemption in the bill, unlike an entity-level exemption, will only apply to the extent the GLBA addresses uses of data that match equivalent activities regulated by the bill.

Some covered entities may achieve GLBA compliance under different rules promulgated by different regulators (i.e., the Federal Trade Commission versus banking regulators), and some credit unions may receive different treatment under the bill depending on whether they are federally- or state-chartered. Application of the APRA's enforcement language amplifies differences across charter types and could result in new burdens falling on state-chartered credit unions. We would urge changes to strengthen the GLBA exemption to an entity level to include all credit unions before moving forward.

Federal Preemption

The APRA would generally preempt state privacy and data security laws, but there is a long list of carveouts for existing state laws built into the legislation. America's Credit Unions has concerns with some of these exceptions. Some of the most problematic of these exceptions to preemption are state laws addressing unfair or unconscionable practices—a catchall that could be used to erode the entire purpose of a uniform federal standard through incremental expansions of state authority or amorphous legal interpretations.

Additionally, the exception for breach notification opens the door for inconsistent state cyber-incident reporting standards, which could be longer or shorter than what is currently required by the National Credit Union Administration (72 hours) and relevant federal law, such as the Cyber Incident Reporting for Critical Infrastructure Act. For the section of law regarding banking and financial records, many FCRA rights could rest within this domain. State laws that are not “inconsistent” with the FCRA—including state laws that are more protective of consumers than the FCRA—are not entirely preempted by the FCRA itself—and might not be preempted by this bill.

Furthermore, the carveout for state laws addressing banking records could also lead to inconsistencies across states in terms of how liability is allocated between data providers and third parties that avail themselves of the Consumer Financial Protection Bureau's proposed rules governing consumer data portability under Section 1033 of the Dodd-Frank Act.

We would urge removal and greater clarity on these exemptions before moving forward with this legislation.

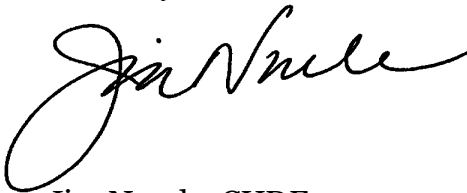
Private Right of Action

In general, the APRA establishes a broad private right of action covering most parts of the bill, including Section 9 which relates to data privacy to the extent a claim alleges a data breach arising from a violation of Section 9(a) (general data security practices), or a regulation promulgated thereunder. Individuals could be awarded actual damages, injunctive relief, declaratory relief, and reasonable attorney fees and litigation costs. While a covered entity would have the opportunity to cure actions or violations in response to a claim for injunctive relief with 30 days' notice, the notice requirement would be waved in cases involving substantial harm (which could be overly broad). We are concerned that this could still lead to frivolous legal action given the exceptions.

Finally, we would urge a stronger data security section be added to strengthen data security requirements for those handling personal financial data that are not already subject to GLBA provisions. As noted above, we firmly believe that there can be no data privacy until there is strong data security for individuals.

In conclusion, while we appreciate the efforts in the draft APRA to create a national privacy standard, we believe the bill still needs to be improved before advancing in the legislative process. On behalf of America's Credit Unions and the more than 142 million credit union members, thank you for the opportunity to share our views. We look forward to continuing to work with you to create an environment where credit union members can thrive.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim Nussle", with a large, stylized loop at the beginning.

Jim Nussle, CUDE
President & CEO

cc: Members of the Subcommittee on Innovation, Data, and Commerce



MORTGAGE BANKERS ASSOCIATION

May 23, 2024

The Honorable Gus Bilirakis
Chair
Subcommittee on Innovation, Data,
and Commerce
Committee on Energy and Commerce
U.S. House of Representatives
2306 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Innovation, Data,
and Commerce
Committee on Energy and Commerce
U.S. House of Representatives
2408 Rayburn House Office Building
Washington, D.C. 20515

Dear Chair Bilirakis and Ranking Member Schakowsky:

As you know, mortgage companies have been subject to extensive federal privacy and data protection laws and regulations for several decades. Thus, real estate finance firms believe protecting consumer financial data is a cornerstone of the trust their customers place in them.

Accordingly, the Mortgage Bankers Association (MBA)¹ appreciates this opportunity to comment on the most recent text of the *American Privacy Rights Act of 2024* ("APRA"). MBA has concerns with a number of provisions included in the bill (as currently proposed). Therefore, we respectfully urge your Subcommittee (and, in turn, the full Committee) to carefully consider these concerns as the APRA proceeds to an initial markup later this week.

Financial Institutions That Are Subject to The GLBA Should Be Exempt from APRA

The primary privacy protection law for consumer financial data is Title V of the *Gramm-Leach Bliley Act* (GLBA). With the GLBA, Congress constructed a privacy and data security regime to provide an effective and successful balance between providing a clear framework for financial institutions and ensuring that consumer financial transactions take place in a safe and secure environment. In particular, the GLBA regime has been carefully structured to ensure compliance with existing laws and regulations, adherence to the judicial process, and protection from fraud, illicit finance, and money laundering. Further, the GLBA grants federal financial regulators broad authority to adopt necessary regulations to enact these standards, allowing the regulatory regime to adapt over time as privacy concerns evolve. Notably, the GLBA requires that financial institutions provide consumers with notice of their privacy practices and generally prohibits such institutions from disclosing financial and other consumer information to third parties without first providing consumers with an opportunity to opt out of such sharing.

¹ The Mortgage Bankers Association (MBA) is the national association representing the real estate finance industry, an industry that employs more than 275,000 people in virtually every community in the country. Headquartered in Washington, D.C., the association works to ensure the continued strength of the nation's residential and commercial real estate markets, to expand homeownership, and to extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of more than 2,000 companies includes all elements of real estate finance: independent mortgage banks, mortgage brokers, commercial banks, thrifts, REITs, Wall Street conduits, life insurance companies, credit unions, and others in the mortgage lending field. For additional information, visit MBA's website: www.mba.org.

As currently drafted, the APRA does not include a full exemption for entities subject to the GLBA. Under section 120(b)(3) of the proposal, a covered entity is deemed to be in compliance with the APRA if it complies with the GLBA – but only with respect to the data subject to the GLBA. This “data-level exemption” does not offer sufficient coverage to truly opt MBA members out of coverage of laws with similar provisions. MBA has consistently advocated for an entity-level GLBA exemption.² This is the approach taken by most individual states with a data privacy law and would fully exempt covered mortgage companies.³ Additionally, an entity that would otherwise be exempt from the APRA under section 120(b)(3) is not exempt from Section 109, concerning data security requirements. MBA believes entities subject to the GLBA should be exempt from all of the APRA, including section 109. The Federal Trade Commission (FTC) recently updated their Safeguards Rule with modern and precise data security requirements for financial institutions.⁴ Thus, the APRA carve-out for Section 109 is unnecessary because the mortgage companies that would need to comply with Section 109 must also comply with the FTC Safeguards Rule.

APRA’s Private Right of Action Should Be Removed

Many data breaches are the result of criminals or nation-state actors improperly accessing a company’s database or misappropriating that company’s information. Consumers have expectations of privacy and protection that must be respected, but with an understanding that the company is also a victim of theft of their information and unlawful intrusion into their data systems. For this reason, a private right of action is inappropriate.

Section 119(a) of the APRA would create a private right of action with very few limitations. While a private right of action, in theory, will only implicate companies that do not follow the appropriate standards, it will likely be utilized by plaintiffs’ attorneys in any instance where there is a data breach. The simple fact that data was taken – and the implication that privacy protections were inadequate – is likely to be the core of a speculative complaint. Speculative litigation and the reputational costs of further litigation will further encourage class actions even for minor compliance infractions or following any breach.

As such, our members oppose provisions in the APRA that would authorize private rights of action and believe the GLBA’s existing regulatory enforcement structure for financial institutions should be preserved. These GLBA regulators have experience in evaluating privacy and data protection regimes, are in regular contact with regulated entities, and can best update their expectations to keep track of data security trends as threats evolve.

² Mortgage Bankers Association, Protecting Privacy and Helping Homeowners, available at https://www.mba.org/docs/default-source/uploadedfiles/state-relations/real-estate-finance-industry-data-protection-amendment-for-state-bills-final-1-15-20.pdf?sfvrsn=8913137a_0.

³ See CO ST § 6-1-1304(2)(j), FL ST § 501.703(2)(b), TX BUS & COM § 541.002(b)(2), VA ST § 59.1-576(B).

⁴ Federal Trade Commission, FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches (Oct. 27, 2021), available at <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data>, see also 16 C.F.R. Part 314.

Congress Should Address Additional Key Concerns

MBA would also note our industry's concerns with other provisions of the APRA, as follows:

- Insufficient Preemption of State Law: The growing patchwork of state privacy laws must be replaced by a federal standard. It is critical that any new federal privacy law preempt existing state laws to avoid duplicative and conflicting requirements that will disrupt financial transactions. A federal standard will also help provide the transparency needed for consumers to understand their rights and responsibilities. More importantly, having a federal standard will ensure that consumers receive the same privacy rights and data protections regardless of where they may live.

Although the APRA would preempt many state privacy laws, it also provides numerous exceptions that undermine the preemption. Under Section 120(a)(3), the APRA does not preempt provisions of state law concerning, amongst other topics, social security numbers and financial records. Many state data privacy laws control how regulated companies protect social security numbers and financial records as nonpublic personal information, the provisions of which would remain in force under the APRA. The APRA should be amended to create a clear and direct preemption of all state privacy and data protection provisions to clarify the duplicative and conflicting patchwork of requirements imposed on our members.

- Clarify Consumer-Requested "Opt-Out" Requirements for Lenders: Under Section 114(a) of the APRA, an individual can request to opt-out of evaluation by an algorithm for "consequential decisions", including housing and credit opportunities. Algorithms are defined broadly to include, "a computational process [that] facilitates human decision-making by using covered data, which included determining the provision of a product or service." This incredibly broad definition includes many mundane and pre-existing uses of algorithms, such as using a calculator to determine a borrower's total earnings. A lender would be required to offer an opportunity to the borrower to opt-out of this process each time these "algorithms" are used.

This requirement is additionally burdensome in the context of mortgage lending. Lenders do not create the automated underwriting systems (AUSs) that they rely on to have a loan guaranteed or securitized. These systems are developed by the federal mortgage insurer (the Federal Housing Administration (FHA)) or the Government Sponsored Enterprises (the GSEs – Fannie Mae and Freddie Mac). For example, Desktop Underwriter (DU) and Loan Prospector (LP) are developed and controlled by the GSEs, while the Department of Housing and Urban Development (HUD) has its own AUS for FHA loan products.

Under Section 114(a), a consumer can opt-out of credit evaluations by an algorithm such as DU/LP. However, allowing consumers to opt-out will result in the imposition of additional costs. Most lenders routinely rely on these automated systems to help them make sound lending decisions. Lenders could underwrite loans manually, but this would be a costly process and those loans may not be accepted by the GSEs or agencies. Although a lender could deny this request, Section 108(b)(3) only allows lenders to decline to provide a product or service if using the algorithms is strictly necessary to provide it

(highly unclear under this scenario). MBA believes Congress should consider enacting a clearer and less restrictive process to allow a lender to decline to provide a product if a borrower opts-out of the use of such automated underwriting systems.


Conclusion

MBA and its members support legislation to create a national privacy standard that recognizes the strong privacy and data security standards already in place for financial institutions under the GLBA and other financial privacy laws. MBA encourages Congress to avoid provisions that run counter to this well-understood framework or create a private right of action.

Consequently, MBA strongly urges the Subcommittee (and, in turn, the full Committee) to amend the APRA, as suggested, to appropriately balance the objectives of protecting consumer data privacy, preserving sound mortgage underwriting practices, and maintaining housing affordability.

Thank you in advance for your consideration of the views expressed within this letter.

Sincerely,



Bill Killmer
Senior Vice President
Legislative and Political Affairs

cc: The Honorable Cathy McMorris Rodgers, Chair, House Committee on Energy and Commerce

The Honorable Frank Pallone, Ranking Member, House Committee on Energy and Commerce

All Members, House Committee on Energy & Commerce

May 22, 2024

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

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

Dear Chairman Bilirakis and Ranking Member Schakowsky:

The undersigned business associations oppose the American Privacy Rights Act (“APRA”) as drafted, which your Subcommittee is expected to consider in the near future. This legislation would have devastating consequences for the American economy and U.S. technological leadership.

APRA would subject businesses, innovators, and entrepreneurs to more than ten new private causes of action. Similar private rights of action laws have driven away legitimate business in states that have implemented this ill-conceived remedy. APRA would empower plaintiffs’ attorneys to engage in sue-and-settle tactics against small businesses, startups, and charities. Companies acting in good faith and not engaging in willfully harmful activity will be forced to agree to pay expensive settlements or risk costly litigation. APRA would also gut arbitration agreements and enable activists to weaponize private rights of action against non-profit organizations with whom they may disagree politically.

In addition, APRA would fail to establish a single, national privacy standard which is necessary to ensure certainty for both businesses and consumers. The APRA’s approach could cost the American economy as much as \$1 trillion, with \$200 billion being incurred by small businesses alone.

APRA would empower the trial bar to engage in litigation that could hinder the digital advertising ecosystem that has enabled people to do online research, get their news, and learn about educational and job opportunities without having to pay out of pocket. The ad-driven internet has enabled diverse viewpoints and products to enter the marketplace with low cost of entry. APRA would also dramatically limit, and in some cases ban, the most effective forms of general advertising which drive competition, growth, and consumer satisfaction in today’s economy. APRA would provide the Federal Trade Commission sweeping new authorities to restrict data for advertising. Such aggressive federal action would harm the online economic framework that has benefited consumers and businesses.

Universal “Do Not Collect” obligations would also endanger many societally beneficial uses of data like anti-fraud and security initiatives.

The bill would also empower plaintiffs’ attorneys in ways that could end loyalty programs that consumers enjoy, including hotel, travel, restaurant, and retail benefits. Under the APRA’s onerous requirements, trial lawyers could sue every time a business shares data with its partners for alleged non-compliance with its novel data transfer rules that are unique to the APRA and do not exist in any state privacy law.

Ultimately, APRA would disadvantage U.S. technological leadership. For example, the proposal would require AI developers to undergo impact assessments that may be impossible to complete because of APRA’s data minimization and opt-in requirements. Since APRA would only permit data to be used for what is necessary for a service and sensitive data is subject to opt-in, companies may not have the full

data to assure their AI systems are not disparately impacting communities. The bill's overly broad definition and regulation of "covered algorithms" would help enrich the trial bar and place online delivery, automated hotel check-in, and emerging AI technology in jeopardy because of the threat of plaintiffs' attorneys suing legitimate businesses for having only an automated feature on their apps. The definition of "covered algorithm" would also capture and fundamentally change regulation for long-standing statistical models that many in the financial services sector have been using for decades. These restrictions could have a significant chilling effect on AI development and use.

We urge you to ensure APRA is not reported as drafted.

Sincerely,

American Hotel & Lodging Association
American Property Casualty Insurance Association
Association of National Advertisers
Consumer Data Industry Association
Direct Selling Association
FMI-Food Industry Association
Interactive Advertising Bureau
International Franchise Association
National Association of Mutual Insurance Companies
National Restaurant Association
National Retail Federation
Small Business & Entrepreneurship Council
U.S. Chamber of Commerce

cc: Members of the House Committee on Energy and Commerce

May 21, 2024

To the Members of the United States Congress:

We write today to share our strong concerns with the American Privacy Rights Act (APRA). As currently drafted, the APRA would fail to establish a meaningful uniform national data protection standard and undermines the harmonized data privacy legislation our 15 states — covering 100 million Americans — enacted.

For many years, the undersigned organizations have advocated for Congress to create a national privacy standard that preempts state laws and establishes a consistent enforcement regime to provide consumers and businesses certainty. However, the lack of federal legislation has forced many states to act. Our states have enacted data privacy laws that provide consistent protections and the same enforcement mechanisms. Laws in our states entrust state attorneys general with enforcement and bar private lawsuits that could be used to harm small business and prevent new innovation. Other states, such as California, take a different approach by allowing a private right of action that sets up a litigation-heavy enforcement environment.

The APRA would create the worst of all worlds by failing to create a single, national privacy standard and giving a preference for the California approach of trial bar enforcement.

APRA would not provide full preemption. The draft bill would allow states to regulate on top of federal requirements. Rather than eliminating differences in how data privacy is regulated from state to state, APRA would compound them and create new confusion, duplication, and uncertainty.

The APRA private right of action provisions would allow for an explosion of frivolous litigation by empowering the trial bar to sue small businesses, charities, and other actors who could be forced to settle because they lack the time, expertise, and financial resources to fight back. Additionally, the bill would effectively block arbitration agreements, depriving consumers of the means of timely dispute resolution and remedies. These potential outcomes are the very reason why our states rejected private rights of actions embraced by California and certain other states.

As noted by the U.S. Chamber of Commerce,¹ the approach of APRA would ultimately threaten programs and services consumers value and enjoy, like loyalty programs at restaurants, retail stores, supermarkets, and hotels, online delivery and

¹ <https://www.uschamber.com/assets/documents/USChamber-APRA-Letter.pdf>

transportation services, and advertising and marketing tools small businesses and startups can use to compete with larger, more established companies.

We believe Congress should draw on the experience of our 15 states where there are well-crafted privacy laws that cover 100 million Americans. In its current form, the APRA is the wrong approach. We stand ready to work with Congress on a better path forward.

Sincerely,

U.S. Chamber of Commerce

Colorado

Colorado Chamber of Commerce
Adams County Regional Economic Partnership
Greater Woodland Park Chamber of Commerce
Vail Valley Partnership

Connecticut

Connecticut Business & Industry Association

Delaware

Central Delaware Chamber of Commerce

Florida

AMPLIFY Clearwater
Southeast Volusia Chamber of Commerce
Tampa Bay Chamber
The Greater Zephyrhills Chamber of Commerce
West Orange Chamber of Commerce

Indiana

Indiana Chamber of Commerce
Decatur Indiana Chamber of Commerce
South Bend Regional Chamber

Iowa

Iowa Association of Business & Industry
Shelby County Chamber of Commerce & Industry

Kentucky

Kentucky Chamber of Commerce
Northern Kentucky Chamber of Commerce
Union County KY Chamber of Commerce

Montana

Montana Chamber of Commerce

Nebraska

Nebraska Chamber of Commerce & Industry
Grand Island Area Chamber of Commerce
North Platte Area Chamber and Development Corp.
Seward County Chamber & Development Partnership

New Hampshire

Business and Industry Association of New Hampshire

Oregon

Oregon Business & Industry
Boardman Chamber of Commerce
Roseburg Area Chamber of Commerce
The Dalles Area Chamber of Commerce

Tennessee

Tennessee Chamber of Commerce
Chattanooga Chamber of Commerce
The Germantown Chamber of Commerce

Texas

Texas Association of Business
Fort Bend Chamber
Fulshear Katy Area Chamber of Commerce
Giddings Area Chamber of Commerce
Greater Houston Partnership
Houston Northwest Chamber of Commerce
Kilgore Area Chamber of Commerce
Metrocrest Chamber of Commerce
North Texas Commission
Plano Chamber of Commerce

Washington County Chamber of Commerce

Utah

South Valley Chamber

The Salt Lake Chamber

Utah Valley Chamber of Commerce

Virginia

Virginia Chamber of Commerce

Loudon County Chamber of Commerce

Prince William Chamber of Commerce

The Honorable Cathy McMorris Rodgers
Chairwoman
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
House Committee on Energy & Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Gus Bilirakis
Chairman
Subcommittee on Innovation, Data, & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Innovation, Data, &
Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

May 23, 2024

Dear Chairwoman McMorris Rodgers, Ranking Member Pallone, Chairman Bilirakis, and Ranking Member Schakowsky:

The American Property Casualty Insurance Association (APCIA) has serious substantive concerns with the current draft of the American Privacy Rights Act of 2024 (APRA). The legislation would create conflicts with the existing unique privacy regime established for the insurance industry under the Gramm-Leach-Bliley Act (GLBA) and state insurance privacy laws.

As articulated in our previous letter, the Gramm-Leach-Bliley Act established a regulatory framework for protecting the privacy of nonpublic information used by financial services institutions, which for insurance is governed and enforced by state insurance regulators. The state regulators – through the National Association of Insurance Commissioners (NAIC) – have further developed and uniquely evolved comprehensive privacy protections through development of numerous additional model laws and regulations including the Insurance Data Security Model Law, the NAIC Insurance Information and Privacy Protection Model Act, the Privacy of Consumer Financial and Health Information Regulation, and the Standards for Safeguarding Customer Information Model Regulation. The NAIC just last year adopted the Model Bulletin on the Use of Artificial Intelligence Systems by Insurers that the states are rapidly enacting and the NAIC is currently finalizing an updated Privacy Protections Model Act.

The GLBA privacy regime and each of these model laws and the related adopted state laws and regulations provide for extensive privacy regulation of insurance entities by the state insurance departments, who have developed an extensive case history of allowable and prohibited practices reviewed regularly through state insurance market conduct examinations. The state insurance departments have determined over time what data sharing is necessary for the business of insurance and what additional consumer protections are necessary beyond the unusually extensive state oversight. For insurance specifically, Congress in the McCarran-Ferguson Act delegated insurance regulation to the states, which has been further underscored in subsequent legislation such as GLBA and the Dodd-Frank Act.

The American Privacy Rights Act of 2024 (APRA) creates a new privacy regime for covered entities that are subject to the Federal Trade Commission Act (FTCA), but that is not limited to the activities for which entities are subject to the FTCA. Insurers specifically and uniquely are currently subject to the FTCA for very limited and specific purposes, but not generally. For example, section 6 of the Federal Trade Commission Act provides that the Act shall not apply to the business of insurance except very specific provisions, such as that “the Commission shall have authority to conduct studies and prepare reports relating to the business of insurance” upon the request of certain Congressional committees. Failure to clarify that APRA does not apply to insurance could create a broad and unintended loophole under which the Federal Trade Commission could attempt to assert extensive new jurisdiction over insurance in contravention of the McCarran-Ferguson Act. The provisions would then create significant conflict with the requirements and enforcement of state privacy and AI regulation – much of which is directed by the GLBA privacy regime, particularly since the APRA specifically lists insurance in the impact assessment scope and definition of “consequential decision”. APCIA would welcome an opportunity to discuss this further with the Committee to ensure that APRA does not inadvertently unwind portions of the McCarran-Ferguson Act by creating new Federal Trade Commission authority over insurance or impede the GLBA-mandated privacy regime.

Importantly, APCIA maintains our concerns that APRA would expose our policyholders to greater legal risks and higher costs by unnecessarily expanding on the already existing and well-established tort system that is currently in place. Section 19 establishes an unnecessary private right of action that may be brought by individuals against an entity for an alleged violation of this new law. The APRA’s private right of action goes well beyond current privacy frameworks in the United States, whether the GLBA or nearly all state privacy statutes, which do not permit private actions. Indeed, the APRA’s private right of action even surpasses the private right of action in California Consumer Privacy Act and the California Privacy Rights Act, which only permits private actions for breaches of data security requirements. The insurance industry is concerned that parts of the United States already suffer from being overly litigious, and this provision threatens to exacerbate the problem creating financial pressures on the customers we serve

APCIA appreciates that the Committee has repeatedly solicited feedback and was pleased to provide two redlines on May 1st following the release of the original discussion draft. However, we remain concerned that the new draft of the bill does not include changes to the problematic GLBA exemption and a private right of action. Because of this, APCIA urges the Committee to continue to work with stakeholders on changes to this legislation before moving forward with it. APCIA strongly opposes the legislation in its current form.

Sincerely,



Nat Wienecke



May 22, 2024

The Honorable Cathy McMorris Rodgers, Chair

House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Attn: Innovation, Data, and Commerce Subcommittee

The Honorable Gus Bilirakis, Chair

Re: The American Privacy Rights Act

Dear Chairperson McMorris Rodgers and Congressman Bilirakis,

As advocates who helped spur the passage of California's first-in-the-nation privacy law, the California Privacy Rights Act (CPRA), Consumer Watchdog urges you to preserve the progress states have made by passing legislation that sets a floor and not a ceiling on data privacy rights.

Nearly 10 million Californians voted for strong data privacy rights when they passed CPRA. CPRA is unique because it gives Californians a baseline of rights that can be improved upon over time, but cannot be eroded by legislators.

However, because of preemption language, the American Privacy Rights Act (APRA) will wipe away years of progress made in California and in nearly 20 states that have passed similar laws across the country.

APRA would also virtually eliminate the authority of the California Privacy Protection Agency (CPPA), which has been building up its privacy enforcement division over the past three years. It will be replaced with the Federal Trade Commission (FTC), which is in the middle of many important antitrust battles and does not gain additional funding under APRA. Per the bill, the FTC will have two years from when the law is enacted to draft regulations. That's a lot of time for people's data to change hands and for rogue algorithms to do damage. Technological innovation moves fast. But Californians have protections right now.

APRA would put a lid on progress, likely never to be opened again. While APRA would give Americans rights surrounding how companies use, share or sell their data, it takes away:

- Opt out rights in effect right now. The ability to limit the use of sensitive personal information, to opt out of the sharing and selling of your personal information for targeted advertising, to know how personal information is used by businesses, and the ability to correct or delete it are all protections Californians would lose for years were this bill approved.
- Protections for sensitive information, such as sexual orientation, union membership, and immigration status. APRA does not include those categories in the definition of sensitive covered data.
- Protections against profiling.
- Protections against targeted advertising. Under APRA, service providers will still be able to combine data to execute targeted advertising.
- Protections against companies that collect or share data with a local or federal agency. Service providers are exempt under APRA.
- Progress made surrounding artificial intelligence and automated decision making technology. The CA privacy agency is currently drafting landmark rules surrounding a right to opt-out of the use of personal information with respect to training automated decisions.
- A stronger private right of action for data breaches. APRA would move all cases to federal court, where it is harder for consumers to seek remedies.

To be clear, Consumer Watchdog supports privacy rights for Americans, but they shouldn't come at the expense of the rights that millions already enjoy. Wiping away years of progress is not what Californians voted for when they passed the California Privacy Rights Act.

Sincerely,



Justin Kloczko
Privacy Advocate
Consumer Watchdog

The Honorable Gus Bilirakis
Chair
House Energy and Commerce Innovation, Data, and Commerce Subcommittee
2125 Rayburn Office Building Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
House Energy and Commerce Innovation, Data, and Commerce Subcommittee
2125 Rayburn Office Building Washington, DC 20515

The Honorable Tim Walberg
Vice Chair
House Energy and Commerce Innovation, Data, and Commerce Subcommittee
2125 Rayburn Office Building Washington, DC 20515

Re: ATA Action Feedback on American Privacy Rights Act (APRA)

Dear Chair Bilirakis, Ranking Member Schakowsky, and Vice Chair Walberg,

We are writing on behalf of the American Telemedicine Association (ATA), the only organization focused solely on advancing telehealth, and ATA Action, the ATA's advocacy arm, to provide our feedback on the American Privacy Rights Act (APRA).

Thank you for the Energy and Commerce Committee's consistent bipartisan support for patient access to telehealth. Your efforts have significantly advanced our collective mission to deliver high-quality care to Americans regardless of their location.

We are particularly grateful for your work in drafting the American Privacy Rights Act aimed at establishing national consumer data privacy rights and setting standards for data security. We fully endorse the need for a consistent national approach to privacy, as reflected in the ATA's Health Data Privacy Principles. Such a national framework is essential to mitigate the complexity and financial burdens faced by organizations, especially our smaller members with fewer resources, in delivering clinically appropriate telehealth services across state lines.

However, we have some significant concerns with the current draft of the legislation, also reflected in our privacy principles. As it stands, it does not pre-empt many existing state laws in this area, which may result in additional layers of compliance rather than removing barriers. This could hinder rather than help organizations striving to provide high-quality telehealth care.

First, in order to derive the benefits of a national data use and information privacy framework, such as reduced compliance costs and legal clarity, we believe that the Act should clearly preempt the patchwork of state data privacy laws recently enacted across the nation which seek to regulate the same sets of covered health data. We recommend changing Section 20(a)(3)(N) to read as follows:

(N) Provisions of laws that protect the privacy of health information, healthcare information, medical information in the possession of a provider of healthcare or health care service plan, medical records, HIV status, or HIV testing.

This change would preempt state laws that cover health data use and privacy, while preserving state laws that deal with actual medical records covering patient health conditions. For example, state laws that protect medical records created by doctors interacting with patients would not be preempted, but state laws that regulate how health data is collected by a phone application or an over-the-counter purchase of aspirin would be preempted and solely governed by federal law.

Second, Section 3 data minimization requirements may create conflicting and overly burdensome obligations for processors of health information. For example, the permitted purposes exceptions for marketing and advertising exclude sensitive covered data (including health data) and therefore appear to significantly limit these uses for health entities even when a consumer has consented or chosen not to opt out. It is also unclear if this draft language would allow for the use of health data in developing innovative internal tools, such as artificial intelligence used in consumer interactions and business operations. The value-added benefit of these restrictions is also unclear, as covered entities are already in possession of this data and the consumer has previously consented to collection.

Finally, we are particularly concerned about the enforcement regime predicated on a private right of action. We believe this will impose undue burdens on organizations by opening the door to potential frivolous lawsuits, which could divert valuable resources away from patient care.

We strongly hope that the committee will reconsider these provisions as the bill advances. Please know that the ATA and ATA Action are available as resources as you continue to refine this important legislation. We believe that with thoughtful adjustments, this bill can better support access to telehealth while ensuring robust consumer data privacy.

Thank you for your continued dedication and hard work.

Kind regards,

A handwritten signature in black ink, appearing to read "Kyle Zebley".

Kyle Zebley
Executive Director
ATA Action



Promoting Innovation Worldwide

May 22, 2024

The Honorable Cathy McMorris Rodgers
Chairwoman
House Committee on Energy & Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
House Committee on Energy & Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Gus Bilirakis
Chairman
House Committee on Energy & Commerce
Subcommittee on Innovation, Data & Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Janice Schakowsky
Ranking Member
House Committee on Energy & Commerce
Subcommittee on Innovation, Data & Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairwoman McMorris Rodgers, Ranking Member Pallone, Chairman Bilirakis and Ranking Member Schakowsky:

As a longtime advocate for a comprehensive federal privacy standard, ITI appreciates the subcommittee's consideration of the American Privacy Rights Act (APRA). We write today to share concerns on behalf of the technology industry that we hope can be addressed as the bill moves forward.

Comprehensive federal privacy legislation is critical to strengthening consumer trust and reasserting U.S. leadership on data policy. The debate since the release of APRA has largely focused on two provisions that have long stymied progress on comprehensive privacy legislation: the scope of preemption of state privacy laws and the inclusion of a private right of action (PRA). ITI shares concerns raised about both issues, but it is imperative that Congress also address other key provisions in APRA, including sections on data minimization and algorithmic accountability which, as drafted, would undermine the competitiveness of U.S. companies.

These critical sections of the bill would restrict U.S. industry from using data to run their businesses in ways that their global peers are free to do, deprive U.S. consumers from freely exercising their choice to use data-driven services, and threaten continued U.S. leadership in artificial intelligence.

Data Minimization

Historically, data collection and processing in the U.S. has been generally permitted, unless prohibited by a specific rule covering certain industries or types of data. Over the last five years, policymakers in the U.S. have sought heightened levels of privacy protection, while preserving a clear legal basis for legitimate uses of data that underpin billions of dollars in economic activity and products and services consumers enjoy today.

Unfortunately, APRA's data minimization provisions take the opposite approach, generally prohibiting *all* data collection and processing other than "to provide or maintain a specific product or service requested by the individual" or for one of the "permitted purposes" articulated in section 3(d) of the bill. This approach creates a flawed scheme that takes away a consumers' right to consent to the use of their own data and fails to recognize the importance and validity of data processing grounded in the legitimate interests of U.S. businesses.

For example, APRA does not fully recognize the legitimate interest of companies to process personal data to carry out core tasks related to their business activities such as developing products or services, or to conduct research or analysis for a wide array of purposes including both scientific and commercial purposes, even where personal data is protected by reasonable technical, physical and administrative safeguards. Further, APRA precludes almost any third-party processing of data. By contrast, the EU's GDPR and prominent state level privacy laws in the United States take a more flexible approach than APRA. APRA should include additional permitted purposes in section 3(d) that allow US businesses to process data for legitimate business purposes while still protecting individual privacy interests.

Consent has traditionally been an important mechanism for data protection, as it recognizes the right of individuals to control their personal data and empowers consumers to make informed decisions about whether and how their data can be used. While APRA does allow processing for a "product or service they [consumers] requested," the bill should expressly include consent as a permitted use in section 3(d), maintaining US consumers' right to consent or opt-in to the processing of their data for the internet services they enjoy.

Algorithms

Beyond its core data privacy provisions, APRA also creates a new regulatory regime for algorithms. While the purpose of this section – to protect against the collection or processing of data in a discriminatory manner – is laudable, its overbroad scope and imprecise language, prescriptive focus on algorithms, and incongruity with APRA's other provisions as well as emerging AI law and policy in the U.S. and globally is highly problematic.

The vagueness of these provisions coupled with the ubiquity of algorithms in modern computing technology means that APRA would require companies to conduct impact assessments and design evaluations on a vast number of algorithms, while not providing any such assessment or evaluation of other integral components of AI systems, such as datasets, which could themselves contain discriminatory biases. Even more concerning, the restrictive data minimization provisions would likely preclude companies from collecting the data they would need to comply with the bill's algorithmic provisions. ITI has long advocated for the importance of taking a holistic, system-level approach to managing AI risk that is sensitive to the deployment context of AI systems.

Compounding these challenges, APRA's approach to regulating algorithms fails to take account of significant AI policy developments including the Biden Administration's AI Executive Order, which is currently being implemented by various federal agencies, the European Union's new comprehensive AI regulation, and multilateral efforts advanced at the G7 and AI Safety Summit convened in Seoul this week, increasing the risk of AI policy fragmentation.

ITI shares the goal of the subcommittee in advancing comprehensive federal privacy legislation that protects American consumers as well as the ability of U.S. companies to continue to lead the world in data and AI innovation. We stand ready to work with Congress and other stakeholders to realize this mutual goal, which must be grounded in getting the pillars of privacy policy right.

Sincerely,

John Miller
General Counsel and Senior Vice President of Policy





May 23, 2024

The Honorable Gus Bilirakis
Chairman
Subcommittee on Innovation,
Data, and Commerce
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

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

Re: May 23, 2024, Subcommittee on Innovation, Data, and Commerce Markup of Privacy Legislation Including the Discussion Draft of the American Privacy Rights Act (APRA)

Dear Chairman Bilirakis and Ranking Member Schakowsky:

The primary privacy and data security consumer protection law for financial institutions is Title V of the Gramm-Leach Bliley Act (GLBA). We support legislation to put in place a national privacy standard, but that standard must recognize the strong privacy and data security standards that are already in place for the financial sector under the GLBA and other financial privacy laws (e.g., the Fair Credit Reporting Act and Right to Financial Privacy Act) and avoid provisions that duplicate or are inconsistent with those laws.

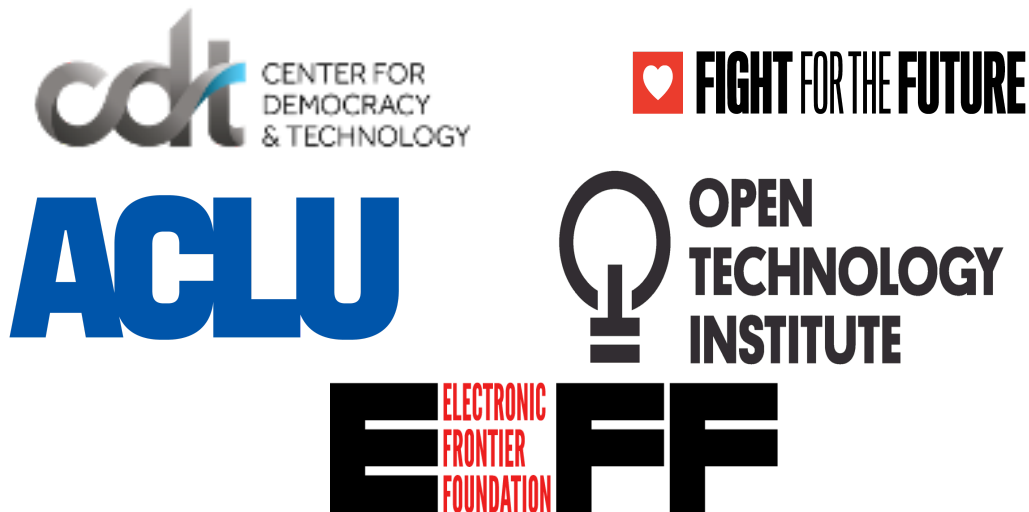
As currently framed, Title I of the American Privacy Rights Act of 2024 (APRA) does not include clear language for financial institutions to understand their exemption from the requirements of the bill. Section 120(b)(3) only excludes data subject to the GLBA, as opposed to exempting financial institutions subject to the GLBA.

This will lead to duplicative and conflicting requirements for financial institutions already subject to oversight by GLBA regulation. As currently drafted, the bill would be disruptive to the financial system, consumers, and the economy. We urge that Title I of the APRA be amended to exempt all financial institutions subject to the GLBA to avoid such disruption.

Sincerely,

American Bankers Association
America's Credit Unions
Bank Policy Institute
Consumer Bankers Association
Independent Community Bankers of America
Mortgage Bankers Association
Securities Industry and Financial Markets Association

Cc: Chairman McMorris-Rodgers, Ranking Member Pallone, Members of the Committee



May 23, 2024

Dear Chairs McMorris Rodgers, Pallone, Latta, Weber, and Ranking Member Matsui and Members of the House Subcommittee on Communications & Technology,

In advance of the markup in the House Innovation, Data, and Commerce Subcommittee tomorrow, we, the undersigned civil society organizations, write to express our concerns with the Kids Online Safety Act (KOSA), H.R. 7891, as currently drafted. We share the goal of keeping kids safe online, and appreciate that there have been positive changes made to the legislation to reduce many concerns raised by civil society, LGBTQ communities, and grassroots advocates. We urge you to continue that process of engagement and to continue making additional changes to the bill to mitigate still extant concerns that it will censor valuable speech and undermine the privacy rights of everyone online as you prepare for a full committee markup.

We continue to have concerns that this bill will be misused to target marginalized communities and politically divisive information, concerns that have not been fully addressed in H.R. 7891, as introduced. Even with key changes to the duty of care to limit its application to “high impact online companies,” KOSA still requires services that users depend on to restrict their services from recommending content that meets the government’s view of what will harm youth mental health. As a result, companies looking to reduce their legal risk will remain incentivized not to recommend content on young people’s feeds that they fear legislators and enforcers could claim relates to negative mental health outcomes, including content related to sexual health and reproductive care, racial justice, LGBTQ+ issues, and other politically divisive content, even though such content can be critically important to many young people and their safety and security.

We also worry that some provisions are worded in such a way that they would permit parents to broadly surveil their kids online, especially since parents and their kids do not always have

supportive relationships. As currently drafted, parents have the right to “manage” settings for both teens and children in the preambulatory text in Sec. 103(b)(2)(A), and then rights to “view” (for teens) or “change” (for children) settings in clauses (i) and (ii). It is not clear, however, if the right to “manage” in the preambulatory text gives parents of teenagers additional controls. Amendments are necessary to clarify that it does not.

While we have outstanding concerns with KOSA, we have been encouraged by lawmakers’ continued engagement on the legislation. Additional amendments to the bill can ensure parents have access to tools to protect their children’s privacy, but do not have broader abilities to surveil or control the content that particularly their teen kids view, are also needed. Other changes might be made to further improve the duty of care and safeguard it against the potential for misuse and constitutional challenges. Those might include edits that would raise the *mens rea* requirement for design features that recommend content related to mental health harms. Alternatively, they could include a bounded definition of “design feature” that does not include the recommendation of particular content, such as vague categories of content potentially related to emotional harms, but instead focuses on content neutral features of the services. There might be many ways to approach this issue. We recommend, welcome, and encourage that conversation.

The Kids Online Safety Act, as currently drafted, continues to raise free expression and privacy concerns. However, changes are possible to improve the bill and reduce these concerns while keeping kids safe online. We urge you to continue improving the legislation before bringing the bill to the floor.

Sincerely,

Americans Civil Liberties Union
Center for Democracy & Technology
Electronic Frontier Foundation
Fight for the Future
New America’s Open Technology Institute

May 23, 2024

Members of the House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Esteemed Members of this Committee:

We the undersigned are a group of individuals and organizations dedicated to protecting kids online and ensuring that tech is accountable for the harm they cause to our most vulnerable population—children. It is why we support the bipartisan Kids Online Safety Act (“KOSA”) as it will provide the necessary tools to address raising children in the digital age.

First, we would like to thank you for including KOSA in this important markup. As the committee is aware, social media companies are a threat to our children. A bipartisan Congress is now stepping up to make Big Tech products safe for our kids; but the social media companies are putting their incredible lobbying power behind efforts to break KOSA’s momentum.

Congress should not listen, because the stakes are just too high.

U.S. Surgeon General Vivek Murthy’s May 2023 advisory warning found “ample” evidence that social media use presents “a profound risk of harm to the mental health and well-being of children and adolescents.”¹ And a recent paper by the Institute for Family Studies and Gallup shows that access to social media has led to higher suicide rates for teenagers.² “Teens who spend more than 5 hours a day on social media,” the report found, “were 2.5 times more likely to express suicidal thoughts or harm themselves, 2.4 times more likely to hold a negative view of their body, and 40% more likely to report a lot of sadness the day before.”

At its core, the issue is that these companies are fully aware of the pernicious impact of their products on children and teens, yet they continue to redouble their efforts to ensnare the next generation. This takes the form of Meta’s creation of a team to study and create products for preteens,³ Twitter hiring online influencers to recruit young people,⁴ and TikTok targeting

¹ The U.S. Surgeon General Advisory, *Social Media and Youth Mental Health* (2023), <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf>.

² Jonathan Rothwell, *How Parenting and Self-Control Mediate the Link Between Social Media Use and Mental Health*, Institute for Family Studies and Gallup (2023), <https://ifstudies.org/ifs-admin/resources/briefs/ifs-gallup-parentingsocialmediascreentime-october2023-1.pdf>.

³ Georgia Wells & Jeff Horwitz, *Facebook’s Efforts to Attract Preteens Goes Beyond Instagram Kids, Documents Show*, Wall Street Journal (Sep. 28, 2021), <https://www.wsj.com/articles/facebook-instagram-kids-tweens-attract-11632849667>.

⁴ Taylor Lorenz, *Twitter is Looking for Younger Users. It’s Turning to the Tech World’s Teen Savant to Help Find Them*, Washington Post (Mar. 8, 2022), <https://www.washingtonpost.com/technology/2022/03/08/twitter-teenagers-michael-sayman/>.

teens with addictive content.⁵ These willful predations in the face of mounting evidence of these companies' destructive effects should push lawmakers to take action.⁶

KOSA would directly address those issues and hold Big Tech accountable. These companies oppose KOSA because it will force them to empower parents to protect their children and limit their influence and monetization of minors.

It also would allow the Federal Trade Commission and state attorney generals to go after tech platforms that fail to provide parents with options to protect their child's information, disable addictive product features, and opt out of algorithmic recommendations. It also creates a "duty of care" for social media platforms to prevent and mitigate harms to minors, such as content that promotes self-harm, suicide, eating disorders, substance abuse, and sexual exploitation.

We understand that privacy, irrespective of age, is a fundamental issue that needs to be addressed. We all support comprehensive privacy solutions and are supportive of the efforts this committee has made to get us closer in achieving that goal. But child safety and privacy must be handled distinctly with child safety taking priority.

The lives of so many children are on the line. Congress cannot wait.

We have a fully vetted and targeted solution, KOSA, that is ready to be delivered to the President's desk and become law. The time for talk is over. The time for action to protect our children is now. No other agenda should slow or deter that and the undersigned demand action now before moving into positive consideration of any comprehensive privacy proposal.

In sum, we ask that Congress not let perfect be the enemy of the good. Yes, we all would love to see comprehensive privacy move through the legislature and become law, but not at the cost of slowing down bills that can have an immediate impact on protecting children.

It is why we ask that KOSA be passed expeditiously and independent of other privacy legislation because it will move us one step closer to protecting our kids from Big Tech.

Sincerely,

Joel Thayer
President
Digital Progress Institute

Jon Schweppe
Policy Director
Americans Principles Project

⁵ Wall Street Journal, *Investigation: How TikTok's Algorithm Figures Out Our Deepest Desires*, (Jul. 21, 2021), https://www.wsj.com/video/series/inside-tiktoks-highly-secretive-algorithm/investigation-how-tiktok-algorithm-figures-out-your-deepest-desires/6C0C2040-FF25-4827-8528-2BD6612E3796?mod=article_inline.

⁶ Matt Richtel, Cathrine Pearson, & Michael Levenson, *Surgeon General Warns that Social Media May Harm Children and Adolescents*, Washington Post (May 23, 2023), <https://www.nytimes.com/2023/05/23/health/surgeon-general-social-media-mental-health.html>.

Tim Estes
CEO & Founder
Angel AI

Dawn Hawkins,
CEO
**National Center on Sexual Exploitation
(NCOSE)**

Chris McKenna
Founder, CEO
Protect Young Eyes

Allison Ivie
Government Relations Representative
**The Eating Disorders Coalition for Research,
Policy, & Action**

Clare Morell
Senior Policy Analyst
**The Ethics and Public Policy Center
(Individual Capacity)**

Alix Fraser
Director of the Council for Responsible Social
Media
Issue One

Josh Golin
Executive Director
Fairplay

Maurine Molak
Parents for Safe Online Spaces

Michael Toscano
Executive Director
The Institute for Family Studies

Patrice Willoughby
Senior Vice President Global Policy and Impact
NAACP



May 22, 2024

Representative Frank Pallone, Ranking Member
House Committee on Energy and Commerce
2322A Rayburn House Office Building
Washington, DC 20515

LETTER: THE KIDS ONLINE SAFETY ACT (KOSA // H.R. 7891)

Dear Representative Pallone:

LGBT Tech is one of the nation's premier organizations working to bridge the technology gap for LGBTQ+ individuals through partnerships with non-profit groups, policy makers, scholars, industry, and innovators. Alongside policy work, LGBT Tech's programmatic branch distributes technology, grants, and education across the country. As an organization committed to the digital rights and well-being of the LGBTQ+ community, including more than 5.7 million LGBTQ+ youth, we write to **respectfully express our concerns with the content and potential impact of H.R.7891, the Kids Online Safety Act (KOSA).**

While we recognize the importance of safeguarding youth and respect this legislature's intention, we believe that this legislation poses significant risks to constitutionally protected content access and the overall inclusivity of platforms for marginalized users, particularly those within the LGBTQ+ community.

THE LGBTQ+ IMPACT

For our millions of LGBTQ+ teens, access to online platforms can be lifesaving. Three-fourths of LGBTQ+ youth are more honest about themselves online than in the real world, and more than half of closeted youth have used the internet to connect safely with peers. Research shows that LGBTQ+ youth



without access to affirming spaces are more likely to consider or attempt to commit suicide. Research also shows that, for these youth, online platforms are far more likely than their homes, communities, or schools to provide those integral spaces. As you consider the crucial issue of protecting youth online, we ask you to remember that preserving autonomous access is critical for LGBTQ+ youth.

In November 2023, LGBT Tech spearheaded a letter to Congress with 74 total signatories from civil organizations and LGBTQ+ centers, outlining concerns with language present in the Kids Online Safety Act. It is our belief that, as it stands, these concerns have yet to be adequately addressed.

LGBT TECH CONCERNS

H.R. 7891 imposes a “duty of care” obligation on online platforms that risks incentivizing online services to remove otherwise legitimate content to avoid violating the bill’s prohibitions and facing legal penalties. This risk is particularly acute in states where attorneys general may aggressively censor positive and enriching content around LGBTQ+ identities that they politically deem offensive or harmful to minors. Such actions are not theoretical; many states have already passed laws or enacted policies hostile to the LGBTQ+ community. H.R. 7891 would provide these political actors with another tool to carry out their anti-LGBTQ+ agenda.

Similarly, the bill's definition of "harmful to minors" is broad and subjective, encompassing a wide range of LGBTQ+ content that could be deemed inappropriate by capricious standards. This lack of specificity can lead to overreach and excessive content moderation, particularly impacting LGBTQ+ individuals who rely on these platforms for community, support, and access to critical information.



The First Amendment guarantees the right to free speech, yet H.R. 7891's provisions could result in widespread censorship. The requirement for platforms to mitigate harms without clear guidelines could lead to the suppression of legitimate, lawful speech. LGBTQ+ content is particularly vulnerable, as discussions around gender identity and sexual orientation often attract unwarranted scrutiny and may be wrongfully categorized as harmful. This bill, as it stands, poses a risk of silencing voices that are already marginalized. Anti-LGBTQ+ efforts are pervasive around the United States, many utilizing the "protection of children" as a smokescreen. Even the most well-intentioned legislation aimed at safeguarding children may inadvertently become a tool for discrimination.

At LGBT Tech, we are committed to ensuring that the digital world remains a safe and inclusive space for all users, particularly those in marginalized communities. We urge you to consider these points and work towards a more balanced approach that protects children without infringing on fundamental rights or disproportionately harming at-risk users. Thank you for your attention to this critical issue.

Sincerely,

A handwritten signature in black ink, appearing to read "Carlos Gutierrez".

Carlos Gutierrez
General Counsel
cgutierrez@lgbttech.org

A handwritten signature in black ink, appearing to read "Shae Gardner".

Shae Gardner
Policy Director
sgardner@lgbttech.org



May 22, 2024

The Honorable Cathy McMorris Rodgers
Chairman
U.S. House Committee on Energy &
Commerce
Washington, D.C. 20515

The Honorable Gus Bilirakis
Chairman
U.S. House Subcommittee on Innovation,
Data, and Commerce
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
U.S. House Committee on Energy &
Commerce
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
U.S. House Subcommittee on Innovation,
Data, and Commerce
Washington, D.C. 20515

Re: Main Street Privacy Coalition's Opposition to the American Privacy Rights Act as Drafted

Dear Chairman Rodgers, Ranking Member Pallone, Chairman Bilirakis, and Ranking Member Schakowsky,

The Main Street Privacy Coalition (MSPC) and its undersigned national trade association members appreciate the ongoing engagement on developing a national privacy framework, however, we are opposed to the current draft of the American Privacy Rights Act of 2024 (APRA) released last night for the markup tomorrow, May 23. We appreciate the revised language intended to address concerns related to customer loyalty programs and the treatment of covered entities with common branding, but our significant concerns remain with the private right of action, preemption, and service provider sections we previously raised in our letter of April 16, 2024, and thoughtfully and constructively addressed in suggested redlined edits to the Committee. The below comments are to be taken in conjunction with the redline edits previously provided to the draft legislative text that would mitigate our concerns.

As conveyed in conversations with Members and staff, most problematic to us and over a million American businesses we collectively represent is the inclusion of a private right of action that will expose Main Street businesses to thousands of demand letters threatening frivolous litigation. In addition, we feel further work is needed during the committee process to improve the effectiveness of the preemption provision, and strengthen legal obligations for downstream business partners that ensure businesses are accountable for their own practices and not for those of other businesses. It is our desire to work collaboratively with the Committee to address these needs in the APRA discussion draft prior to its consideration in a full committee markup. Unfortunately, without improvements to these sections that address our significant concerns, the undersigned associations cannot support the legislation.

The MSPC is comprised of 20 national trade associations that together represent more than a million American businesses—a broad array of companies that line America's Main Streets¹ and interact with consumers day in and day out. From retailers to REALTORS®, hotels to home builders, grocery stores to restaurants, gas stations to travel plazas, and self-storage to convenience stores, including franchise establishments, the businesses represented by MSPC member associations can be found in every town, city, and state, providing jobs, supporting our economy, and serving Americans as a vital part of their communities.

¹ The Main Street Privacy Coalition website and member list may be accessed at: <https://mainstreetprivacy.com>.

Collectively, the industries that MSPC members represent directly employ approximately 34 million Americans and constitute over one-fifth of the U.S. economy by contributing \$4.5 trillion (or 21.8%) to the U.S. gross domestic product (GDP). Our success depends on maintaining *trusted* relationships with our customers and clients: trust that goods and services we provide are high quality and offered at competitive prices; and trust that information customers provide to us while we are serving them is kept secure and used responsibly. For these reasons, our associations have been actively engaged for many years with policymakers on data privacy legislation and regulations.

The MSPC continues to be concerned with the inclusion in the APRA of a private right of action (PRA) that, as drafted, will have a disproportionate impact on Main Street businesses. In its current form, the bill would allow persons or classes of persons to bring a civil action in federal court seeking actual damages, injunctive and declaratory relief, and reasonable attorney's fees and litigation costs. Additionally, its scope has been expanded from the Committee's prior legislation, the American Data Privacy and Protection Act (ADPPA), to explicitly cover almost every critical requirement of the bill placed on covered entities, including loyalty programs, the exercise of "reasonable care" in selecting business partners like a service provider and third parties, and novel data minimization requirements that now exclude service providers, to name just a few. Worse yet, the proposed PRA would have a buzzsaw-like effect, becoming effective a mere six months following enactment of the bill, while simultaneously denying businesses the right they have in every state privacy law to "cure" alleged violations when facing lawsuits with damages claims. The ability to cure alleged violations in the APRA's notice and cure provision is limited only to injunctive relief, and plaintiffs are not required to even prove harm has occurred when pursuing lawsuits against Main Street businesses that typically do not use pre-dispute arbitration clauses like big tech companies and ISPs.

As we have shared with Members of the Committee and their staff for the last few years, Main Street businesses have serious concerns that this PRA language as drafted would enable trial lawyers to primarily target Main Street businesses in so-called privacy "troll" campaigns that will send thousands of demand letters to companies seeking quick settlement payments for businesses to avoid class action lawsuits for alleged violations that may not have actually occurred or caused any harm. We have discussed at length our experience with this trolling practice of unscrupulous trial lawyers in other areas of the law, such as the alleged patent infringement claims and ADA website accessibility-related lawsuits where Main Street businesses have been besieged by the onslaught of demand letters that force them to settle, while smaller entities can face bankruptcy by these monetary demands. A federal data privacy law enforced by such a robust PRA that targets consumer-facing businesses will only result in lawful Main Street businesses being forced to fight never-ending lawsuits pursued on baseless allegations instead of truly protecting consumers and their personal data from bad actors. Additionally, the need to reallocate resources to pay settlements or fight lawsuits without merit will cost Americans jobs.

All MSPC member associations firmly believe that consumers across the nation should be empowered to control the data that they have shared with businesses who serve them. We continue to be strong advocates for a preemptive federal data privacy law that creates a single, uniform national standard that applies consistent protections for consumers and obligations for businesses rather than a patchwork of state privacy laws that are confusing and burdensome for consumers and businesses alike. While we appreciate the ARPA's attempt to establish a federally preemptive framework, we are concerned that the bill as drafted includes far too many carveouts for other relevant state-level privacy laws, consumer protection laws, and laws that govern both employee and biometric data, among others. These carveouts essentially nullify the bill's preemptive effect and would require businesses to continue complying with the multitude of federal and state data privacy laws that already exist today. The end result is that this could lead to profound levels of confusion for consumers who want to protect their personal information

in a simple and understandable way as states work around the holes in the bill's preemption clause to continue to create inconsistent standards with the national framework.

Virtually every industry sector—whether consumer-facing or business-to-business—handles significant volumes of consumer information, and the MSPC member associations believe that all industry stakeholders within the digital ecosystem should have statutory obligations under federal data privacy legislation so that no consumer is left unprotected. We recognize that consumer-facing businesses like the Main Street businesses represented by the MSPC are often the businesses with whom consumers directly share their personal information, but Main Street businesses do not monetize consumer data in opaque and deceitful ways and should not be held liable for potential data privacy violations committed by their service providers or other downstream business partners. Therefore, we urge the Committee to better align the APRA's service provider and third-party requirements to match the provisions that were negotiated among several stakeholders and finalized within the text of the ADPPA as reported by the Committee. Doing so would not only help small businesses across the country in their contractual negotiations by requiring service providers and third parties to meet their obligations or otherwise be in violation of the law; more importantly, it would ensure that there are no privacy loopholes that leave consumers unprotected when their personal data is handled by any business, regardless of where they live.

Finally, the MSPC appreciates that the latest draft of the APRA aims to preserve customer loyalty programs and, upon initial review, the revised language in the draft released for markup appears to confirm that covered entities must offer the same rights and protections to customers participating in customer loyalty plans as they do today under all comprehensive state privacy laws. Loyalty programs are a critical and ever-growing facet of nearly all Main Street businesses, and most importantly are already "privacy protective" in that they are solely established and maintained on an opt-in basis in which consumers affirmatively consent to participate. We agree with the Committee that customers should not be discriminated against for choosing to exercise one of their privacy rights, and we look forward to working with the Committee to ensure the revisions to this section do not unintentionally inhibit the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships and set the terms of those relationships.

We appreciate your consideration of our significant concerns with the APRA as it is currently drafted and urge you to work with us to ensure the legislation does not disproportionately impact Main Street businesses. We stand ready to work with Members of the subcommittee and full committee to address these concerns prior to the full committee markup of the APRA.

Sincerely,

American Hotel & Lodging Association
American Beverage Licensees
American Pizza Community
American Resort Development Association
Direct Selling Association
Energy Marketers of America
FMI – The Food Industry Association
International Franchise Association
National Association of Convenience Stores
National Association of Home Builders

National Council of Chain Restaurants
National Grocers Association
National Restaurant Association
National Retail Federation
NATSO, Representing America's Travel Centers
and Truck Stops
Retail Industry Leaders Association
Self Storage Association
SIGMA: America's Leading Fuel Marketers
Small Business & Entrepreneurship Council

cc: Members of the House Committee on Energy and Commerce

May 22, 2024

The Honorable Cathy McMorris Rodgers
Chairwoman
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
House Committee on Energy & Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Gus Bilirakis
Chairman
Subcommittee on Innovation, Data, & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Innovation, Data, & Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairwoman McMorris Rodgers, Ranking Member Pallone, Chairman Bilirakis, and Ranking Member Schakowsky:

The National Association of Mutual Insurance Companies (NAMIC) is pleased to provide comments to the U.S. House Energy and Commerce Committee Subcommittee on Innovation, Data, and Commerce for its markup May 23, 2024.

NAMIC is the largest property/casualty insurance trade group with a diverse membership of nearly 1,500 local, regional, and national member companies, including seven of the top 10 property/casualty insurers in the United States. NAMIC members lead the personal lines sector representing 68 percent of the homeowner's insurance market, 56 percent of the auto market and 31 percent of business insurance markets. Through our advocacy programs we promote public policy solutions that benefit NAMIC member companies and the policyholders they serve and foster greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.

Introduction

This subcommittee markup will touch upon three bills, but this statement will focus upon one – the proposed American Privacy Rights Act, which seeks to implement a new national regulatory framework for comprehensive data privacy standards. The concept of data privacy is nothing new and conversations about the advances in technology have necessitated updates to consumer data protections. With the rapid digitization in various parts of the economy and the monetary value of collecting data on individuals, the federal government has been exploring expansions of consumer data privacy protections. There is urgency from members of Congress as well as everyday Americans to address the massive quantities of personal data and information that Big Tech is collecting on everyone, especially children.



We agree that when consumers share personal information with the entities with which they do business, they deserve to know that it will not be used in ways that will harm them or left vulnerable to bad actors. Unfortunately, the flaws in the proposed American Privacy Rights Act make it ill-fitting for the insurance industry and the broader financial services sector.

The financial services industry has been governed under the Gramm-Leach Bliley Act (GLBA) since 1999 and the insurance industry falls under that regime, in addition to enforcement by state insurance regulators. Insurance companies utilize data to better match appropriate rates and coverage to an individual's specific risk. In doing so, the insurance industry has a long history of protecting the privacy interests of its consumers.

The Gramm-Leach-Bliley Act established a landmark privacy framework for financial services, including insurance. Financial Services should be fully carved out of all aspects of APRA.

The financial services industry, including insurance, was the first sector of the economy to come under comprehensive nationwide privacy regulation, an important point to consider compared to other business segments outside of regulated financial institutions. When GLBA was enacted for financial services over 20 years ago, it set forth a rigorous regulatory framework for protecting the privacy of nonpublic personal information of financial services consumers. This current federal law also sets forth notice requirements and standards for the disclosure of nonpublic personal financial information – it specifically requires giving customers the opportunity to opt-out of certain disclosures.

While privacy impacts all industries, for financial institutions its impact must be considered in an industry-specific manner, given the nature of the customer-relationship and of the specific products/services which depend on data in a unique way. For insurance in particular, functional state insurance regulators are experts in understanding the context of the insurance products and services which rely on data to understand and price risk for consumers. It was in recognition of this expertise that Congress wisely delegated enforcement of the GLBA Title V privacy provisions to state insurance regulators, and there could be significant unintended consequences for insurance consumers that result from privacy regulation that is not appropriately tailored to their needs. Indeed, functional state insurance regulators prioritize the key tenet of consumer protections in their mission – and consumer complaints are taken very seriously in the insurance industry and regulatory community. Every state insurance department has authority to review privacy compliance as well as a market regulation program that examines and monitors insurers' practices. With nearly 11,000 employees at state insurance departments across America, the insurance regulators have a solid infrastructure in place to enforce data privacy and security requirements. In addition, in an expression of confidence in this well-established financial sector approach, the nearly one-third of state legislatures that have recently enacted comprehensive privacy laws of general applicability have included a form of GLBA exemption.

As now drafted, the wording of subsection 120(b)(3)(A) appears to have been incrementally improved by moving toward a limited exemption, but the parallel provision in subsection 120(b)(4)(A) was not similarly modified. However, even the change within the former was not a clean and full exemption, and should be further revised for incorporation in both provisions. To the extent the compliance deemer approach remains in the latter, it would essentially require that individual lawsuits (with potentially differing interpretations) be the venue for determining whether a company is in compliance with the law – so it



may not have the effect of limiting litigation or its costs and it could have the effect of complicating an area where clarity is essential. Further, “insurance” should not be referenced in Sec. 114 given GLBA as well as the state regulatory context.

In summary, a federal bill that cleanly and fully exempts financial institutions subject to GLBA is the best manner in which to proceed. NAMIC urges that the APRA language be amended to completely comport with that approach.

The APRA Does Not Eliminate the Patchwork of State Laws, Regulations, and Enforcement

Regulated entities – and consumers – benefit from clear and unambiguous rules. NAMIC appreciates the stated goal of meaningful preemption; however, the proposal falls short of removing the patchwork of state laws currently in existence through its assorted carveouts – of which there are more than a dozen. Meaningful preemption of state law must further the goal of cohesive, single, and definitive standards.

The list of state items preserved and not subject to an exemption include the following: California’s data breach notification, data security via encryption, contract or tort laws, state unfair/deceptive practices statutes, consumer protection laws, civil rights laws, unsolicited email/solicitations, employment laws, and a number of financial records laws around credit reporting and investigations. Furthermore, the APRA does not prevent states from passing additional privacy laws on top of this and would make an already unclear patchwork even more complicated.

Strong and meaningful preemption is indispensable to an efficient and effective privacy regime. Possible overlapping and/or inconsistency between privacy and data security requirements may occur when requirements come from various sources. These evolving and multi-faceted challenges are costly and time consuming for businesses, especially those that are small- and medium-sized, and this may have downstream impacts to consumers.

At a time when most want simplified and efficient communications, additional – and possibly duplicative – layers of compliance are likely to be confusing and require more of a consumer’s time for a transaction and may impede a business’s ability to meet customer expectations. When more than one agency may engage in rulemaking or enforcement, the potential for differing views may leave financial institutions subject simultaneously to potentially inconsistent or conflicting interpretations. Uncertain legal and regulatory requirements make a business environment more costly and unpredictable, at best.

The APRA includes a broad expansion of Private Right of Action (PRA) and severely limits arbitration to the detriment of consumers.

As drafted, the PRA in APRA is expanded to cover ten new areas. It also has different forms of relief and retains penalties for violations relating to Illinois’ aforementioned biometric and genetic information privacy laws in addition to California’s data breach law. Private lawsuits could sweep in technical non-compliance items, and it could further erode uniformity. This unfortunately adds costs to doing business for everyone, including the consumer. Where a knowledgeable regulator ensures that businesses are protecting data consistently, lawsuits distract from the goal of meaningful privacy protections.

A U.S. Chamber Institute for Legal Reform (ILR) 2019 paper¹ highlights the superior consumer protection of regulator enforcement over a PRA. It concluded: “... *privacy statutes that are enforced by government agencies provide a robust process through which noncompliance with protected privacy interests can be identified, remedied, and monitored while promoting consistency, fairness and innovation.*” NAMIC urges the committee to avoid the pitfalls associated with inviting privacy class actions that may largely benefit only lawyers (potentially bringing cases for intangible harm) as well as organizations profiting from litigation funding.

In previous hearings, members of Congress and witnesses have noted their concerns with a PRA in upending small- and medium-sized businesses without the financial resources to deal with the onslaught of lawsuits and litigation (potentially including speculative/securitized third-party funded lawsuits) that would likely occur under potential PRA provisions. Such provisions may open the door to compensatory damages as well money for mental anguish, inconvenience, loss of opportunity, loss of enjoyment of life, etc. – all of which lawyers may try to leverage to inflate dollars at stake in lawsuits/settlements.

Stepping back to consider the broader public policy, private rights of action provisions often turn out to be less valuable to consumers than intended. Much of the United States already suffers from being overly litigious; inclusion of a PRA threatens to exacerbate the problem. This is not in the interests of consumers because of the increasing operational challenges for businesses where there is heightened risk of uncertainty, inconsistency, and confusion. Moreover, with additional time and money devoted to litigation on matters that regulators have authority, this will distract from the data privacy and security measures. Instead, NAMIC believes it is much more efficient and effective for the government to enforce privacy laws, as this would mean consistent interpretation and implementation leading to a more stable privacy landscape for businesses and consumers. Additionally, it is concerning that pre-dispute arbitration agreements would be significantly limited as they would not apply where a claim alleges substantial privacy harm resulting from a violation. Arbitration agreements are inherently preferable to litigation due to the expedited and less costly manner for resolving disputes.

Finally, as drafted, there is no period of time set for implementation, and the private right of action and significant restrictions on arbitration would go into effect at the same time as the entire bill. **For these reasons, NAMIC opposes the passage of any federal privacy bill that contains a broad PRA.**

Algorithms and Artificial Intelligence are not synonymous. The business of insurance has long-standing and valid reasons for using models and those should not be disrupted or conflated by APRA.

At the outset, it is important to delineate between “algorithm” and “artificial intelligence,” as the terms are not one and the same. An algorithm is simply a set of instructions or rules to perform a particular task. By this definition, an algorithm can be as simple and straightforward as a cookie recipe. Conversely, artificial intelligence is a field of study, or according to the

¹ https://www.instituteforlegalreform.com/uploads/sites/1/III-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf

National Institute of Standards and Technology, “a branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning and self-improvement.” Artificial intelligence models are trained on vast amounts of data to make predictions on data they have not seen, or with generative AI, produce new content based on the model’s learning or insights from past data. By focusing the scope of Sections 13 and 14 on “algorithms”, the draft and its impact on insurance is unnecessarily, and inappropriately, broadened when applied to the insurance industry.

The foundation of insurance, and fairness in insurance, is accurately matching a policyholder’s rate to their risk. To achieve this, insurers have consistently used statistical methods and models that seemingly fit the definition of “algorithm” from the draft, as the definition of covered algorithm includes “computational process(es).” To subject insurers to the requirements of Section 13 would fundamentally disrupt risk-based pricing and likely have unintended effects on the availability and affordability of insurance for consumers. Subjecting insurers to the requirements of Section 14 would have a similar consequence, as insurers would be required to provide consumers with the ability to opt-out of being subject to the use of algorithms in the determination for issuance of the insurance product. Though paragraph (a)(1) states that the replacement process for the covered algorithm would be human review, and paragraph (a)(2) allows covered entities to refuse the consumer request, the alternate human review would still need to involve the use of algorithms as defined, and the covered entity may only refuse the request due to technology or cost. Insurers use statistical methods and models (which are not “technology”) to price the product and determine issuance for consumers, even with human review. If consumers can opt out of such algorithms, and insurers can only refuse based on technology or cost, insurers cannot adequately price the product. In effect, insurers would not have a way to price the product in accordance with state law without using an algorithm.

Even if the draft is narrowed to focus on artificial intelligence, insurance should still be distinguished to avoid dual and conflicting regulation. The insurance industry is already scrupulously regulated to prevent unfair discrimination, and that regulation is specific to the functioning and foundation of the insurance industry. For example, Section 4 of the National Association of Insurance Commissioners Property and Casualty Model Rating Law (#1780) instructs that:

“Risks may be grouped by classifications for the establishment of rates and minimum premiums. Classification rates may be modified to produce rates for individual risks in accordance with rating plans which establish standards for measuring variations in hazards or expense provisions, or both. Such standards may measure any differences among risks that can be demonstrated to have a probable effect upon losses or expenses. No risk classification, however, may be based upon race, creed, national origin, or the religion of the insured.”

If an insurer’s use of pricing or rating models produces a rating factor which is not predictive of risk or which is based on a protected class, then such conduct violates the already existing prohibition on unfair discrimination in state insurance codes. Insurers have been diligently applying these objective and understandable rules for many decades and are continuing to do so today. To subject insurers to the requirements relative to algorithms in the APRA introduces a new and separate standard that is inconsistent with governing law pertaining to unfair discrimination in risk classification.



Avoid duplicative enforcement and rely fully on the state-based system of insurance and its functional regulators to enforce data privacy and data security standards for the insurance industry and to protect insurance customers in their respective states.

While the APRA nominally respects the state-based system of insurance regulation, despite their long-standing engagement in this area, it does not rely on those functional regulators to enforce new data privacy standards. Rather, an entirely new federal regime is also introduced and financial institutions are brought within its scope. In this case, as drafted, the Federal Trade Commission would temporarily be in charge of enforcement before an entirely new bureau is created (which would be housed under the FTC). This new data privacy bureau would oversee the whole of the data privacy ecosystem (other than other forms of parallel enforcement granted – including civil actions – under APRA), including an industry that the FTC – let alone the federal government – has not regulated before.

Insurance has a long history of being regulated at the state level. A “whole of economy” approach, even broken down by sector, most certainly does not work for the insurance industry – or its consumers. A one-size-fits-all approach on data collection, usage, and protection mechanisms is not appropriate for financial institutions.

Conclusion

NAMIC represents a wide range of insurance companies providing valuable services, peace of mind, and financial resources to consumers, and any legislation should account for the different data privacy requirements these entities already follow. The existing insurance legal and regulatory framework relating to data privacy and security relies on regulators familiar with the context of insurance. They navigate the nature of consumer relationships as well as the types of products and services offered by insurers while remaining cognizant of the operations of different sized companies within their state market. NAMIC encourages continuing with this proven approach that is both risk-based and scalable to ensure that insurers have necessary protections in this evolving threat landscape.

On behalf of nearly 1,500 member companies, NAMIC is prepared and willing to engage on the important subject of privacy laws and regulating our industry. We applaud the work of Chair McMorris Rodgers’ work on this topic and we stand ready to provide valuable input to help ensure this draft appropriately accounts for the business of insurance and avoids adding new costs and burdens to consumers.

In addition, NAMIC supports efforts undertaken by Chair McHenry of the House Financial Services Committee to modernize and update GLBA in the Data Privacy Act, H.R. 1165. Recognizing that more drafting needs to be done to address concerns, this legislation maintains state enforcement for insurers, does not include a PRA, and importantly updates GLBA to provide consumers with additional consumer protections. We believe any new privacy legislation applying to financial institutions should occur within sector-specific legislation.

It will be critical to make certain the standards put forth in any comprehensive legislation are appropriate for the insurance



industry. The best way to accomplish this goal is through a clear and full exemption for entities subject to GLBA. NAMIC looks forward to working with Committee Leadership and members of the Committee to ensure that any language that becomes law avoids potential unintended consequences for the insurance industry and the consumers that it protects.

Sincerely,

Jimi Grande
Senior Vice President – Federal & Political Affairs



May 22, 2024

The Honorable Cathy McMorris Rodgers
Chair, House Energy and Commerce Committee
United States House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone, Jr.
Ranking Member, House Energy and Commerce Committee
United States House of Representatives
2322A Rayburn House Office Building
Washington, D.C. 20515

Re: American Privacy Rights Act and Kids Online Safety Act

Dear Chair McMorris Rodgers and Ranking Member Pallone:

We write today to add our voice to the chorus that are expressing views on the proposed legislation being heard tomorrow. Our members appreciate the efforts to continue to find consensus to pass national, uniform consumer privacy legislation. We wanted to take the opportunity to provide our feedback on two bills under consideration during this hearing: **American Privacy Rights Act of 2024 (APRA), including the Children's Online Privacy Protection Act 2.0 (COPPA 2.0), and the Kids Online Safety Act (KOSA)**. We remain hopeful that Congress will work together to move comprehensive legislation across the finish line. As such, we request that this letter be submitted into the legislative record.

SIIA is the principal trade association for those in the business of information. Our nearly 400 member companies reflect the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services. On behalf of our members, we view it as our mission to ensure a healthy information ecosystem: one that fosters its creation, dissemination and productive use.

Privacy is essential to the health of that ecosystem. Our members believe that a comprehensive privacy law is critical to address concerns about the lack of accountability and transparency with how consumer data is collected, processed, and used. However, we are concerned that the bill could unintentionally hamstring a

variety of productive data uses that in turn create far-reaching domestic and international consequences.

Title I of the American Privacy Rights Act of 2024 - American Privacy Rights

Areas of Strength

Title I is a thoughtful draft that improves on the earlier APRA discussion draft and will serve as a positive step towards comprehensive federal privacy legislation. We are pleased to see that the FTC is now empowered to add additional permitted purposes in response to technological developments via Section 125's "Innovation Rulemakings." We are also generally pleased with clarifications to the APRA's treatment of artificial intelligence. For example, the definition of "covered algorithm" has been substantially improved, and significantly reduces uncertainty around such an algorithm's activities and the extent to which it assists human decision making. Furthermore, we appreciate the clarification around the definition of "consequential decision" to avoid advertising, which would otherwise wrap in a great deal of unintended and innocuous commercial activity, though would encourage further clarity around the phrase "educational enrollment or opportunities" in that definition to avoid adverse consequences to learners.

We also applaud the creation of a pilot program to encourage private sector use of privacy-enhancing technologies (PETs) for the purpose of protecting covered data. SIIA has long advocated in favor of PETs, which have the potential to reduce or eliminate privacy risks for consumers while simultaneously enabling the productive use of valuable data sets.

For our members, it is imperative that the legislation respect the bounds of the First Amendment. To that end, the bill exempts publicly available information (PAI), as well as inferences derived solely from PAI. With one exception, noted below, the draft helpfully clarifies that inferences that reveal sensitive covered data remain protected under the First Amendment unless combined with sensitive data itself. We were also pleased that the new draft avoids removing PAI's public designation when temporarily combined with covered data.

From our perspective, the preemption provision has improved, and we applaud the express statement that it is intended to serve as a single, comprehensive federal privacy law. The bill then includes strong preemption that avoids a confusing and expensive patchwork of state privacy laws, and eliminates the carve outs reserved for states that happened to pass privacy laws pre-introduction. We believe that the preemption provision can be further refined so that states may not use common law or existing statutory law to evade Congress's stated intent. That evasion is of particular concern because of the private right of action provision.



Areas that Require Further Attention

First, although we are glad to see that the bill exempts PAI and inferences derived solely from PAI, we are concerned that Title I does not exempt data derived from PAI. This feature, set out in Section 101 (39)(B)(iii)(II) would turn PAI into sensitive covered data. This would include, for example, anything to do with a child.

Second, APRA imposes a presumption of illegality around benign areas of technological development and use, with minimal or no link to a privacy harm. For example, Section 102 would restrict all covered data collection and processing to a set of predetermined permitted purposes, resulting in unforeseen legal technicalities that would hamstring future technological development. For example, AI development would largely violate APRA's permitted purpose restrictions. Not only is general AI development not included as a permitted purpose, but models' natural application for a variety of purposes would run afoul of this section.

Third, the bill expands the definition of sensitive data to include new, inflexible categories that are overinclusive of data that may pose little risk, but also underinclusive of high-risk uses of data that the definition does not cover. For example, the APRA defines "sensitive data" to include "information *about* a minor under the age of 17." There are two implications of this that we find concerning. First, it places the bill at odds with laws at the federal level and in the states designed to protect children's privacy, wrapping children's data into the "sensitive data" regulatory framework. Second, the word "about" would render this provision seriously overbroad (e.g., a picture of a child). In our view, the term "sensitive data" should be limited to that information which, by its nature, is intrinsically subject to abuse or the release of which would be offensive to a reasonable person.

Lastly, APRA imposes significant requirements on data brokers, and omits a variety of exemptions we believe would be helpful to permit entities that fall under this definition to engage in societally positive data sharing. The bill also departs from the definition of "data broker" in every U.S. state data broker law, which cover entities that process *and* transfer personal data. Instead, APRA defines data brokers as entities that process *or* transfer personal data they did not collect directly from a consumer. Even with APRA's service provider exemption, this could wrap in a variety of businesses that are neither commonly understood nor appropriately regulated as data brokers. For example, it could capture a social media platform that uses a user-generated photo of multiple subjects—but where only one subject posts the photo—to inform the user experience and generate personalized content.



Title II of the American Privacy Rights Act of 2024 - COPPA 2.0

Areas of Strength

We see the inclusion of language to update COPPA in APRA as an encouraging step on protecting the privacy and safety of children while ensuring they are able to connect, learn, and access information online. We appreciate the attempts to harmonize language protecting children under both titles of APRA to avoid conflicting requirements.

We are pleased that COPPA 2.0 includes language that clarifies how COPPA works in public schools. The lack of clarity on how to protect student data subject to protections under both the Family Educational Rights and Privacy Act (FERPA) and COPPA has been unclear since the passage of COPPA over two decades ago. The proposed changes in this legislation will ensure student data is protected without creating conflicting legal obligations for schools and vendors or rights for students and parents.

The text of COPPA 2.0 also codifies internal operations language that was included in the 2013 rulemaking and has been incorporated into many business practices over the past decade. We are pleased this will allow businesses some predictability in their compliance work going forward.

Areas that Require Further Attention

We are concerned that COPPA 2.0 would, even if unintentionally, prohibit contextual advertising, which could lead operators to charge for access or cut off services. Contextual advertising has played an important role in supporting the creation of free high-quality content for kids. Without the support of contextual advertising revenues, this content may no longer exist. We urge the Committee to consider amending the definition to allow contextual advertising as defined under the 2013 Rule's internal operations definition.

Kids Online Safety Act (H.R. 7891)

Areas of Concern

We are extremely concerned about the impact of KOSA on both young people and all Americans. We believe this bill will require extensive modifications in order to protect the privacy and safety of young Americans. As written, it will require companies to censor content for users, which raises First Amendment concerns. A negligence standard for "duty of care" would create a burdensome risk of liability, leaving online platforms with virtually no choice but to restrict content.



The current text also requires companies to offer different services to users of different ages, effectively requiring age verification, which could be invasive to privacy. Experts have noted this could require companies to collect more information than necessary on all users, not just kids.

We urge Congress to consider further improvement to KOSA that would meaningfully strengthen privacy protections and uphold Constitutional rights for all Americans. We encourage Congress to consider the [Child and Teen Privacy and Safety Principles](#) that SIIA released in March as a framework for legislation that avoids the concerns outlined above.

We stand ready to continue to work with the Committee to ensure the proposals represent balanced and comprehensive federal standards to protect the privacy of all Americans. Thank you for considering our views.

Respectfully,

Christopher A. Mohr

President





TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

May 22, 2024

To the Members of the House Energy and Commerce Subcommittee on Innovation, Data, and Commerce:

We believe comprehensive and preemptive federal data privacy legislation should end the growing privacy patchwork, protect consumers, and allow American innovation to flourish. Unfortunately, the proposed *American Privacy Rights Act* (APRA), even in its updated form, fails to meet this standard.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. Our [membership](#) includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.4 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

This week, Minnesota became the [20th state](#) to pass a comprehensive privacy bill. It is critical that Congress work to enact comprehensive federal privacy legislation that preempts state law and protects all Americans regardless of their age or where they live, thereby ending the growing state-by-state privacy patchwork. Comprehensive privacy legislation should not include private rights of action, must be tech- and sector-neutral and apply to online and offline entities that collect and process personal information, and should ensure that consumers have the right to access, correct, and delete their data without undermining privacy or data security interests. As drafted, APRA fails to accomplish these goals and would actively hurt American businesses.

First, APRA includes language that fails to recognize the value of reasonable data collection, processing, use, and retention activities to improve and personalize consumer services. Instead of empowering consumers to have greater control over their data while providing clarity for businesses, APRA empowers the Federal Trade Commission to serve as the gatekeeper for private sector innovation and could have a significant negative impact on the digital advertising ecosystem and the free and open internet. Burdensome regulations will likely entrench the largest companies while imposing significant [barriers to entry](#) for startups and small- and medium-sized enterprises. According to an [analysis](#) of the European Union's General Data Protection Regulation (GDPR), GDPR ultimately "induced the exit of

approximately 33 percent of available apps and reduced the entry of new apps by 50 percent.”

APRA also contains several provisions that will undercut the stated goal of creating a consistent and uniform national standard that would permanently address the costs of a growing patchwork of state privacy laws, estimated at [\\$1 trillion over ten years](#), with \$200 billion being borne by small businesses. For example, APRA’s preservation of a variety of state laws could allow states to expand the existing privacy patchwork based on their own interpretation of whether a particular product or service amounts to a deceptive, unfair, or unconscionable practice. Notably, APRA’s inclusion of a carve-out for state health privacy laws would preserve Washington’s *My Health, My Data Act*.

Finally, under APRA, companies that provide services to consumers would face the threat of costly litigation for a variety of circumstances. In addition to creating an expansive federal private right of action, APRA also separately preserves several state-specific private rights of action, such as the *California Privacy Rights Act* and Illinois’ *Biometric Information Privacy Act*, further undermining the goal of creating a consistent and uniform national standard.

In the absence of substantive changes to address this bill’s negative impacts on consumers and businesses, we respectfully urge you to oppose this legislation and instead craft comprehensive and preemptive privacy legislation that protects consumers, allowing the American people to enjoy the benefits of continued innovation in the data-driven economy, and ensures America wins the next era of innovation.

Thank you for your consideration of our perspective on this important issue.

Sincerely,



Carl Holshouser
Executive Vice President



Center for American Progress
1333 H Street NW, Suite 100E
Washington, DC 20005
202.682.1611
americanprogress.org

May 20, 2024

The Honorable Cathy McMorris Rodgers
Chair of Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Maria Cantwell
Chair of Committee on Commerce, Science and Transportation
U.S. Senate
Washington, DC 20515

Dear Chair McMorris Rogers and Chair Cantwell,

The undersigned researchers and groups commend your bipartisan efforts to create comprehensive privacy legislation through the American Privacy Rights Act (APRA).¹ The draft represents a step forward in establishing robust privacy protections for all Americans.

As researchers and academics, we understand that privacy protections are critical. At the same time, informed research plays a vital role in helping us understand the nuances of online activities and the operations of large digital platforms, and to hold them accountable. This research is essential for ensuring transparency and accountability in the digital space, providing critical insights into the complexities of online environments.²

However, we are concerned that the current draft of the APRA may inadvertently limit the capabilities of public interest researchers under the bill. In particular, Section 3(d)(7)(C), which stipulates that covered data must be processed “such that the data becomes de-identified data,” could significantly impair researchers’ ability to validate findings, replicate studies, and could lead to the exclusion of certain demographic groups or vulnerable populations from research initiatives. This requirement for de-identification could pose significant challenges, as it often necessitates the removal or modification of key identifiers and critical contextual information essential for comprehensive research, including detailed demographic studies. Furthermore, the process of de-identifying online data could disproportionately exclude or obscure data related to specific demographic groups or vulnerable populations, thereby skewing research outcomes and undermining the inclusivity and relevance of online data-driven studies. Moreover, the current language in Section 3(d)(7) that states “with respect to covered data previously collected in accordance with this Act”³ seems to extend the permissible purpose only to data previously

¹ American Privacy Rights Act of 2024, available at https://d1dth6e84htgma.cloudfront.net/PRIVACY_02_xml_005_6e97fe914c.pdf

² Nathaniel Persily and Joshua A. Tucker, “How to fix social media? Start with independent research.” Brookings, December 1, 2021, available at <https://www.brookings.edu/articles/how-to-fix-social-media-start-with-independent-research/>

³ American Privacy Rights Act of 2024, Sec 3(d)(7)

collected under APRA for purposes other than public research, significantly limiting the scope of information available to researchers, since, unlike companies they generally will have no other purpose for collecting data. These restrictions might inadvertently diminish the quality and relevance of the research that is crucial for informed policy making and governance.

We specifically suggest revisiting and clarifying the language in Section 3(d)(7)(C) of APRA to clarify that researchers have access to data and that access to data remains useful and representative for their studies. To this end, we propose aligning with the language and provisions found in Section 101(b)(10)⁴ of the American Data Privacy and Protection Act (ADPPA), which offers a more balanced approach to handling research data while ensuring privacy. This provision from ADPPA provides a standalone permissible purpose for public interest research, distinct from research conducted by companies, and does not impose a de-identification requirement, thus facilitating more robust and inclusive research outcomes.

For your reference, here is the language from Section 101(b)(10) of the ADPPA:

A covered entity may collect, process, or transfer covered data for any of the following purposes if the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to such purpose

(10) (A) To conduct a public or peer-reviewed scientific, historical, or statistical research project that—

(i) is in the public interest; and

(ii) adheres to all relevant laws and regulations governing such research, including regulations for the protection of human subjects, or is excluded from criteria of the institutional review board.

(B) Not later than 18 months after the date of enactment of this Act, the Commission should issue guidelines to help covered entities ensure the privacy of affected users and the security of covered data, particularly as data is being transferred to and stored by researchers. Such guidelines should consider risks as they pertain to projects using covered data with special considerations for projects that are exempt under part 46 of title 45, Code of Federal Regulations (or any successor regulation) or are excluded from the criteria for institutional review board review.

We believe that adopting this adjusted or similar language will significantly strengthen the bill, enhancing its capacity to protect privacy effectively while also supporting critical research activities. Such enhancements will ensure that the APRA legislation not only meets its intended goals but also adapts to the complex and evolving landscape of digital interactions. We commend you for your dedication and leadership on this critical issue and look forward to collaborating closely with your offices to ensure the American Privacy Rights Act serves as a robust framework for privacy.

Sincerely,

⁴ American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022), available at <https://www.congress.gov/bill/117th-congress/house-bill/8152/text>

Center for American Progress

Brandon Silverman

Center for Democracy & Technology

DatastrategIA

Dhavan Shah, University of Wisconsin-Madison

Dr. Emma L. Briant, Monash University

Filippo Menczer, Observatory on Social Media, Indiana University

Jeff Hancock, Stanford University

Jonathan Stray, UC Berkeley

Kostadin Kushlev, Georgetown University

Morgan Quinn Ross, The Ohio State University

New America's Open Technology Institute

Public Citizen

Rebekah Tromble, George Washington University

Renee DiResta, Stanford Internet Observatory

Shannon McGregor, University of North Carolina

May 17, 2024

Honorable Cathy McMorris Rodgers
Chair
House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515-4705

Honorable Frank Pallone
Ranking Member
House Energy and Commerce Committee
2322A Rayburn House Office Building
Washington, DC 20515-3006

Honorable Gus Bilirakis
Chairman Innovation, Data, and Commerce
House Energy and Commerce Committee
2306 Rayburn HOB
Washington, DC 20515

Honorable Jan Schakowsky
Ranking Member Innovation, Data, and Commerce
House Energy and Commerce Committee
2408 Rayburn HOB
Washington, DC 20515

The undersigned organizations and experts are writing to express our strong support for provisions that would ensure oversight and accountability of the tech sector, including platform transparency and researcher access. As you look to protect minors and safeguard Americans' data privacy online, we urge you to include the strongest possible transparency provisions, which are crucial to ensuring compliance with federal statutes and creating safer, healthier online spaces.

With key bills gaining momentum right now, Congress has a chance to do what many thought would never be possible and what tech companies have fought against for nearly two decades — dramatically tilt the balance of power on the internet towards consumers by requiring the largest online providers to prioritize the privacy and safety of their users. The attention of both parties and both chambers to these important proposals deserves to be celebrated.

However, meaningful transparency is a key pillar of tech accountability. Without any legislative or regulatory mandate to do so, the largest tech companies have chosen to reveal little about how their platforms work. Through the persistent work of researchers and Congressional offices, as well the bravery of whistleblowers, we have learned key information about how tech companies scrape and monetize our data, hook the attention of our children, and divide our

communities with the most inflammatory content. But too often, efforts to uncover the truth are blocked by the companies or silenced by the threat of lawsuits.

This year, both [TikTok](#) and [Meta](#) restricted tools used by independent researchers and academics. The U.S. needs a consistent, meaningful transparency framework to truly unlock the black box, empower policymakers, and enforce other reform efforts like kids' safety and comprehensive privacy. Right now, we're heading in the opposite direction.

Bipartisan, effective provisions to ensure accountability, oversight, and compliance include:

- Advancing our understanding of the societal and mental health impacts of social media by requiring large platforms to provide qualified, independent, and approved researchers with access to certain platform data;
- Requiring online platforms to conduct and publish risk assessments focused on the online safety of minors and data privacy, including detailing their risk mitigation efforts. Using third-party, independent auditors to confirm these risk mitigation practices annually (similar to construction-industry safety audits).
- Assuring user privacy and protecting proprietary corporate information through strict privacy and cybersecurity requirements; and
- Preventing retaliation against researchers and companies by shielding individuals, organizations, and platforms that adhere to privacy and cybersecurity safeguards from legal liability.
- Requiring online platforms to develop comprehensive "ad libraries." These libraries should include the content of all advertisements on the platform, who paid for each advertisement, the period during which an advertisement was presented, the total number of recipients reached, and information about the extent to which an advertisement was recommended, amplified, or restricted. Meta has long maintained an ad library, but has [restricted researcher access](#) to it.

These provisions are crucial for holding social media companies accountable for how their design choices and business models impact our kids, our communities, and our democracy. The disclosures enabled by this framework would provide policymakers with high-quality, independently verified information vital to crafting effective solutions and ensure compliance with other tech reform priorities.

As you continue to craft important bills to reign in the practices of Big Tech companies, we, the undersigned organizations and experts, strongly urge you to remember and incorporate the strongest transparency provisions possible. Thank you for your attention to these critical issues.

Sincerely,

American Psychological Association
Anti-Defamation League
Brightlines
Center for Countering Digital Hate

Children and Screens: Institute of Digital Media and Child Development
Child Mind Institute
Coalition for Independent Technology Research, Board of Directors
CrowdTangle
Institute for Strategic Dialogue
Issue One
National Conference on Citizenship

Baobao Zhang, Syracuse University*
Cameron Hickey, National Conference on Citizenship
Connie Moon Sehat, Analysis and Response Toolkit for Trust
Dean Jackson, Public Circle, LLC
Dimitri Christakis, University of Washington
Dr. Emma L. Briant, Monash University
Francesco Andrea Causio, Società Italiana Intelligenza Artificiale in Medicina
Ilan Strauss, University College London
Jonathan Haidt, New York University
Peter Gerhardstein, Binghamton University-SUNY
Renee DiResta, Stanford Internet Observatory
Dr. Toussaint Nothias, New York University
Yael Eisenstat, Cybersecurity for Democracy

**Affiliations listed for identification purposes only*