

June 15, 2026

Connecticut Amends Privacy Law for a Third Time and Introduces New Requirements for Data Brokering, Personalized Pricing, Using Facial Recognition, Selling Geolocation Data, and More

by [Tatum Andres](#)

A new package of Connecticut privacy laws significantly expands the state's privacy framework. Through SB 4, HB 5222, and HB 5563, Connecticut has amended the Connecticut Data Privacy Act (CTDPA), created a new data broker registration and deletion regime, imposed restrictions on certain forms of data-driven pricing, and established a direct-to-consumer genetic testing privacy law.

Key changes include a prohibition on the sale of precise geolocation data, expanded consumer deletion rights, new transparency obligations for facial recognition technology used for security and fraud prevention, annual registration requirements for data brokers, a state-administered deletion mechanism similar to California's Delete Act, restrictions on "surveillance pricing," and enhanced protections for consumers' genetic data and biological samples. Many of the requirements take effect beginning October 1, 2026, with additional obligations rolling out through 2028 and beyond.

The bottom line: Organizations that collect, use, sell, or share consumer data in Connecticut should assess whether these changes affect their privacy programs and products. The new requirements are particularly relevant for any company that collects or shares geolocation data, operates as or works with data brokers, uses facial recognition technology, personalizes pricing, or offers direct-to-consumer genetic testing services.

What you need to do:

- Companies should review their data inventories and privacy disclosures to identify any sale of precise geolocation data, which will be prohibited under the amended CTDPA.

- Companies using facial recognition for on-premises security may no longer use third-party or public datasets (i.e., face images captured outside of the company's locations). Companies must instead use facial recognition technology that matches scanned faces to an *internal* database under the company's exclusive control.
- Organizations using facial recognition technology for security or fraud prevention should also prepare to implement signage and policy disclosure requirements before the October 1, 2026, effective date.
- Businesses that may qualify as data brokers should evaluate registration obligations, prepare for annual reporting requirements, and assess readiness for future deletion requests submitted through Connecticut's centralized deletion mechanism. These obligations go into effect on a rolling basis from 2027 to 2028.
- Retailers and other organizations that use consumer data (e.g., browsing history, real-time location, or perceived willingness to pay) to personalize pricing should review their practices for compliance with Connecticut's new surveillance pricing restrictions and disclosure requirements. The law will take effect July 1, 2027, so businesses have a long runway to prepare.
- Direct-to-consumer genetic testing companies should update consent processes, data governance practices, consumer rights workflows, and security measures to address Connecticut's new genetic privacy requirements.