DATA PRIVACY & GOVERNANCE HUB

Connecticut Data Privacy Updates and the New Delete-Style Framework

JUNE 10, 2026

Key Takeaways

- Connecticut enacted updates to its state privacy law (CTDPA), including a one-stop data deletion mechanism modeled after California's Delete Act.
- The law creates a state-run data broker registry, restricts the sale of precise geolocation data, and expands consumer rights.
- The new rules require transparency for profiling driven by AI, mandatory assessments for certain automated decision-making systems, and stronger protections for minors.
- The reforms reflect the growing national trend toward state-level privacy regulation in the absence of federal legislation.

What Happened

In May 2026, the Governor of Connecticut, Ned Lamont, signed Senate Bill 4, which updated the Connecticut Data Privacy Act (CTDPA). The legislation was influenced heavily by California's Delete Act, which requires data brokers to honor deletion requests universally submitted through a centralized state portal.

Connecticut's updated version adopted a similar model, which directs the state to build a single online platform where residents can request the removal of their personal data from all registered data brokers.

The bill also establishes a mandatory data broker registry, prohibits the sale of precise geolocation data, expands CTDPA's applicability to smaller businesses, and introduces new rules for facial recognition and automated profiling. These reforms arrive amid growing

national concern about data brokers, algorithmic profiling, and the sale of sensitive location data. The Federal Trade Commission has repeatedly warned that data brokers pose significant threats to consumer privacy and national security.

Privacy and Governance Concerns

Connecticut's new deletion portal and data-broker registry strengthen consumer rights, but also bring up concerns about whether companies will honor deletion requests globally and reliably. Even with a centralized system that is modeled after California's Delete Act, experts continue to warn that deleted data could persist in unregistered broker networks or backup environments.

The law's ban on selling precise geolocation data reflects that location information can be easily re-identified and misused for stalking, tracking visits to sensitive locations, or targeting individuals for scams. Privacy researchers have repeatedly shown that "anonymized" location datasets can still reveal identities.

New requirements for AI transparency and automated profiling also show the gaps in governance. Regulators will need the technical capacity to ensure companies accurately disclose how automated decision-making tools influence consumers and correctly evaluate impact assessments. The FTC's findings on data brokers further show the risk that sensitive information can continue circulating even with stronger state laws in place.

Why It Matters / Policy Considerations

Connecticut's new privacy law highlights how consumers and institutions are dependent on data brokers and third-party digital services. The creation of a centralized deletion portal modeled after California's Delete Act raises some concerns about whether companies will honor universal deletion requests or if copies of personal data will continue circulating through networks that are unregulated.

These developments point out the need for legislators to consider stronger oversight of data brokers and more consistent rules for automated profiling and AI-powered decision-making, and clearer standards for deletion compliance. Technical capacity is needed for regulators to evaluate whether companies disclose how automated systems influence consumers and if

sensitive data is handled securely. The FTC's findings on data brokers show how easily personal information can circulate in markets that are poorly monitored, which calls attention to the need for better coordinated enforcement mechanisms across states.