STATE PRIVACY & SECURITY COALITION

March 26, 2024

Chair Julie Gonzales
Vice Dylan Roberts
Committee on Judiciary
Old Supreme Court
Denver, CO 80203

Re: HB24-1130 (Amend)

Dear Chair Gonzales, Vice Chair Roberts, 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 significant 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 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 regulations also require deletion of data when it is no longer used – and sets particular requirements on biometric identifiers and data when consent is outdated.

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 thoughtfully designed 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 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

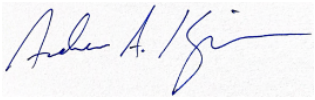
The aforementioned issues are major issues, but additional issues include:

- A lack of 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;
- The use of the terms "lease, trade, 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 proposes solutions to problems that don't exist while creating new problems of its own.

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

Thank you, Madame Chair, and esteemed members of the Committee. My name is Maggie Gómez, and I am the Colorado State Director with the State Innovation Exchange. We are a national research and strategy center that collaborates with state legislators to improve people's lives through transformative public policy. I am here in support of HB-1130, to increase protections for an individual's biometric data.

Biometric identifiers are our most personal, vulnerable, and unchangeable data. It makes us who we are and can be connected directly back to us for identification, tracking, or other purposes. This bill amends the Colorado Privacy Act to improve protections to this information that is increasingly at risk for exploitation or misuse and is especially timely. HB-1130 ensures that Coloradans know exactly what biometrics are being collected, for what reason, and for how long. At minimum, people deserve to know exactly who companies are sharing their biometric identifiers with and why, and should have the right to give affirmative consent for the collection of their biometric information. No corporation or government should be able to have nearly unlimited power to collect, store, buy or sell huge data sets of this highly sensitive information, and this bill makes it illegal to buy or sell this data.

The technology that makes all this possible is not slowing down or going away. That's why 1130 is so timely. Consumers deserve to use the technologies they want while knowing and trusting that their most vulnerable data is kept safe. Innovation is necessary to progress, and privacy is paramount in keeping public trust in innovation to move us all forward together. That is why this bill requires businesses to delete a person's biometric data one year after an individual last interacted with the company, or upon the person's request. Keeping this information indefinitely presents grave security risks and unforeseen consequences. We can't predict how this sensitive data will be handled in the future, but we can protect Coloradans now from the harms we already understand.

Thank you for your time and I respectfully ask for your support on HB1130.

My name is Andrew Barton, the Programs & Engagement Manager for Colorado Common Cause, a nonpartisan, nonprofit organization that works for open, honest, and accountable government and fights for the public interest.

We urge the you to vote yes on HB-1130.

In our increasingly digital world, data privacy is necessary to a secure and healthy democracy.

Corporations that use facial recognition and genetic testing software are soliciting, storing, and using biometric data from their user bases who are often "along for the ride" as the technology and uses for user data rapidly evolve. Biometric data fundamentally contains highly compromising information about an individual, ranging from their fingerprints to exact scans of their face, to genetic indicators of health issues and their entire genetic code.

Once stored, it is easy for data to be mishandled and protected by inadequate data security. The genetic testing company 23andMe stores the genetic data of millions of users, and in 2023, the company confirmed that nearly 7 million profiles had been accessed by a nefarious actor seeking to specifically target and expose Ashkenazi Jewish and Chinese customers' genetic data, selling the profiles' information. 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 businesses currently have to indefinitely store and sell the sensitive data of Coloradans.

There is no reason, beyond profit incentive, for these businesses to sell or trade user biometric data. It does not benefit users, rather it exposes users to discrimination by insurance companies, security breaches of their accounts, and public leaks of personal, identifiable information. We support the provision in this bill to ban the sale and trade of user data, full stop.

Coloradans should have the right to know exactly 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 that they're soliciting biometric data from.

Colorado Common Cause sees HB24-1130 as an effective and urgent set of protective measures to ultimately make our democracy and civic society stronger. We are now in a world where nefarious actors, both foreign and domestic, are increasingly using digital tools to foster mistrust in public officials and institutions, pit communities against one another using misinformation, and undermine our elections. As it can reveal a great deal of personal, identifiable, and behavioral information, biometric data is an extremely powerful tool for accomplishing these goals. We must act now to put guardrails around who can access the biometric data of Coloradans, what data they can access, and for how long.

We urge the committee to vote yes on HB24-1130.

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

March 27, 2024

The Honorable Julie Gonzales, Senate Chair
Colorado General Assembly
Judiciary Committee
200 E Colfax Avenue
Denver, CO 80203

Dear Chair Gonzales and Members of the Committee:

EPIC writes in support of HB24-1130, Privacy of Biometric Identifiers & Data. Biometric data is highly sensitive. A person's biometric data is linked to that person's dignity, autonomy, safety, and identity.[1] Unlike a password or account number, a person's biometrics cannot be changed if they are compromised. HB24-1130 would protect Coloradans by requiring that the use and retention of biometric data is minimized, and that data is kept secure.

The Electronic Privacy Information Center (EPIC) is a public interest research center established thirty years ago to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has long advocated for strict limits on the collection and use of biometric data.[3]

HB24-1130 is modeled after the Illinois Biometric Information Privacy Act (BIPA).[4] Passed in 2008, BIPA has been referred to as one of the most effective and important privacy laws in America.[5] BIPA and HB24-1130 set out a simple privacy framework: businesses may not sell, lease, trade, or otherwise profit from a person's biometric information; businesses must comply with specific collection, retention and deletion guidelines; and companies must use a reasonable standard of care in transmitting, storing, and protecting biometric information.

[1] Woodrow Hartzog, *Facial Recognition Is the Perfect Tool for Oppression*, Medium (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.
[2] EPIC, *About EPIC*, https://epic.org/about/.
[3] See e.g. Brief for EPIC as Amici Curiae, *Patel v. Facebook*., 932 F.3d 1264 (9th Cir. 2019), https://epic.org/amicus/bipa/patel-v-facebook/;
Brief for EPIC as Amici Curiae, *Rosenbach v. Six Flags Entm't Corp.*, 2017 Ill. App. 2d 170317 (Ill. 2019), https://epic.org/amicus/bipa/rosenbach/; Comments of EPIC to the Dept. of Homeland Security, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 F.R. 56338, 4 (Oct. 13, 2020), https://epic.org/apa/comments/EPIC-DHS- BiometricNPRM-Oct2020.pdf.
[4] 740 Ill. Comp. State. Ann. 14/15.
[5] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), https://ssrn.com/abstract=3722053.

Other critical provisions of HB24-1130 include:

- **Application to all biometric identifiers regardless of whether it is affirmatively used to identify an individual.** Biometric data should include information that could be used to confirm the unique identification of a consumer rather than limited to data that is affirmatively used to do so. However, the definition of biometric data used in the Colorado Data Privacy Act regulations is limited to biometric identifiers that "are used, or are intended to be used […] for identification purposes."[6] HB24-1130 rightly applies to biometric identifiers regardless of whether they are intended to be used to identify an individual. A fingerprint or faceprint is very sensitive data, whether it will be used to identify the individual yet or not.

- **Expansion of rights over biometric data to the workplace.** Increasingly, employers are using biometrics not just for time logging, but in hiring and to monitor employees by scanning faces to "determine" individual's emotions.[7] At a minimum, employees and prospective employees should know when their biometrics are being collected and how they are being used.

- **Prohibits the sale of biometric data.** This bill allows for the transfer of biometric data to processors who are operating under a contract with the company who collected the biometric information, but it does not allow the sale of biometric data. Our personal data is routinely bought and sold by data brokers, at which point the individual loses control of their data completely.[8] EPIC believes this practice should be banned outright, but because of the sensitivity and security threat posed by the improper storage of biometrics, it certainly needs to be prohibited for biometric data at a minimum. HB24-1130 rightly prohibits the sale of biometric data.

Conclusion

An individual's ability to control access to their identity, including determining when to reveal it, is an essential aspect of personal security and privacy. The unregulated collection and use of biometrics threatens that right to privacy and puts individuals' identities at risk. We urge the Committee to vote yes on HB24-1130.

If EPIC can be of any assistance to the Committee, please contact EPIC Deputy Director Caitriona Fitzgerald at fitzgerald@epic.org.

Sincerely,

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Deputy Director

[6] 4 Colo. Code Regs. §904-3, 2.02.
[7] Rachel Metz, There's a new obstacle to landing a job after college: Getting approved by AI, CNN (Jan. 15, 2020), https://edition.cnn.com/2020/01/15/tech/ai-job-interview/index.html.
[8] *See generally* EPIC, *Data Brokers*, https://epic.org/issues/consumer-privacy/data-brokers/.