Statement of Jake Parker
Senior Director of Government Relations
Security Industry Association

Before the

Committee on Commerce, Science and Transportation
Subcommittee on Consumer Protection, Product Safety and Data Security

United States Senate

"Strengthening Data Security to Protect Consumers"

May 8, 2024

Committee Hearing Room, Russell 253

Chairman Hickenlooper, Ranking Member Blackburn and distinguished members of the Committee, my name is Jake Parker, Senior Director of Government Relations for the Security Industry Association (SIA). SIA is a nonprofit trade association representing more than 1,500 companies that provide safety and security products essential to protecting lives, property, businesses, schools, and critical infrastructure throughout the U.S. and employ thousands of technology leaders.

Best Practices and Commitment of the Security Industry to Data Protection

Data security is essential to the delivery and operation of security systems and services. SIA members are committed to protecting personal data, whether it is consumer or operational data. Through our Data Privacy Advisory Board[1] and Cybersecurity Advisory Board,[2] SIA is encouraging members to implement best practices for data security by providing resources like our *Privacy Code of Conduct,*[3] *Ten Tips for Implementing Data Privacy,*[4] *How to Counter AI-Driven Cybersecurity Threats to Physical Security Products,*[5] and enterprise security risk management (ESRM) strategies for our industry.[6]

It is critical to provide our customers with tools and strategies that address risks both inside and outside their organizations. Data minimization – in the operational sense – is important to the secure implementation of key security products like access control and video security systems. Across many applications, privacy-by-design also enhances end-to-end security. Features like strict permissions-based data access, de-centralized data storage, encryption of data in transit/at rest, customer-only access to cloud-hosted data, "edge" device processing, user audit capabilities and data retention schedules all serve to enhance privacy and security by limiting the availability of data for potential misuse and limiting the usefulness of data if it is compromised. Our members provide technology for multi-factor authentication and high assurance identity authentication, including remote identity proofing services that are essential to meeting today's (and tomorrow's) identity theft and fraud prevention needs. And in emergency communications applications, our members are the first to raise the alarm in an emergency, using the right data to help law enforcement and other first responders get to where they need to be as quickly as possible.

Key Role of Authentication Technologies in Data Security

Technology innovations are playing a key role in enhancing data security. Biometric technologies are a good example as they are becoming increasingly important for many types of secure transactions. When provided as an option to consumers to authenticate identity for example, these technologies provide more convenience and additional data security at the same time. Biometric technologies offer faster and higher-assurance authentication while reducing the transfer or exposure of personal information that is

[1] https://www.securityindustry.org/committee/data-privacy-advisory-board/
[2] https://www.securityindustry.org/committee/cybersecurity-advisory-board/
[3] https://www.securityindustry.org/report/sia-privacy-code-of-conduct/
[4] https://www.securityindustry.org/report/ten-tips-for-implementing-data-privacy/
[5] https://www.securityindustry.org/2023/10/05/how-to-counter-ai-driven-cybersecurity-threats-to-physical-security-products/
[6] See *Security Convergence 2024*, https://www.securityindustry.org/wp-content/uploads/2024/02/SIA-Security-Convergence-2024.pdf

more vulnerable to exploitation. In fact, there is natural cryptography for biometric data that prevents identity hacking even if that data is stolen, and naturally serves to limit unauthorized use by third parties. It is far less vulnerable than information like social security numbers and passwords, that is easily exploited by identity thieves and cyber-attackers.

Biometric software creates a numerical "template" based on an individual's physical characteristics to compare with a template or templates already enrolled in a database or on a device. This numerical string of data (based on "mathematical vectors") is created and readable only within that specific software. Contrary to a common misunderstanding that such data is unchangeable and more vulnerable, this data is in fact infinitely "changeable," both software version to software version and in that templates will be slightly different each time they are created by the software (due to varying positions of a finger placed on a sensor or varying photography conditions for example). Templates are then "matched" based on mathematical similarity with the enrolled information.

A biometric template itself does not contain any personally identifiable information, and it is unusable outside of the software system that created it. Importantly, a template cannot be used to re-create the image (of a fingerprint, face, etc.) or physiological feature that it was derived from. Since each provider uses a different process to create and compare templates unique to that proprietary system, a template created in one system cannot be used in another. While such data would be useless if sold or shared, its collection, storage and processing should optimize privacy and security using encryption and other best practices in securing sensitive information.

Importance of Uniform Data Privacy Rules in Enhancing Data Security

We are following with interest recent renewed discussions in Congress regarding the development of a federal data privacy standard that would bolster data security through data minimization among other elements. Such a standard could potentially provide tremendous benefits if it applies clear, workable and uniform rules that are predictable for both businesses and consumers. We believe any national standard must ensure the continued functionality and effectiveness of safety and security technology applications and the benefits to society. This means ensuring data can be collected and processed as needed for these purposes, as well as ensuring requirements do not inadvertently create new security risks.

Uniformity is essential. Express preemption of all state and local laws related to data privacy and security that is iron-clad against challenge in court is necessary to avoid the potential for adding layer upon layer of complex requirements. Recent legislation in Colorado is just one example of layering that could continue to occur without strong preemption. Despite the Colorado Privacy Act having just become effective in July 2023, the legislature recently passed a measure[7] imposing an extra layer of different requirements specifically for biometric data despite existing regulation of this data under the CPA. The measure dramatically expands applicability both to small businesses and to employee data, which had previously been out of scope under the CPA. The potential increasing complexity of such state-by-state rules covering an ever-expanding set of data and number of entities that must comply is likely to cause confusion and slow business decisions both locally and nationally. The same goes for

[7] https://leg.colorado.gov/bills/hb24-1130

potential non-preemption of state and local laws providing a private right of action to enforce data privacy and security requirements.

A national data privacy law should limit the potential for abusive lawsuits by plaintiffs' attorneys seeking "sue-and-settle" outcomes, as the applicability to nearly all sectors of the economy could provide an irresistible target. We have seen the impact firsthand under the deeply flawed Illinois Biometric Information Protection Act (BIPA) where such lawsuits have been filed against many of our members and their customers in Illinois, even though no actual consumer harm is alleged. 88% of the cases have been related to biometric timekeeping processes for hourly employees to clock in to work, but many others have involved security and identity verification services.[8] As a result, today there are many industry products that suppliers refuse to provide to Illinois businesses and consumers due to the litigation risk, despite wide availability elsewhere, cutting off access to effective technologies for home and building security, workplace safety, security investigations and emergency response.

Any national standard should also limit the potential for layers of conflicting requirements and/or frivolous litigation stemming from local jurisdictions enacting their own data privacy laws. For example, the latest class action lawsuit under the City of New York's 2021 Biometric Identifier Information Law,[9] a major retailer is being sued over allegations it is "profiting from" data in violation of the measure, simply due to use of security systems to protect employees and customers, and limit victimization by organized retail crime gangs.[10] And, during the City of Baltimore's 18-month ban on use of certain biometric technologies by businesses that ended in 2022, a popular rideshare service was forced to discontinue its remote authentication of drivers in the area, with potential impact to rider safety. Again, such issues can be addressed by full and uniform state and local preemption.

Conclusion

On behalf of SIA, I appreciate the opportunity to provide collective input from our industry on the important matter of data security. We are committed to working in partnership with Members of Congress in addressing related areas of public policy. I will do my best to answer any questions you may have. However, if there is any information requested that I cannot provide today, I will be happy to work with our members to provide helpful information.

[8] https://progresschamber.org/wp-content/uploads/2023/03/Who-Benefits-from-BIPA-Analysis-of-Cases-Under-IL-Biometrics-Law.pdf
[9] https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCadmin/0-0-0-42626
[10] https://findbiometrics.com/t-mobile-profited-from-biometric-security-by-preventing-theft-lawsuit-alleges/