STATE PRIVACY & SECURITY COALITION

January 30, 2024

Chair Mike Weissman
Vice Chair Jennifer Bacon
200 E Colfax
RM 307
Denver, CO 80203

Re: CO HB24-1058 (Neural Data)

Dear Chair Weissman, Vice Chair Bacon, and Members of the Committee,

The State Privacy & Security Coalition, a coalition of over 30 companies and six trade associations in the telecom, technology, retail, payment card, and automobile sectors, writes in the hope of aligning the text of HB24-1058 more closely with the intent of the bill – to protect consumer biological data and neural data by establishing strict controls on the entities that collect such data.

The bill as drafted suffers from overbroad definitions. The proposed characterization of "biological data" would include data that may not be appropriately deemed sensitive. We recommend adopting the approach in the Colorado Privacy Act for genetic and biometric data, specifically that such data is considered sensitive only when processed "for the purpose of uniquely identifying an individual" (see C.R.S. 6-1-1303(24)(b)). It is logical to classify biological data as sensitive when utilized for the unique identification of an individual. However, if the data is not employed for this purpose, there is no justification for labeling it as sensitive.

We are similarly troubled by the current breadth of the "neural data" definition. Particularly, we would recommend eliminating the phrase "generated by the measurement" in reference to both the central nervous system and the peripheral nervous system because this language would relate to ***all bodily activities***. When considering speech, for instance, the central nervous system, specifically the brain, generates signals sent to the peripheral nervous system for action execution. Consequently, the existing draft's wide-ranging scope would encompass virtually any measurable and observable human behavior as "information generated by the measurement" of the peripheral nervous system. This expansive interpretation could lead to the classification of data related to keystrokes, mouse movements, and clicks as sensitive personal information.

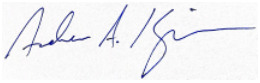
We respectfully recommend refining the scope of the “biological data” definition and “neural data” definition to align with the bill’s intended purpose. Our recommendations are as follows:

- “Biological data” means data derived from direct measurements of an individual’s biological, genetic, biochemical, physiological, or neural properties, that are used to uniquely identify an individual. “Biological data” includes neural data.
- “Neural data” means information obtained from direct measurements of neural activity of an individual’s central nervous system, including the brain and spinal cord, and processed by or with the assistance of a device.”

STATE PRIVACY & SECURITY COALITION

We would be happy to answer any questions and welcome discussions with you, your staff, and other stakeholders on this bill as it moves forward.

Respectfully submitted,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition

March 20, 2024

Chair, Mike Weissman
Vice Chair, Jennifer Bacon
200 E Colfax
RM 307
Denver, CO 80203

RE: HB 24-1058 - Biometric Data
Position: Amend

Chair Weissman:

The Alliance for Automotive Innovation (Auto Innovators) is writing to inform you of **our request to amend HB 24-1058,** which expands the scope of sensitive data under the Colorado Privacy Act to include certain types of biological and neural data.

From the manufacturers producing most vehicles sold in the U.S. to autonomous vehicle innovators to equipment suppliers, battery producers and semiconductor makers – the Alliance for Automotive Innovation represents the full auto industry, a sector supporting 10 million American jobs and five percent of the economy.

Maintaining Consumer Privacy and Cybersecurity
The protection of consumer personal information is a priority for the automotive industry. Through the development of the "Consumer Privacy Protection Principles for Vehicle Technologies and Services," Auto Innovators' members committed to take steps to protect the personal data generated by their vehicles. These Privacy Principles provide heightened protection for certain types of sensitive data, including biometric data.[1] Consumer trust is essential to the success of vehicle technologies and services. Auto Innovators and our members understand that consumers want to know how these vehicle technologies and services can deliver benefits to them while respecting their privacy. Our members are committed to providing all their customers with a high level of protection of their personal data and maintaining their trust.

Unique Considerations for Vehicle Safety Technology
Auto Innovators' members invest heavily in research and development to design and implement state-of-the-art safety systems to protect our consumers. Among those safety systems is the use of different types of driver monitoring systems, which use in-vehicle cameras and sensors to detect if a driver is inattentive, fatigued, intoxicated, or experiencing a medical emergency.

[1] https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf

1050 K Street, NW
Suite 650
Washington, DC 20001

AutosInnovate.org

These technologies are just a snapshot of how automakers utilize technology to equip cars with advanced safety features. These, and other safety systems, help ensure not only the safety of the driver, but the safety of their passengers and other roadway users.

HB24-1058, and the addition of “neural data” to the definition of sensitive data under the Colorado Privacy Act, could raise unique challenges for the auto industry and jeopardize the use of these safety systems. As written, automakers could be required to obtain affirmative consent to collect data critical to the use of these safety systems.

In other words, this bill could be interpreted to allow drivers to opt out of the use of in-vehicle safety systems that would alert the driver or safety disable the vehicle if they cannot or should not be operating the vehicle. This puts not only the driver of the vehicle at risk, but also other road users.

Furthering our concerns on this issue, last month the National Highway Traffic Safety Administration (NHTSA) announced an Advance Notice of Proposed Rulemaking that may lead to a final rule requiring alcohol-impairment detection technology in all new passenger vehicles[2]. The detection technology is a requirement of a provision from the 2021 Bipartisan Infrastructure law.

Since the rulemaking process is only recently underway, it remains to be determined what type of technology may be used to fulfill the requirement, but potential options include a breath test, light technology that scans under a driver’s fingers to detect impairment, or cameras and sensors that collectively determine if a driver can legally operate a vehicle. Once again, the requirements in HB24-1058 could be directly at odds with these and other vehicle safety systems by allowing drivers to opt-out of the use of these systems.

While we do not believe this legislation was intended to interfere with these safety sensitive systems, both those currently installed on new vehicles and those that could be forthcoming, it’s a potentially critical unintended consequence that could put the safety of drivers, passengers, pedestrians, and other roadway users at risk if HB24-1058 passes in current form. This issue could be remedied by modifying the definition of "biological data " so that it explicitly excludes vehicle-generated data necessary for the operation of these safety technologies.

Thank you for your consideration of the Auto Innovators’ position. Please don’t hesitate to reach out if there are any questions or additional recommendations that we can provide.

Sincerely,

Nick Steingart
Director, State Affairs

---

[2] https://www.nhtsa.gov/sites/nhtsa.gov/files/2023-12/anprm-advanced-impaired-driving-prevention-technology-2127-AM50-web-version-12-12-23.pdf

January 30, 2024

House Committee on Judiciary
Room 0112, Colorado State Capitol
200 East Colfax Avenue
Denver, CO 80203-1784

RE: HB 1058 "Protect Privacy of Biological Data" (Oppose unless amended)

Dear Chair Weissman and Members of the House Committee on Judiciary:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 1058.

CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For over 50 years, CCIA has promoted open markets, open systems, and open networks. The Association supports the enactment of comprehensive federal privacy legislation in order to promote a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights and responsibilities for organizations that collect data. A uniform federal approach to the protection of consumer privacy is necessary to ensure that businesses have regulatory certainty in meeting their compliance obligations and that consumers are able to understand and exercise their rights.

We appreciate, however, that in the absence of federal privacy protections, state lawmakers have a continued interest in enacting local legislation to guide businesses and protect consumers. As you know, Colorado is out in front of this effort as one of the growing number of states with a comprehensive consumer data privacy law. CCIA commends lawmakers in their thoughtful approach in enacting legislation that supports meaningful privacy protections while avoiding interference with the ability of businesses to meet their compliance obligations and the opportunity for consumers to benefit from the innovation that supports the modern economy.

CCIA strongly supports the protection of consumer data and understands that Colorado residents are rightfully concerned about the proper safeguarding of their biological and neural data. However, as currently written HB 1058 would encompass almost every wearable technology device, beyond those directly related to health applications, which could result in degraded consumer services and experience.

We appreciate the committee's consideration of our comments regarding several areas for potential improvement.

Align key definitions with privacy standards to promote regulatory interoperability and mitigate unnecessary compliance burdens.

By introducing a broad definition and compliance obligations relating to "biological data", which encompasses and includes a new definition for "neural data", HB 1058's scope extends

beyond the subject of "biometric" and "health" data as defined in other privacy laws, with multiple implications. To meet compliance requirements under a new privacy regime, businesses inevitably face logistical and financial challenges. Given the significant costs associated with developing privacy management systems, even minor statutory divergences between frameworks for definitions or the scope of compliance obligations, can create significant burdens for covered organizations.[1] HB 1058's definition of "neural data" includes "information that concerns the activity of an individual's central nervous system or peripheral nervous systems, including the brain and spinal cord, and that can be processed by or with the assistance of a device" and therefore would encompass "potential use" rather than "actual". As such, this definition should be more narrowly tailored to avoid unnecessary regulatory burdens, which may deter business from researching and developing solutions in healthcare and other important sectors. And, by extension, HB 1058 might result in Coloradoans being denied innovative products in the marketplace.

Sufficient time is needed to allow covered entities to understand and comply with newly established requirements.

HB 1058 fails to provide covered entities with a sufficient onramp to achieve compliance. A successful privacy framework should ensure that businesses have an appropriate and reasonable opportunity to clarify the measures that need to be taken to fully comply with new requirements. As you know, Colorado's recently enacted privacy law, along with those in California and Virginia included two-year delays in enforcement of those laws. CCIA therefore recommends amending the current effective date of 90 days following the adjournment of the Colorado General Assembly to a later date.

* * * * * *

We appreciate your consideration of these comments and stand ready to provide additional information as the legislature considers proposals related to technology policy.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association

[1] A study commissioned by the California Attorney General estimated that in-state companies faced $55 billion in initial compliance costs for meeting new privacy requirements, with small businesses facing disproportionately higher shares of costs. Berkeley Economic Advising and Research, LLC, "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations," (August, 2019), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

Name: Jameson Spivack
Title: Senior Policy Analyst
Organization: Future of Privacy Forum
Bill: HB24-1058: Protect Privacy of Biological Data
Committee: Judiciary
Position on Hearing Item: Neutral
Date: 1/30/24

Chair Weissman, distinguished members of the committee, thank you for the opportunity to present. My name is Jameson Spivack, representing the Future of Privacy Forum, and I am here to provide informational testimony about the privacy of body-based data, and neural data in particular. As such, I am neutral on House Bill 24-1058.

The Future of Privacy Forum is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies in the United States and globally. We seek to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective regulation. We have published multiple reports analyzing the privacy risks associated with the collection and use of biological and neural data, as well as best practices companies can adopt to protect users.

Colorado has played a leading role in protecting people's privacy, being the third state in the country to enact a comprehensive privacy law. As rapidly advancing technologies become integrated into our everyday lives, establishing guardrails for collecting and processing new categories of sensitive personal data becomes increasingly important. Emerging technologies like artificial intelligence, extended reality, smart devices, and neurotechnologies promise transformative improvements in healthcare, education, productivity, entertainment, and beyond. But these technologies rely on data about our bodies and behaviors, and without proper protections could raise serious risks to privacy and safety.

Data about our bodies is especially sensitive, as it can potentially reveal some of our most private information: health conditions, sexual orientation, race, religious beliefs, attitudes, personality, and interests. Neural data in particular could provide insight into what bioethicist Nita Farahany calls the "final frontier of human privacy"—the brain. Data from our brain and the rest of our nervous system is unconscious and involuntary, and critical to understanding how we interact with the world around us. It is core to who we are, and to the most intimate parts of our identities. Protecting this data is key not only to maintaining our dignity, but to preventing discriminatory or otherwise harmful decisions made on the basis of our sensitive data.

We appreciate this committee's attention to the risks associated with neural and body-based data. To ensure that regulations allow for emerging technologies' beneficial uses while effectively protecting against their privacy risks, we encourage the committee to consider the following:

1. The Colorado Privacy Act, like most privacy laws, provides heightened protections for data that is sensitive and identifiable. Clarifying that this identifiability standard also applies to biological and neural data could clear up confusion about the scope of covered data, and align the amendment with the underlying statute.
2. Similarly, definitional precision can clarify exactly what data types are covered, providing both companies and the general public with greater understanding of their rights and responsibilities. For example, under the current formulation of "biological data," information such as shoe size may be covered, even if not linked or linkable to an identified or identifiable individual. Being clear on the extent of "biological" and "neural" data would clear up confusion.
3. Finally, new regulations on biological data should align with existing law regarding biometric data, as well as any additional CPA amendments passed this session regarding biometric data.

Thank you for your time, and we look forward to providing any additional feedback or information you may need.