June 26, 2024

Chair Cathy McMorris Rodgers (R-WA)
Committee on Energy and Commerce
Washington, DC 20515

Ranking Member Frank Pallone (D-NJ)
Committee on Energy and Commerce
Washington, DC 20515

Dear Chair McMorris Rodgers, Ranking Member Pallone, and Members of the House Committee on Energy and Commerce:

The Computer & Communications Industry Association (CCIA) is an international nonprofit association representing a broad cross section of communications and technology firms. For more than fifty years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. For decades, CCIA has advocated for a national consumer-focused privacy law which provides certainty to both consumers and businesses. Because the American Privacy Rights Act (APRA) fails to accomplish these goals, CCIA opposes this legislation.

Overarching concerns underscore a cross-cutting flaw with APRA: it fails to engage with the reality of how digital service technologies interact and function. A strong comprehensive national privacy framework must protect consumers and enable technological innovations that are essential to U.S. productivity. With this in mind, CCIA offers substantive commentary to explain APRA's fundamental issues:

I. Data minimization prohibitions misconstrue data processing;
II. Knowledge standards conflict with privacy protections;
III. Required mitigation of undefined "privacy risks" harm communities; and
IV. Broad enforcement and limited preemption will not protect consumers.

I. APRA's Data Minimization Prohibitions Demonstrate a Lack of Understanding of How Data Processing Operates

APRA's data minimization provision bars data processing unless a company can prove it had an ambiguous "permitted purpose." This prescriptive approach deters innovation, thereby harming economic growth in a competitive digital services marketplace.

Concerningly, because a permissible purpose is subject to the overall data processing prohibition, companies may be forced to ensure that every individual processing choice fits neatly within a permitted purpose. In practice, this result would shift the sole burden of defending processing choices in any future litigation. Such a burden is only heightened by APRA's broad monitoring requirement that would force businesses to bear sole responsibility for any partnerships with service providers or other third parties.

The fundamental issue with this provision is that it demonstrates a lack of understanding of how digital service technologies work. For most applications, data is processed to provide a consumer function. Whether it is to return the most helpful answer to a query or curate a user's online experience, processing one dataset may flow to an untold number of distinct services and applications. In a world where each processing decision would first require a strict legal analysis, businesses will be forced to step into the shoes of a future enforcer. This guesswork would prioritize limiting liability over improving functions for consumers.

The result would be to divert development resources away from innovative products that consumers love and benefit from to a world where today's free services would be heavily restricted or subject to user fees. Taken together, APRA's data processing prohibitions would represent one of the most restrictive regimes in the world, thereby endangering the availability and development of countless digital services and tools. While minimizing data processing is certainly a laudable goal, there must be more flexibility for reasonable data collection, backed by clear permissible purposes that ensure continued innovation over increased litigation.

II. A Confusing Knowledge Standard Will Conflict With Privacy Protections

Along with APRA's overly restrictive approach to data processing are increased burdens on companies to intimately know each of their users. Besides creating a natural conflict with data minimization requirements in the bill, compliance with these provisions could force covered entities to collect more data than needed to provide a consumer-focused service.

APRA defines "knowledge" as "actual knowledge or knowledge fairly implied on the basis of objective circumstances." Confusingly, the definition qualifies that it may potentially only apply towards a "child, teen, or covered minor," despite the term "knowledge" arising in multiple

other sections that apply more broadly. This conflict would first need to be settled through substantial litigation, which could implement entirely different interpretations of the term "knowledge" depending on the state.

Even assuming the "knowledge" standard is limited, its implications are broad. All data processing and transfers related to children, teens, and covered minors would be generally banned unless that activity falls within an even more limited set of permissible purposes and affirmative express consent is provided.

This creates a natural conundrum: if APRA prohibits data processing, how does a covered entity or service provider know whether a user is a child, teen, or covered minor?

One answer may be that covered entities must employ age verification standards that require additional sensitive data collections including geolocation and government identifications for all users. However, because sensitive data also requires affirmative express consent, a circular outcome occurs where a covered entity must, but also cannot, legally collect the appropriate data to ensure it is complying with APRA.

And, even if covered entities tried to employ such technologies, age verification is expensive, and above all, inaccurate in many circumstances. This raises serious concerns about false positives and negatives. Moreover, compliance generally requires digital services to use third-party services, heightening security risks. Given the potential for broad litigation by state attorneys general and the FTC, APRA's attempt to provide a dubious rule of construction stating that companies need not employ forced data collection and age-gating technologies will be meaningless in practice.

Finally, APRA closes the door on additional guidance to understanding knowledge standards by making clear that, although the FTC will provide additional non-legally binding information about its breadth within 180 days, it cannot hinder any future action. Courts will scramble to understand what this provision means in relation to current long-standing jurisprudence on non-legally-binding agency guidance, especially in relation to APRA's allowances for actions to be both consistent, or inconsistent, with FTC guidance depending on the allegations.

In sum, there must be clear guidelines in place to ensure covered entities understand their obligations. Extra care should be taken to limit compulsory collection or unworkable age verification methods.

III. Ambiguous Requirements to Mitigate Undefined Privacy Risks Censor Speech and Harm Communities

APRA ambiguously requires all covered entities and service providers to mitigate "privacy risks" for minors under 17 and individuals over 65 in products, services, and with service providers. The term "privacy risks" is entirely undefined.

Given the breadth of this provision in serving as a broad basis for new liability, the implications are chilling on lawful content and services. To avoid liability, companies may be forced to limit access to certain communities and speech altogether. Communities who may be unable to freely express themselves or find like-minded individuals offline will be further cut off from these valuable resources online. For example, when users access content and services relating to important and sensitive subjects like mental health and behavioral disorders, LGBTQ+ matters, sexual health, reproductive information, and family planning, for example, the prospect of an undefined 'privacy risk' arising is not trivial.

The internet is an integral component of community building and social expression. In light of the extraordinary volume of internet communications, imposing liability unless companies increase review and removal of constitutionally protected speech is a chilling barrier that only hurts internet users. This entire section should be removed, or substantially more information should be provided to define "privacy risks" as compared to "substantial privacy harms," which is already defined, as well as how a business can understand its obligations before being hauled into court.

IV. Broad Enforcement and Limited Preemption Will Not Protect Consumers

APRA contains a broad private right of action, backed by requirements that judges account for new theories of liability which would employ emotional or reputational damages. Such an expansion goes substantially further than even the U.S. Supreme Court is comfortable in defining privacy harms that warrant remedies.

Included in the broad private right of action, for example, is the ability for individuals to sue if they believe a company's privacy policy is not "clear and conspicuous." Often a question of fact rather than one of law, this cause of action will be weaponized to avoid early dismissal of even the most unfounded of complaints. When combining this with a dozen other opportunities for private litigation, companies will be constantly under threat of defending actions rather than protecting privacy.

In addition to broad enforcement, APRA contains a similarly expansive list of preserved state laws, which will do little to persuade courts of APRA's stated purpose: "to establish a uniform

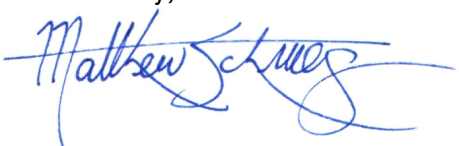
national privacy and data security standard in the United States." Indeed, the savings clause provides a list of 25 categories of state law that are expressly preserved under APRA. This includes theories of liability that drive nearly all existing state-based privacy claims such as negligence, fraud, and state consumer protection laws. In sum, it would be exceedingly difficult to prove that any state law is preempted, leading to a result that only further increases the burdens on companies and consumers alike in understanding the rules of the road.

APRA should instead make clear that any conflict between federal and state law should lead to preemption, as envisioned by the Supremacy Clause of the Constitution. The private right of action should also be limited to match existing legal theories or harm, which generally require showing an actual cognizable injury before assigning a remedy.

* * * * *

In sum, APRA proceeds by attempting to regulate an industry it does not understand. It implements restrictive burdens on companies that will break many digital services. Backed by broad enforcement mechanisms, the result will be a net negative on consumer privacy and technological innovation. Nothing less than a substantial re-working of APRA is necessary to deem this legislation worthy of being signed into law.

Sincerely,



Matt Schruers
President & CEO
CCIA