PUBLICATION

Colorado Enacts BIPA-Like Regulatory Obligations (and More), Ushering in a New Era of Biometrics Regulation in the U.S.

Authors: David J. Oberly
May 08, 2024

In late April, Colorado took a major step toward adding further complexity to the already fragmented U.S. biometrics legal landscape with the passage of HB 1130. The bill, which amends the Colorado Privacy Act (CPA), is likely to be signed into law by Governor Jared Polis and will take effect on July 1, 2025.

HB 1130 is a noteworthy development in the biometrics space. First, it sets forth not only a number of traditional compliance obligations similar to the Illinois Biometric Information Privacy Act (BIPA) but also a range of additional, unique requirements and restrictions that have – until now – been historically confined to broader consumer privacy statutes. This will require many companies to satisfy a detailed set of new obligations pertaining to the use of biometrics.

HB 1130's broad reach will ensnare many organizations that operate or otherwise conduct business in the Centennial State – but which are outside the scope of CPA compliance – significantly enhancing their legal risk and liability exposure.

Companies that develop, supply, or use biometric technologies are advised to take proactive steps to determine whether they fall under the scope of HB 1130 and, if so, develop a concrete plan for the completion of all modifications to organizational compliance programs needed to achieve compliance ahead of July 2025.

Key Aspects of HB 1130

Sweeping Scope and Low Applicability Thresholds

Under HB 1130, controllers (a defined term in the CPA meaning an organization or individual that, alone or jointly with others, determines the purposes for and means of processing personal data) that process *any amount* of biometric data are subject to compliance with HB 1130 – even if they do not meet the thresholds for compliance with the CPA. Thus, all companies that conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to Colorado residents are subject to compliance with HB 1130 in connection with the collection and processing of biometric data. In addition, HB 1130 also sets forth express obligations on biometric data processors.

Moreover, unlike the vast majority of consumer privacy statutes enacted to date (including the CPA) – which provide an across-the-board exemption for the personal data of employees and job applicants – employee/job applicant biometric data is *not* exempted from HB 1130, bringing employers squarely within the scope of compliance when they employ any Colorado resident.

Expansive Definitions for Covered Biometric Identifiers/Data

HB 1130 applies to "biometric identifiers" and "biometric data." A biometric identifier is defined as "data generated by the technological processing, measurement, or analysis of a consumer's biological, physical, or behavioral characteristics, which can be processed for the purpose of uniquely identifying an individual."

Biometric data is defined as "one or more biometric identifiers that are used or intended to be used, singly or in combination with each other or with any other personal data, for identification purposes."

Together, the scope of covered data under HB 1130 is much broader as compared to BIPA, Texas's Capture or Use of Biometric Identifiers Act (CUBI), and similar biometrics laws currently in effect. This aspect of HB 1130 not only increases the extent of legal risk and liability exposure that companies will face but will also create significant complexities and challenges in ascertaining whether organizational biometric data processing activities fall under the scope of HB 1130.

Importantly, the combination of HB 1130's broad applicability and its expansive definitions of biometric identifiers/data will subject controllers to compliance even where only an amount of biometric data is processed, and no actual biometric identification or authentication is performed.

For example, a small online eyewear retailer that offers a virtual try-on (VTO) tool on its website – allowing visitors to "try before they buy" and see how sunglass frames look on their face before making a purchase – would fall under the sweeping scope of HB 1130. Although VTO tools do not perform any function relating to the identification or authentication of individuals' identities, this use case nonetheless triggers compliance because it involves data generated by the technological measurement and analysis of visitors' faces – a biological characteristic – which *can* be processed for the purpose of uniquely identifying an individual.

Similarly, a ten-employee warehouse facility that uses warehouse automation technology, such as a voice-picking solution – a hands-free system that utilizes an intelligent voice agent and speech recognition software to direct fulfillment workers through their tasks—would also fall under HB 1130's ambit because of the speech recognition component of the technology. Here, the mere fact that the tool is analyzing the employee's voice – another type of biological characteristic – is enough on its own to trigger compliance with HB 1130, even if the software is only used to interpret the fulfillment employee's spoken responses (but not for purposes of identifying or verifying that employee's identity).

Significant Potential Civil Penalties and Disgorgement

HB 1130 provides for the imposition of staggering civil penalties of up to $20,000 per violation. In addition, disgorgement, restitution, reimbursement of attorney's fees, and injunctive relief can also be imposed for HB 1130 non-compliance.

While HB 1130 does not contain a private right of action, the law's high civil penalties alone pose the threat of potentially wreaking havoc on companies' bottom lines, especially for those organizations that process a high volume of biometric data.

In addition, the equable remedy of disgorgement – which entails the forced deletion and destruction of not only improperly collected personal data, but all algorithms and associated AI models and tools created through the use of such data – poses a particularly outsized threat to the developers and suppliers of biometric technologies, the vast majority of which rely heavily on advanced algorithms, such as facial prediction models.

BIPA-Like Obligations

In terms of its core compliance requirements, HB 1130 includes several obligations that are common across current biometrics laws, including the following:

- biometrics-specific privacy policies;
- data retention and destruction protocols;
- pre-collection individualized notice;
- pre-collection consent;

- disclosure obligations and limitations;
- a transactional prohibition on selling, leasing, or trading biometric data; and
- data security.

Importantly, however, HB 1130 goes beyond BIPA, CUBI, and the like by adding further obligations to these compliance components that are unique to the Colorado law.

For example, under HB 1130 organizational privacy policies must include not only guidelines and schedules for biometric data retention and deletion but also organizational security incident protocols specific to biometric data.

HB 1130 also contains unique timing triggers for when biometric data must be deleted; namely, on "the earliest reasonable feasible date, which date must be no more than 45 days after a controller determines that storage of the biometric identifier is no longer necessary, adequate, or relevant to the express processing purpose identified by a review conducted by the controller at least once annually." This aspect of HB 1130 adds a significant degree of complexity to the already challenging task of having to satisfy divergent time limitations on the retention of biometric data under the current patchwork of biometrics laws. Not only that, but this obligation will also require companies to conduct periodic reviews of biometric data, and the deletion of any data determined to be no longer necessary, adequate, or relevant to the express processing purposes for which the data was it was originally collected.

Hybrid Obligations

The most notable aspect of HB 1130 is its inclusion of several compliance obligations that, until now, have traditionally been confined to broader consumer privacy statutes like the CPA and its California counterpart, the California Consumer Privacy Act (CCPA).

Here, HB 1130 first requires that controllers satisfy all the following duties imposed on controllers under the CPA:

- **Transparency.** Additional, specific, information regarding data processing activities must be included in privacy policies.
- **Purpose Specification.** The express purpose for which biometric data is collected and processed must be described in detail in both external disclosures to consumers, including privacy policies and written notices/consents, as well as in any internal documentation required by the CPA.
- **Data Minimization.** The processing of biometric data must be limited to the minimum amount that is necessary, adequate, or relevant for the express purposes for which such data is collected and used.
- **Secondary Use.** Consent must be obtained from consumers before processing biometric data for purposes that are not reasonably necessary or compatible with the express purposes for which the data was originally collected.
- **Sensitive Data**. Consent must be obtained from consumers before processing biometric data (classified as a type of sensitive data under the CPA).
- **Care (Security).** Reasonable and appropriate safeguards must be maintained to protect and secure biometric data from unauthorized access, disclosure, or acquisition.

In addition, controllers must comply with HB 1130's consumer access right, which requires additional, separate disclosures to be provided upon the request of a consumer regarding a number of aspects of the controller's biometric data processing activities as it relates to that specific consumer. This will require many companies that have not been required to comply with consumer rights under state consumer privacy statutes – particularly smaller biometric technology vendors – to implement consumer rights compliance and management solutions, which in almost all instances will be a time- and resource-intensive endeavor.

Finally – separate from the incident response disclosures discussed above – the law explicitly requires controllers must implement incident response plans and programs tailored to potential *biometric* data compromise events, and which must comply with Colorado's data breach notification statute.

Processor Obligations

Processors, like controllers, must implement security incident response plans and programs specific to biometric data.

Also, like controllers, processors are subject to the CPA's security requirement with respect to biometric data, which includes (among other things) working with controllers to establish a clear allocation of responsibilities between the two for implementing effective measures to safeguard biometric data.

Employer Obligations

As indicated above, HB 1130 imposes explicit requirements and restrictions on employers in connection with the collection and use of employee/job applicant biometric data.

Aside from four very narrow exemptions, employers must obtain employee or job applicant consent prior to the collection and processing of their biometric data and must honor all refusals to provide consent for such biometric practices. In practice, this will require employers to maintain at least one alternative non-biometric solution that accomplishes the same objectives as the employer's biometric system.

Analysis and Takeaways

Significant Compliance Burdens in Aligning Compliance Programs With Unique Legal Obligations

As discussed above, HB 1130 marks the first "hybrid" biometrics legislation to be enacted in the U.S. With that said, it will almost certainly not be the last.

Notably, these hybrid laws not only create significant legal risk and liability exposure but also impose significant compliance costs due to the range of modifications and additions that companies will need to make to compliance programs in order to align their practices with the obligations imposed by this new type of biometrics regulation.

Such is the case with HB 1130, which will require wholesale changes to compliance programs to align with the law's unique requirements pertaining to consumer rights, periodic biometric data evaluations, special data retention/destruction requirements, and incident response plans, among others.

Potential Ripple Effect, With Additional Hybrid Regulation to Follow?

In 2024, lawmakers continued to show an increased interest in imposing strict requirements and restrictions over biometrics with hybrid legislation similar to HB 1130. Looking ahead, the success of the Colorado legislature in enacting HB 1130 may accelerate the timeframe for the enactment of additional hybrid regulation in other states. Notably, future hybrid laws will almost certainly come with their own nuances and unique compliance components, which will significantly increase compliance burdens for those companies that develop, supply, and use biometrics. And it goes without saying that as more regulation targeting biometrics becomes law, companies will see a precipitous rise in the scope of legal risk and liability exposure faced in connection with biometrics.

What to Do Now: Practical Compliance Tips and Strategies

Due to the complexity of HB 1130 and the heavy compliance burden that companies face in meeting the requirements set forth under the new Colorado law, businesses should get an early start on working toward compliance with HB 1130 in advance of next July.

Companies can consider the following high-level action steps for adapting current biometrics compliance programs for compliance with HB 1130, and to help prepare for copycat legislation that may follow closely behind HB 1130.

1. Determine whether your organization is subject to compliance with HB 1130.

First, organizations should conduct a threshold analysis to ascertain whether they are subject to compliance with HB 1130. Key questions to consider include:

- Does the organization's operations or business collect, process, or otherwise implicate "biometric identifiers" or "biometric data" as those terms are defined in HB 1130?
- Does the organization determine the means and purposes for the processing of biometric identifiers/data, or does it process such data on behalf of another entity?

Companies must be cognizant of the fact that with HB 1130's lower applicability thresholds, many organizations not subject to compliance with the CPA may still nonetheless fall within HB 1130's ambit, thus requiring compliance with Colorado's new biometrics regulation.

2. Conduct a gap analysis to ascertain the level of alignment between current biometrics compliance practices and the requirements of HB 1130.

Second, companies that are required to comply with HB 1130 should conduct a gap analysis to evaluate the organization's current compliance practices against the requirements and restrictions set forth by HB 1130 to ascertain any compliance gaps that will need to be remediated prior to the time the law goes into effect on July 1, 2025.

3. Develop a compliance action plan to remediate all compliance gaps and achieve full compliance with HB 1130.

Lastly, based on the results of the above gap analysis, companies should formulate and develop a concrete plan for implementing all changes to their current compliance program to remediate any gaps between their current practices and HB 1130 in advance of the law's July 1, 2025, effective date.

Baker Donelson's Biometrics Team Can Help

Completing the above analysis and planning will likely entail an extensive and complex endeavor for most, if not all, organizations.

Our dedicated Biometrics Team is well-versed and experienced in working closely with clients to complete gap analyses and formulate practical remediation action plans to facilitate compliance across the full range of current and proposed biometrics regulations across the globe.

For assistance with HB 1130 or other biometrics-related matters, please contact David Oberly or another member of Baker Donelson's Biometrics, Artificial Intelligence, or Data Protection, Privacy, and Cybersecurity Teams.