VENABLE LLP

Connecticut Signals an Increased Focus on Biometric Data Compliance

June 10, 2025

Brian R. Tengel, Roy Auh, Rob Hartwell and Michael A. Signorelli

In April, the Office of the Connecticut Attorney General (OAG) released an updated enforcement report under the Connecticut Data Privacy Act (CTDPA) to highlight privacy enforcement actions taken in 2024.

As part of the report, the OAG provided "informal guidance" to help ensure retailers are complying with the CTDPA's requirements for biometric data when using facial recognition technology (FRT) as a loss-prevention tool. The OAG's decision to issue biometrics guidance puts Connecticut on the growing list of states—Illinois, Texas, and Colorado among them—that retailers and other businesses should focus on when mapping out compliance plans for deploying FRT or other technologies that use biometric data.

The report's biometrics guidance follows on the heels of a cure notice that OAG sent "after becoming aware of media reports and receiving consumer complaints regarding a Connecticut supermarket's use of biometric software for purposes of preventing and/or detecting shoplifting."

As the report reiterates, biometric data is a type of "sensitive data" under the CTDPA, subject to heightened requirements. Notably, the report recognizes the CTDPA's exception if biometric data is used to prevent fraud or any other illegal activity, but states that "this is not a blanket exception." And even where this or another exception does exist, requirements related to data minimization, purpose limitation, and data security still apply. As the report explains, "businesses that deploy FRT must comply with the CTDPA—there is no 'out' on compliance."

Beyond reminding businesses about notice and consent requirements, the report also advises businesses to ensure that the processing of biometric data is monitored and assessed for risks to consumers, that data minimization and purpose limitation principles are implemented, and that the data is protected throughout its life cycle.

Notice and Consent for Biometric Data Use

The report reiterates that the core requirements of notice and consent for sensitive data processing apply to the use of biometrics in FRT. Specifically, businesses must provide consumers with a reasonably accessible, clear, and meaningful notice about the use of FRT, obtain informed and freely

given consent to process the biometric data, and provide an effective mechanism to revoke consent.

Data Protection Assessments (DPAs)

The report also notes that businesses that use FRT and process biometrics must conduct DPAs, as processing this sensitive data poses a heightened risk of harm to consumers.

The report states that DPAs are a tool to detect and address potential bias or discrimination resulting from the use of FRT. Businesses that deploy FRT "should track the number of true and false positive identifications and understand whether these correlate with demographic differences that may result in discrimination," the Report states, adding that this monitoring is especially important because the CTDPA "prohibits businesses from processing personal data in a manner that unlawfully discriminates against consumers."

Before deploying FRT, businesses are advised to develop and maintain robust policies and procedures on carrying out DPAs, including "an appropriate risk rating methodology," as well as implementation of "FRT-specific bias and discrimination training for all relevant stakeholders."

Because technology changes quickly, the report makes clear that businesses should continually monitor the impact of any changes to FRT and conduct updated DPAs "upon substantial changes to the system or trends in the observed data."

Securing and Minimizing Biometric Data Use

The report closes by reminding businesses to pay particular attention to the CTDPA's data minimization, purpose limitation, and data security provisions, which are "at the heart of the CTDPA and become even more significant in the context of FRT."

The report states that businesses should limit how much personal data is processed through FRT, establish and follow biometric data retention and deletion policies, protect the data, and process the data only for the specific purpose for which it was collected. The report highlights access controls, multifactor authentication, and appropriate segmentation as key safeguards.

Steps Toward CTDPA Biometric Compliance

Businesses considering the use of FRT or other technologies that process biometrics should assess sooner rather than later how they will develop the notices, consents, and other policies and procedures required under applicable laws to deploy this technology.

If you would like assistance determining your biometric privacy obligations and creating a path toward compliance, contact the authors or visit Venable's Privacy and Data Security web page.