# Colorado Expands Protections for Biometric Information under the Colorado Privacy Act

By Joseph J. Lazzarotti on June 4, 2024

When Colorado enacted the **Colorado Privacy Act** (CPA), it included "biometric data that may be processed for the purpose of uniquely identifying an individual." However, the CPA as originally drafted did not cover the personal data of individuals acting in a commercial or employment context. Last week, Colorado amended the CPA to broaden the protections for biometric data when Gov. Jared Polis signed **HB-1130** into law.

**Application of the CPA Biometric Amendment.** Importantly, HB-1130 alters the scope of the CPA's application. Recall that under the CPA, a controller is subject to the CPA if it:

> *(i) determines the purposes and means of processing personal data, (ii) conducts business in Colorado or produces or delivers commercial products or services intentionally targeted to residents of the state, and (iii) either: (a) controls or processes the personal data of more than 100,000 Colorado residents per year or (b) derives revenue from selling the personal data of more than 25,000 Colorado residents.*

HB-1130 adds that a controller can be subject to the CPA without meeting the requirements above, provided that it would be subject to the CPA solely to the extent that it controls or processes any amount of biometric identifiers or biometric data.

**Key Definitions.** The amendment added language expressly applicable to employers, including defining employees to include not only individuals employed on a full or part time basis, but also individuals who are "on-call" or hired as a "contractor, subcontractor, intern, or fellow." The amendment also adds definitions for biometric data and biometric identifier,

*"Biometric data" means one or more biometric identifiers that are used or intended to be used, singly or in combination with each other or with other personal data, for identification purposes. "Biometric data" does not include the following unless the biometric data is used for identification purposes: (i) a digital or physical photograph; (ii) an audio or voice recording; or (iii) any data generated from a digital or physical photograph or an audio or video recording.*

*"Biometric identifier" means data generated by the technological processing, measurement, or analysis of a consumer's biological, physical, or behavioral characteristics, which data can be processed for the purpose of uniquely identifying an individual. "Biometric identifier" includes: (a) a fingerprint; (b) a voiceprint; (c) a scan or record of an eye retina or iris; (d) a facial map, facial geometry, or facial template; or (e) other unique biological, physical, or behavioral patterns or characteristics.*

While there are some similarities in these definitions to the corresponding definitions in the popular **Illinois Biometric Information Privacy Act** (BIPA), there are some significant differences. One is that a biometric identifier under the BIPA is defined as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." The Illinois law does not make reference to "other unique biological, physical, or behavioral patterns or characteristics." There is also not a private right of action for violations of the CPA amendment, as there is in the BIPA.

**Requirements**. HB-1130 establishes several requirements for controllers that control or process one or more biometric identifiers. These requirements include:

- Obtaining consent from the consumer (including the employee) before collecting the consumer's biometric data.
- A written policy that
    - Establishes a retention schedule for biometric identifiers and biometric information,
    - Includes a process for responding to the data security incident that would compromise the security of biometric identifiers or biometric information. This would include the process for notifying consumers under the state's existing data breach notification law.

    - Establishes guidelines addressing the deletion biometric identifiers within certain time frames.
- Subject to certain exceptions, controllers must make the written policy available to the public. One exception is for a policy applying only to current employees of the controller.
- Providing a reasonably accessible, clear, and meaning privacy notice satisfying specific content requirements including the purposes for processing.
- Satisfying certain rights the consumer may have with respect to their biometric data, including the right to access.

HB-1130 also prohibits controllers from certain activities concerning biometric identifiers such as:

- Selling, leasing or trading such information,
- Disclosing biometric identifiers, subject to limited exceptions including consent and complying with federal or state law.
- Refusing to provide a good or service to a consumer, based on the consumer's refusal to consent to the controller's collection, use, disclosure, etc. of a biometric identifier unless same is necessary to provide the good or service.

Controllers and processors also must use a reasonable standard of care when storing, transmitting, and protecting biometric identifiers from disclosure.

**Employment provisions**. HB-1130 includes certain specific provisions for employers. While the law provides that employers may require current or prospective employees to allow the employer to collect and process their biometric identifiers, they may do so only to

- Permit access to secure physical locations and secure electronic hardware and software applications (but not obtain consent to retain such data for current employee location tracking or tracking time using a hardware or software application),
- Record the commencement and conclusion of the employee's full workday, including meal breaks and rest breaks in excess of 30 minutes,
- Improve or monitor workplace safety or security or ensure the safety or security of employees,

- Improve or monitor the safety or security of the public in the event of an emergency or crisis situation.

Collecting or processing biometric identifiers for other purposes will require consent which satisfied the applicable CPA requirements. However, employers will be able to collect and process biometric identifiers where the anticipated uses are "aligned with the reasonable expectations" of an employee based on the employee's job description or role, or a prospective employee based on reasonable background check, application or identification requirements.

Organizations that collect and process information that could be considered biometric identifiers or biometric data in various jurisdiction around the country will need to do a detailed analysis of the growing privacy and cybersecurity obligations, including incident response requirements. For assistance with that, please see our **biometric law map**.