



April 17, 2024

The Honorable Gus Bilirakis  
Chairman  
Innovation, Data, and Commerce Subcommittee  
2306 Rayburn House Office Building  
Washington, DC 20515

The Honorable Jan Schakowsky  
Ranking Member  
Innovation, Data, and Commerce Subcommittee  
2408 Rayburn House Office Building  
Washington DC, 20515

**RE: Hearing on Legislative Solutions to Protect Kids Online and Ensure Americans' Data Privacy Rights.**

Dear Chairman Bilirakis and Ranking Member Schakowsky:

Thank you for convening today's hearing on legislative proposals to ensure Americans' data privacy rights, including the recently released discussion draft of the American Privacy Rights Act (APRA). BSA commends House Energy & Commerce Chair Cathy McMorris Rodgers and Senate Commerce Chair Maria Cantwell for their bicameral and bipartisan work on APRA but note that we have concerns with the current version of the discussion draft. Establishing a strong comprehensive federal privacy law is a top priority for BSA and we welcome continued engagement to ensure that the next version of APRA is effective, workable, and provides consumers and businesses with the certainty they deserve.

BSA | The Software Alliance is the leading advocate for the global software industry.<sup>1</sup> Our members are enterprise software companies that create the business-to-business technology products and services that power the digital transformation of companies in every industry. BSA members provide design and project management services, customer relationship management software, human resource management programs, cybersecurity services, identity management services, and remote collaboration software, along with a range of other enterprise technology products.

Every day, American consumers share their personal information with businesses just by using routine products and services. Consumers deserve to know that their data is being used responsibly. As more states consider or advance comprehensive privacy legislation, consumers and businesses alike face the possibility of fragmented regulatory regimes that

---

<sup>1</sup> BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

could prove to be difficult to both navigate and enforce. A strong national data privacy standard will provide consumers and businesses the certainty they deserve. It should address three key issues:

- **Establish Consumer Rights.** A federal privacy law should create new rights for consumers, including the rights to access, correct, and delete their personal data, as well as the right to opt out of the sale and sharing of their personal information. These rights can help provide consumers control over their information and increase their ability to both trust and verify how their data is used.
- **Create Clear Obligations for Businesses to Handle Data Responsibly.** A federal privacy law should place meaningful limits on businesses that handle consumers' personal data and require them to handle consumers' data responsibly. Those limits should also reflect a business's role in handling consumer data, including whether a company decides why and how to collect a consumer's personal data, or instead acts as a service provider that processes a consumer's data on behalf of another company and pursuant to that company's instructions. The distinction between these two types of companies is critical to a host of privacy laws worldwide and in newly enacted state laws. These laws recognize that both types of businesses have important responsibilities and obligations to safeguard consumers' personal data and that those obligations must reflect how the company interacts with consumers' data to avoid creating new privacy and security risks for consumers.<sup>2</sup>
- **Provide Strong and Consistent Enforcement.** Effective enforcement is important to protecting consumers' privacy, ensuring that organizations meet their commitments and legal obligations, and deterring potential violations. A federal privacy law should not be enforced by a single regulator, but by federal and state agencies working together. We support enforcement of a federal privacy law not only by the FTC but also all state Attorneys General, to create consistent and effective enforcement.

The APRA discussion draft recently released by Chairs McMorris Rodgers and Cantwell makes notable bipartisan progress on the above key issues, but there is still significant work to be done to ensure the final product is effective, workable, and functions as intended. To achieve such an outcome, we urge you to increase clarity by further defining key terms and to make the following revisions:

- **Develop and refine the bill's approach to minimizing the risk of bias in AI systems.** BSA strongly agrees that when AI is used in ways that could adversely impact civil rights or access to important life opportunities, the public should be assured that such systems have been thoroughly vetted to identify and mitigate risks associated with unintended bias. BSA has worked with member companies for several years on AI issues and we appreciate that Section 13(b) of the APRA focuses on requiring impact assessments and design evaluations for certain AI systems. However, key improvements are needed to ensure these provisions are effective and workable, including providing clear thresholds and ensuring that obligations fit the organization's role.
- **Revise the data minimization provisions to provide appropriate grounds for processing and avoid undermining the role of service providers.** The APRA

---

<sup>2</sup> See BSA, Controllers and Processors: A Longstanding Distinction in Privacy, *available at* <https://www.bsa.org/files/policy-filings/10122022controllerprodinction.pdf>.

aims to require companies to minimize the amount of data they process. This is an important principle of privacy laws globally. However, legislation should permit the type of processing that a consumer would expect, such as improving a product or service. It is also important that the minimization requirement not inadvertently lead to *more* parties looking at personal data, such as by requiring a service provider to review its customer's data.

- **Further clarify the role and responsibilities of service providers.** We welcome the bill's recognition of the distinct roles of covered entities and service providers, and we strongly support defining these terms in line with the globally-recognized definitions of controllers and processors, as APRA does. However, APRA undercuts the longstanding and widespread distinction between these two roles by applying obligations designed for covered entities to service providers. As a result, some obligations are not appropriate to the role of service providers and do not align with how the services they provide function.

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these recommendations for improving the recently released APRA discussion draft. We look forward to working with lawmakers to ensure that any privacy legislation is effective, workable, and provides consumers and businesses with the certainty they deserve. We welcome and look forward to further engagement with the Committee on these important issues.

**Sincerely,**



Craig Albright  
Vice President, US Government Relations

CC:  
The Honorable Cathy McMorris Rodgers  
The Honorable Frank Pallone