Colorado Common Cause
Holding Power Accountable

My name is Aly Belknap, Executive Director of Colorado Common Cause, a nonpartisan, nonprofit organization that has fought for the public interest in Colorado since 1971.

We urge the committee to vote yes on HB24-1130: Privacy of Biometric Identifiers & Data. Data privacy is a critical piece of having a secure, healthy democracy.

Corporations who use facial recognition software are soliciting, storing and using biometric data from their user bases, who are generally "along for the ride" as technology rapidly evolves and complex terms and conditions are thrown at them at a constant pace. Biometric data contains highly compromising information about an individual; it can range from their fingerprint, to an exact scan of their face, to their entire genetic code.

Once stored, this data can be easily mishandled: genetic testing company 23andMe stores genetic and ancestral information for millions of users, and in late 2023, the company confirmed that nearly 7 million profiles were accessed by a nefarious actor seeking to specifically target and expose Ashkenazi Jewish and Chinese genetic data. The hackers then sold the information for $1-$10 per profile. This bill's common-sense provision that specific biometric data be deleted within one year of customer interaction would mitigate future harm to Colorado consumers by taking away the blank check these corporations currently have to store and sell Coloradans' sensitive data indefinitely.

There is no reason, beyond profit incentive, for these corporations to sell or trade their user's biometric data. It does not benefit users, and in fact, opens them up to discrimination by insurance companies, security breaches into their personal accounts, and public exposure. We support this bill's provision to ban the sale and trade of user data, full stop.

Coloradans should have the right to know who is storing their data and have agency over the continued use of their data. This bill creates sensible, actionable solutions to this problem by requiring companies who do business in Colorado to gain consent from, inform more fully, and allow the withdrawal of consent from Colorado users they are soliciting for biometric data.

Colorado Common Cause sees HB24-1130 as an effective, urgent set of protective measures that will ultimately make our democracy stronger. We are now living in a world where nefarious actors, both foreign and domestic, are reaching for any tool in their toolbox to sow chaos in our elections, feed mistrust in our public officials, and pit communities against one another using misinformation. Biometric data is powerful tool for accomplishing these goals. We must act now limit access to Coloradans biometric data.

We urge the committee to vote yes on HB24-1130. Thank you for considering our arguments.

February 14, 2024

Representative Mike Weissman
Chair
House Judiciary Committee
Colorado General Assembly
Denver, CO 80203

Representative Jennifer Bacon
Ranking Member
House Judiciary Committee
Colorado General Assembly
Denver, CO 80203

Re: Security Industry Association concerns with HB24-1130, Privacy of Biometric Identifiers & Data

Dear Chair Wiessman, Ranking Member Bacon & Members of the Committee:

The Security Industry Association (SIA) is a nonprofit trade association representing more than 1,400 companies nationwide, including 32 headquartered in Colorado and many more providing products, services and jobs in the state. Our members provide a broad range of security and life safety products and services. Among them are the leading developers of biometric technologies used in a wide variety of government, commercial and consumer products, including products used to better protect lives, property and critical infrastructure, as well as bolster public safety.

Using biometric technology allows individuals to quickly and conveniently prove their identity to enter a venue, board a plane, perform online transactions, seamlessly access personalized experiences and for many other purposes. The use and popularity of such technologies are growing not only due to the convenience, speed and cost advantages they offer, but also because ***the process and data involved are more secure than traditional methods*** (explained below).

It's critical that advanced technologies – including biometrics – are used in a secure manner and only for purposes that are ethical, responsible and beneficial to individuals and society. We support polices that safeguard biometric data and other forms of personal data, like the existing Colorado Privacy Act (CPA), and believe any additional requirements should align with the data privacy framework established by the CPA and its implementing regulations.

Alignment with the Colorado Privacy Act Needed

We deeply appreciate the openness of the bill sponsors to stakeholder feedback prior to and after introduction of HB24-1130, however, more alignment needs to occur to avoid unnecessary compliance burdens, confusion and barriers to beneficial technology use in Colorado. We understand further changes to the bill are under consideration by the sponsors. However, the following are the needs we see based on the text of HB24-1130 as introduced:

1. Making applicability of the CPA's security/anti-fraud exceptions to new biometric data provisions explicitly clear in the text.

2. Fully ensuring that under the bill's definitions, photos and video (excluding derived data) cannot be misconstrued as biometric data under any circumstances.

3. Bringing consumer notice requirements, and data deletion, retention and access rights into closer alignment with current CPA regulations for sensitive data.

4. Full uniformity in using the CPA-defined term "processing," in lieu of "collection" throughout the bill ("Processing" already includes collection under the CPA).

5. Removing applicability to employee data. Consumer data is fundamentally different than employee data. The latter is outside the current scope of CPA and already protected under several federal laws. Including employee data in the bill would vastly increase the number and types of businesses subject to the CPA, and significantly burden small businesses. Further, the bill would outright prohibit employer collection and use of such data in blanket fashion (subject to limited exceptions) without justification.

   For example, under the bill businesses would not be permitted to require use of biometric authentication as a condition of employment under many scenarios even if it is needed for valid employee or consumer safety reasons. Such scenarios include, for example, remote biometric identity verification for ride-hailing service drivers prior to pickups (and related location tracking), or location tracking of employees that may be working alone in remote and/or in dangerous environments, which speeds needed responses to events. For such operations and unique circumstances, it may not be feasible to make use of biometric technology by employees optional.

Note on the Nature of Biometric Technologies and Related Data

Unfortunately, some concerns surrounding biometrics stem from misunderstandings regarding the nature and security of the data created and used in biometric technology applications. Biometric technology actually plays a key role in protecting privacy during transactions that require identity verification, by preventing exposure of personal information (date of birth, Social Security Number, address, etc.) that is far more vulnerable to compromise and abuse.

The misunderstandings stem from confusing the software-created data used in biometric technology applications with the physical or biological characteristics they compare. All biometric technologies create 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 by and readable only within that specific version of the software used. Such templates are 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 "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 that created it. It cannot be used for identification unless it is linked to an identity within that system. Importantly, a template cannot be used to re-create the image (of a fingerprint, face, etc.) or physical feature that it was derived from. 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. In this way, the use of templates acts as natural cryptography for biometric data, preventing identity hacking even if that data is stolen, and naturally serves to limit unauthorized use by third parties. 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 protecting other types of sensitive information.

Conclusion

We are concerned that as drafted, HB24-1130 will lead to confusion about what data is covered and what rules apply under different circumstances. It would also apply a more complex compliance architecture for biometric data than for other types of sensitive data, which is unnecessary and contrary to the CPA. Without further changes, the proposed bill could hamstring commercial use of biometric technologies in Colorado, harm companies developing related products in the state, and discourage the sale of innovative products that benefit consumers.

We urge the Committee not to approve the bill without further changes needed to bring the measure into alignment with the CPA, and we stand ready to continue to work with the sponsors and the committee to help achieve workable policies that safeguard biometric information.

Respectfully,

Jake Parker
Senior Director, Government Relations
Security Industry Association
jparker@securityindustry.org
www.securityindustry.org

STATE PRIVACY & SECURITY COALITION

February 14, 2024

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

Re: HB24-1130 (Amend)

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

The State Privacy and Security Coalition, a coalition of over 30 companies in the retail, telecom, tech, automotive, and payment card sectors, as well as six trade associations, writes with concern about HB24-1130. As currently drafted, HB24-1130 does not align with the Colorado Protection Act (CPA) or its attendant regulations. While we acknowledge and appreciate the sponsors' consideration in not rushing the introduction of this bill, and their continued efforts to listen to stakeholder concerns, this bill would create duplicative and conflicting provisions that disregard the CPA and its attendant regulations.

Our members recognize the importance of consumer privacy and the heightened sensitivity of biometric data that is used to identify individuals. SPSC did not oppose the Colorado Privacy Act (CPA) and we greatly respect the work that the Attorney General's office put into crafting detailed and substantive regulations.

Simply put, the proponents of this bill used stock legislation that they have gotten filed in other states without making any effort to harmonize any of its requirements with existing law and regulations. The problems laid out below stem entirely from this singular fact. The CPA was negotiated over a two-year period, with another year spent by the Attorney General's Office soliciting stakeholder input and crafting detailed regulations. This bill ignores all of that work and attempts to overlay redundant and conflicting requirements onto a detailed and well-conceived statutory scheme.

The CPA established heightened protections for biometric data by designating it as "Sensitive Data," meaning that a business must obtain affirmative consent in order to collect such data. The CPA regulations added significant requirements for sensitive data by delineating exactly what that consent must consist of, requiring a periodic refresh of consent for continued permission to use the biometric data, and strongly disincentivizing the sale of biometric data. These are just a few of the many protections ***that are already existing law and that this legislation ignores.***

This legislation should not move forward because it ignores the existing provisions in the CPA and attendant regs in the following ways:

The Bill's Processor Requirements Deviate from Every Privacy Modern Privacy Framework

The proponents of the bill have added provisions that, except for consent requirements, would put the same requirements on processors as on controllers. This fundamentally contradicts the entire point of separating entities into "controllers" – the consumer-facing entities that collect the data from the consumer and decide how it is to be used – and "processors," which are the back-end entities that provide services to the controller.

No modern privacy framework places the same requirements on each role because it does not make sense to do so. Under the CPA, processors are subject to strict controls about how they can process data. They must assist controllers in responding to consumer rights requests such as the right to access or delete data, delete or return data to the controller at the end of their contract, and submit to audits at the controller's request to ensure compliance with their contractual requirements.

Leaving this provision in the bill would be deleterious to a strong compliance posture by the business community because it would force processors to take on roles that they are not suited for and with which they cannot comply.

The Bill's Retention Schedule Ignores the CPA and CPA Regulation Requirements

The bill sets forth retention schedule requirements for the permanent destruction of biometric identifiers, ignoring the fact that the CPA regulations set forth three separate scenarios that require either the deletion or cessation of processing of Biometric Data. The timeline in this legislation does not sync up with the requirements in the existing CPA or the CPA regulations.

"Right to Update" is Redundant with CPA's Right to Correct

The proponents of this bill claim that the Right to Update is a necessary right in order to allow individuals who have transitioned genders to let a controller know this. While this is certainly well-intentioned, it is not necessary because the CPA already includes a Right to Correct, which allows a consumer to correct personal data – including biometric data, if applicable.

The bill's language here also includes a requirement on how long a controller has to respond to such a right, yet even this timing requirement conflicts with the response times that were negotiated and set forth in the CPA.

"Right to Delete" is Redundant and Confusing

The bill makes a passing reference to a "verified request to delete" a consumer's biometric data. However, the CPA already contains a right to delete. It does not, however, use the term "verified request" but instead uses the term "authenticate," which it defines. Using the undefined term "verified request" creates confusion with the process already set forth in the CPA.

Additionally, the regulations set forth extensive requirements on how to effect the deletion right, and this bill's processes ignore those regulations here, as it does in so many other ways. As drafted the Right to Delete does not make sense in the context of the CPA and the regulations.

The Bill's Non-Discrimination Provisions Ignore with the CPA and the CPA Regs

HB 1130 attempts to set forth requirements for nondiscrimination, but the CPA already has language to this effect and HB 1130 makes no attempt to harmonize these requirements. Furthermore, the CPA regulations have detailed requirements and strong limits on how loyalty programs may be deployed, and HB 1130 ignores these requirements as well.

Additional Issues

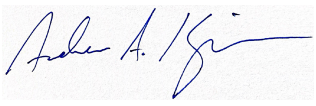
The aforementioned issues are major issues, but additional issues include:

- A lack of clarity on how this fits into the CPA, including how the CPA's exemptions and limitations apply to this section;
- A lack of cross-referencing to the data breach notification statute in Colorado, which already includes biometric data in its notification requirements;
- The inclusion of employee and employer requirements, when CO makes clear that the CPA and CPA regulations apply only to consumers, not to employees;
- A definition of "control" in the bill that conflicts with the definition set forth in the CPA; and
- The use of the terms "disclosure, redisclosure," and "dissemination" which are; undefined, and which are already covered by the CPA's broad definition of "sale," which covers ***any*** **exchange of data for** ***any*** **type of valuable consideration**.

We are aware of additional efforts in this legislative session to expand the CPA's scope for issues such as artificial intelligence and children's privacy. We believe that those offer potential solutions that can move privacy forward in Colorado. Because the CPA and the CPA regulations extensively regulate biometric data already, this bill is unnecessary.

We are more than willing to discuss our concerns further, and appreciate your consideration and time.

Respectfully submitted,



Andrew A. Kingman
General Counsel, State Privacy & Security Coalition

February 13, 2024

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

RE: HB 24-1130- Biometric Data
Position: Oppose

Chair Weissman:

The Alliance for Automotive Innovation (Auto Innovators) is writing to inform you of **our opposition and requests to amend HB 24-1130,** which amends the Colorado Privacy Act.

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.

Practical Concerns
While not a representative sample of all of our concerns with this legislation, a handful of practical concerns specific to the automotive industry are detailed below.

First, the current definition of "biometric identifier" is extremely broad and could capture several important safety-related technologies that are not used or intended to be used for the unique personal identification of an individual. For example, external-facing vehicle sensors

[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

that are integral to an Advanced Driver Assistance Systems or automated driving systems may be used to recognize that an object in the path of the vehicle is a pedestrian. In addition, internal-facing cameras may be used on some lower-level automated vehicle systems to detect driver misuse or disengagement. While these "images" are not used by an auto company to identify individuals, they are potentially captured by the definition of "biometric identifier."

This issue could be remedied by modifying the definition of "biometric identifier" so that it explicitly excludes images obtained by vehicle safety technologies. It could also be remedied by striking the references to "biometric identifiers" throughout and limiting the applicability of these provisions to "biometric data." Since "biometric data" is defined as information that is used to identify an individual (as opposed to information that can be used to identify an individual), it would presumably exclude the images captured by these vehicle safety technologies.

Second, while the requirement to have a written policy that lays out a retention schedule conforms with the industry's existing Privacy Principles, the requirement to destroy the information no later than one year after the company's last interaction seems somewhat arbitrary. A requirement to provide clear disclosure to consumers about how long such information will be maintained should be sufficient. Moreover, in practice, this requirement may prove challenging because, in the automotive case, manufacturers do not generally have visibility into who is driving or using a particular vehicle at a particular time and using vehicle technologies that may utilize biometric technology. In addition, manufacturers may not always know when a vehicle has been sold to another owner.

Third, privacy requirements of this nature require a standardized, nationwide approach so there is not a dizzying array of varied state requirements. Privacy protections regarding biometrics are being enforced by the Federal Trade Commission (FTC), and the Colorado Privacy Act and subsequent regulations already lay out requirements for sensitive data, including biometric data. The FTC has been the chief regulator for privacy and data security for decades, and its approach has been to use its authority under Section 5 of the FTC Act to encourage companies to implement strong privacy and data security practices. The auto industries "Privacy Principles" are enforceable under Section 5 of the FTC Act.

Thank you for considering Auto Innovators concerns and recommendations for this legislation, and please don't hesitate to reach out to me at nsteingart@autosinnovate.org if I can provide any further information.

Sincerely,

Nick Steingart
Director, State Affairs