TECHNET
THE VOICE OF THE INNOVATION ECONOMY

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

June 26, 2024

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

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

Dear Chair Rodgers and Ranking Member Pallone:

In advance of the House Energy and Commerce Committee's markup of the *American Privacy Rights Act* (APRA), we write to share our opposition to this legislation in its current form.

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.

Since 2018, the rapidly growing landscape of state-level privacy laws has created a fragmented patchwork of rules and regulations that are confusing consumers, stifling innovation, and increasing uncertainty for America's businesses, especially small businesses. In May, Minnesota became the 20th state to pass a comprehensive privacy bill. It is critical, now more than ever, that Congress work to enact comprehensive federal privacy legislation that preempts state law and protects all Americans regardless of where they live, permanently ending the growing state-by-state privacy patchwork. Comprehensive privacy legislation should not include private rights of action, must be 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.

We believe comprehensive federal data privacy legislation should protect consumers, mitigate abusive lawsuits, and avoid costly and burdensome regulations that undermine the innovative American products and services that consumers rely on or impose disproportionate burdens and compliance challenges on new entrants

and startups. Comprehensive federal privacy legislation should not only empower consumers but also ensure they can enjoy the benefits of continued innovation in the 21st century digital economy. In addition, federal privacy legislation must not undermine America's global competitiveness or leadership in emerging technologies, such as artificial intelligence. Unfortunately, in its current form, APRA fails to meet this standard.

First, APRA includes several provisions that fail to recognize the value of reasonable data collection, processing, use, and retention activities to improve and personalize consumer services. These include, but are not limited to, APRA's stringent and overbroad data restrictions, which would undermine consumer choice and impact the ability of companies to provide features and personalized content that consumers value.

Instead of empowering consumers to have greater control over their data while providing clarity for all businesses, APRA would impose significant constraints on the data-driven economy and could shift much of the free and open ad-supported internet behind paywalls. Specifically, APRA would place severe restrictions on digital advertising, fundamentally threatening the ability of creators, publishers, and sites of all sizes to provide high-quality content for free or help small businesses reach new customers. Notably, APRA does not allow for ad measurement because it classifies data needed for ad measurement as "sensitive covered data," pushing digital advertising out of reach for small businesses who cannot afford or justify larger ad spends without the ability to determine their effectiveness.

In addition, the creation of unprecedented "Innovation Rulemakings" authority for the Federal Trade Commission is an admission that APRA's restrictive framework would stifle innovation and American competitiveness.[1] Ultimately, burdensome data privacy regulations will likely entrench the largest companies while imposing significant barriers to entry for startups and small- and medium-sized enterprises.[2] 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."[3]

---

[1] *American Privacy Rights Act* Discussion Draft, June 20, 2024, at 157: Sec. 123. Innovation Rulemakings: "The Commission may conduct a rulemaking pursuant to section 553 of title 5, United States Code—(1) to include other covered data in the definition of the term "sensitive covered data", except that the Commission may not expand the category of information described in section 101(49(A)(ii); and (2) **to include in the list of permitted purposes in section 102(d) other permitted purposes for collecting, processing, retaining, or transferring covered data** [emphasis added]."

[2] "A New Study Lays Bare the Cost of the GDPR to Europe's Economy: Will the AI Act Repeat History?" Center for Data Innovation (April 9, 2022)

[3] "GDPR and the Lost Generation of Innovative Apps," National Bureau of Economic Research (May 2022).

APRA also contains ineffective preemption language 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.[4] As drafted, APRA only preempts state laws, rules, and regulations "covered by" the provisions of APRA instead of the more substantive "related to" preemption language.[5] In practice, APRA's "covered by" preemption language only preempts what is "covered by" APRA, giving states the green light to pass new variations of privacy laws featuring terms or addressing practices not included in the federal bill.

In addition to ineffectively preempting state privacy laws, APRA separately preserves a variety of state laws that will allow states to recreate a privacy patchwork. For example, states and consumers are given the freedom to litigate based on their own state law interpretations of whether a particular product or service amounts to a deceptive, unfair, or unconscionable practice.[6] APRA's inclusion of a carve-out for state health privacy laws could also be interpreted as preserving Washington's *My Health, My Data Act*.[7]

Finally, under APRA, companies that provide services to consumers via the Internet would face the threat of costly litigation for a variety of circumstances and could face penalties for merely attempting to personalize the online experience for consumers or striving to improve and develop new products and services. In addition to applying an expansive federal private right of action to a majority of the bill's provisions, APRA also continues to separately preserve 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.[8]

For these reasons, we strongly urge you to oppose this legislation and instead craft comprehensive and preemptive privacy legislation that protects consumers, allows the American people to enjoy the benefits of continued innovation in the data-driven economy, and ensures America wins the next era of innovation.

---

[4] "The Looming Cost of a Patchwork of State Privacy Laws," Information Technology & Innovation Foundation (January 24, 2022).
[5] "In *CSX Transportation, Inc. v. Easterwood*, the Supreme Court interpreted ["covering" preemption language] as having a narrower effect than "related to" preemption clauses." *See* Congressional Research Service, "Federal Preemption: A Legal Primer" (May 18, 2023)
[6] *American Privacy Rights Act* Discussion Draft, June 20, 2024, at 141: Sec. 118(a)(3)(A): "Paragraph (2) may not be construed to preempt, displace, or supplant…(A) Consumer protection laws of general applicability, such as laws regulating deceptive, unfair, or unconscionable practices."
[7] *See* Id. at 143: Sec. 118(a)(3)(N): Paragraph (2) may not be construed to preempt, displace, or supplant…(N) Provisions of laws that protect the privacy of health information, medical information, medical records, HIV status, or HIV testing."
[8] *See* Id. at 134-136

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

Thank you for considering our perspective on this important issue.

Sincerely,

Carl Holshouser
Executive Vice President