BCLP. Client Intelligent

Insights

COLORADO'S NEW REQUIREMENTS FOR BIOMETRIC DATA: WHAT BUSINESSES NEED TO KNOW

Jan 09, 2025

On December 6, 2024, the Colorado Attorney General's Office notified the public that it adopted the updated Colorado Privacy Act (CPA) Rules, as a follow-up to the amendments to the CPA made earlier in the year (collectively, "Biometric Requirements"). Although the Biometric Requirements have garnered relatively limited attention, they do introduce significant new obligations for businesses that collect and process biometric identifiers and data that will need to be addressed by the time they come into force on **July 1, 2025.**

EXPANDED APPLICABILITY

Unlike most other portions of the CPA, smaller organizations and/or those that only collect non-consumer data (e.g., HR data only) can also find themselves on the hook for complying with the Biometric Requirements. While the CPA generally only applies to businesses that meet certain thresholds (processing personal data of 100,000 or more Colorado residents or selling personal data of 25,000 or more residents), the new requirements in section C.R.S. § 6-1-1314 apply much more broadly. Any entity doing business in Colorado or targeting Colorado residents must now comply with these Biometric Requirements, regardless of size or data volume. Moreover, the Biometric Requirements apply to employers that collect biometric information from their employees, in spite of the fact that the CPA otherwise excludes from its application personal information used in the employment context. However, the CPA maintains the existing exemptions, including, for example, HIPAA related exemptions.

REQUIREMENTS

BIOMETRIC IDENTIFIERS AND BIOMETRIC DATA

As a first step in parsing out the Biometric Requirements, it is crucial to understand the distinction between biometric identifiers and biometric data, as those terms are defined under the CPA. "Biometric identifiers" are defined to mean the raw data points generated by processing, measuring, or analyzing an individual's biological, physical, or behavioral characteristics that can uniquely identify someone. "Biometric data" is a narrower category, defined as one or more biometric

identifiers that are specifically used or intended to be used for identification purposes, either alone or in combination with other personal data. This distinction is important because certain requirements under the CPA apply specifically to one category or the other. Practically, though, most biometric information collected by companies will probably be considered biometric data, as most companies collect biometric identifiers for identification purposes.

BIOMETRIC IDENTIFIER POLICY

Under the Biometric Requirements, companies must adopt and publicly disclose (subject to certain exceptions) a written policy governing their handling of biometric identifiers and biometric data. This policy must establish clear retention schedules and outline comprehensive incident response protocols, including specific procedures for notifying consumers when their biometric identifiers and/or biometric data have been compromised. The policy must also establish strict deletion timelines triggered by the earliest of three events: (1) when the original purpose for collecting the identifier has been fulfilled, (2) 24 months after the last consumer interaction, or (3) within 45 days after determining through mandatory annual review that the data is no longer necessary (with the possibility of a 45-day extension if justified by complexity or volume). Companies are not required to disclose this policy publicly if it applies only to current employees of the company, is used solely by the company and its personnel for internal operational procedures (the exception which we expect most companies to rely on) and/or the information regarding incident response to the extent such information could compromise the security of biometric identifiers.

NOTICE

The Biometric Requirements also require companies to provide clear notice to individuals (or their authorized representatives) before collecting or using biometric identifiers (and practically biometric data because it is a subset of biometric identifiers). The notice must be provided in advance of the collection of biometric identifiers in a manner that is clear, accessible, and understandable. From a content perspective, the notice must contain four essential pieces of information. First, companies must plainly state that they are collecting biometric identifiers, with this disclosure being clear and prominent. Second, the notice must provide specific reasons for collecting this information. Third, companies must specify how long they will retain the biometric identifier. Fourth, if companies plan to share the biometric identifiers with processors, such as third-party service providers, this must be disclosed along with the reasons for sharing.

For companies with an online presence, the notice must be implemented in specific ways. Websites must include a clearly labeled link to the notice on their homepage. If companies have mobile applications, there are additional requirements that mandate access to the notice both in the Apple or Android app store and within the application's settings menu.

CONSENT

The Biometric Requirements also require consent before collection of biometric data and, for most situations, consent must be refreshed after 24 months of no interaction between the organization and the individual, applying to both consumer and employee data, though certain employer uses are exempt from this requirement (discussed below). Additionally, any selling, leasing, trading, disclosing, redisclosing, or otherwise disseminating of biometric identifiers requires a valid consumer consent before such actions. And a vaguely worded portion of the Biometric Requirements suggests that individuals have to consent to the disclosure of their biometric identifiers even to service providers. Practically, therefore, companies will likely need to collect consent for all collections of biometric information (including the narrower biometric data category), because companies generally collect biometric identifiers with the express goal of using such information for identification purposes (making such information, "biometric data" under the Biometric Requirements for which consent is required). In addition, a new consent must be obtained if the processing purpose materially changes to a secondary use or a use not otherwise addressed by the consent.

Finally, companies cannot discriminate against consumers who refuse to provide biometric identifiers that require consent before disclosures, for example, by denying services or charging different prices, unless the biometric identifier is essential to providing the service. Companies also cannot provide lower quality services to consumers who exercise their privacy rights.

EMPLOYEE RIGHTS AND EMPLOYER OBLIGATIONS

The expansion of the Biometric Requirements in its applicability to employers is one of the more seismic changes to the CPA. Unlike the rest of the CPA, the application of which specifically excludes HR data, these new obligations expressly apply to the collection and use of employee biometric identifiers. Employers that collect and use biometric identifiers in the employment context (e.g., for access to buildings) must meet the same requirements as other organizations, including the deployment of a biometric policy as well as notice and consent, with a few nuances. Employers can require biometric identifier collection as a condition of employment (i.e., a coerced consent), but only for the following specific purposes: securing physical and digital access (except that this exception does not apply to the use of biometric identifiers/data for location tracking of employees and/or monitoring of IT systems), recording workday time periods, enhancing workplace safety, and ensuring public safety during emergencies. Employers can collect biometric identifiers for other purposes but only with employee consent. Such consent must be truly voluntary however, meaning that employers cannot make such additional collection/use mandatory or retaliate against employees who decline. However, the Biometric Requirements preserve employers' ability to process biometric data within reasonable job-related expectations and standard hiring practices.

As noted above, employers are generally not required to refresh consent unless the employer is processing additional categories of an employee's biometric identifier for which the employee has not yet provided consent or when processing an employee's biometric identifier for a secondary use.

ENFORCEMENT AND COMPLIANCE

The Colorado Attorney General will have primary enforcement responsibility, with the power to investigate potential violations, seek civil penalties, and require corrective actions. The Biometric Requirements do provide some protection for businesses through a good faith compliance defense, which has been expanded from previous versions of the draft rules, and the ability to seek opinion letters for clarity. Fortunately for companies, the CPA does not allow for a private right of action for violation of its rules (as opposed to the heavily litigated Illinois Biometric Information Privacy Act), including the new Biometric Requirements.

MOVING FORWARD

To address these Biometric Requirements, businesses should develop a comprehensive biometric compliance strategy, giving themselves time to develop and implement solutions prior to the July 1, 2025, effective date. As a first step, companies should identify and understand current and potential collections and uses of biometric identifiers and data, noting that companies otherwise subject to the CPA are already required to treat biometric data (not identifiers) as sensitive data. Companies then will need to:

- Develop and deploy appropriate notices (including for employees where applicable) and a consent management process, if required (often one of the thornier issues);
- Revisit their security programs to make sure they provide appropriate protection for biometric information;
- Establish (and implement) a biometric policy that addresses data retention and deletion; and
- Review and update incident response plans to make sure they adequately cover biometric identifiers and data.

As with any compliance effort, early preparation and thorough implementation will be key to successful compliance with these new Biometric Requirements. And crucially, employers can no longer sit on the sidelines for these efforts. Remember also that these requirements are part of a broader trend in privacy law focusing on biometric data protection. Similar laws exist in other states (e.g., BIPA), and federal legislation may be on the horizon. Building robust compliance programs now can help prepare for future regulatory changes in this rapidly evolving area.

Please reach out to the BCLP Global Privacy & Security team with any questions about these new requirements, and stay tuned for information about the other changes to the CPA.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448

Andrea Rastelli

Boulder

andrea.rastelli@bclplaw.com
+1 303 417 8564
