



June 26, 2024

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

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

RE: Concerns with the latest draft of the American Privacy Rights Act

Dear Chair Rodgers and Ranking Member Pallone:

Our respective organizations represent the leading providers of security, life safety and identity products and systems integration for government programs, commercial customers, and consumers throughout the United States.

We write to express concerns with certain significant changes to the draft American Privacy Rights Act (APRA) scheduled to be considered by the Committee on June 27. Despite no realistic opportunity provided for stakeholder review or feedback, these changes to APRA include reversals of longstanding policy elements from its predecessor. This includes but is not limited to the following:

Biometric Information

Under the current draft, data minimization requirements in subsection 102 (c) were amended to remove previously referenced permissible purposes for collection, processing, retention and transfer of biometric information. This would have the effect of outright prohibiting use of important technology applications for security and fraud prevention and imposing a deeply flawed model from the 2008 Illinois Biometric Information Protection Act (BIPA) nationwide.

For example, the long-term retention of such data to prevent identity theft or for other anti-fraud purposes would no longer be permitted. Also prohibited would be security technologies used daily through the rest of the U.S. by many top 100 retailers and small businesses that have emerged as key tools to fight organized retail crime and prevent associated violence. Over the last two years, more than 1,100 customers, employees, and security personnel have been killed by criminals in retail settings.¹ The human cost extends far beyond these victims, as revenue generated from organized retail theft fuels drug smuggling, human trafficking, and other criminal enterprises. And, without needed exceptions for APRAs permissible purposes for collection and processing of information, the changes will also likely interfere with use of access control systems and other voluntary authentication systems that must distinguish between enrolled and non-enrolled individuals.

¹ Analysis of data and reports from Downing & Downing, Inc, see <http://d-ddaily.com/archivesdaily/2023-Q4-Fatalities-Report.htm>.

Additionally, new affirmative consent procedural requirements are added for biometric information regarding data retention – despite that this would already be addressed in required privacy notices – which adds an onerous and unnecessary layer of complexity and compliance. This would make voluntary applications of biometric technology even more difficult to implement and is sure to invite abusive litigation under APRA's private right of action concerning the form, methods, scope or content of consent.

Such lawsuits under BIPA in Illinois foretell what would result nationwide.² Today there are many biometrically enabled products or services that suppliers do not provide to Illinois businesses and consumers due to BIPA requirements, its ambiguity or the litigation risk, cutting off their access to effective technologies for home and building security, workplace safety, security investigations and emergency response.

Applicability to Government Contractors

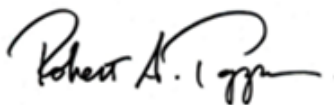
In yet another example of a significant reversal, the definition of “service provider” was amended to include government contractors acting on behalf of government entities, which were previously outside of the bill's scope. This has enormous potential for disruption of federal agency mission capabilities, public safety, including school safety, and other state and local government entity operations. Contractors may no longer be able to process information as needed due to APRA' obligations or may become bogged down with translating compliance requirements that were designed to address activity outside the public sector.

Conclusion

We continue to believe that a national data privacy standard could provide tremendous benefits if it applies clear, workable and uniform rules nationwide, and we support your work directed at achieving this objective. However, as these and other issues in the current draft of APRA under consideration will have serious negative impacts on businesses and consumers, we cannot support the measure as currently written. That said, SIA, IBIA, and our members stand ready to assist you and your colleagues as work continues on APRA. Thank you for your consideration.



Don Erickson
CEO
Security Industry Association
www.securityindustry.org



Robert Tappan
Managing Director
International Biometrics + Identity
Association
www.ibia.org

cc: Members of the House Committee on Energy and Commerce

² <https://progresschamber.org/wp-content/uploads/2023/03/Who-Benefits-from-BIPA-Analysis-of-Cases-Under-IL-Biometrics-Law.pdf>