Connecticut’s Privacy Report Highlights Rising Expectations for Businesses

Paul L. Singer, Alyssa Z. Hutnik, Andrea deLorimier

March 2, 2026

Earlier this month, Connecticut Attorney General William Tong released the 2025 Connecticut Data Privacy Act (CTDPA) Enforcement Report, offering the most comprehensive view yet of the state’s privacy enforcement priorities and emerging risk areas for businesses. The Report analyzes consumer complaint trends, highlights core enforcement themes, and underscores how Connecticut’s privacy regime is shifting from foundational implementation to more targeted enforcement. The report also includes a number of legislative recommendations that may signal future changes to the CTDPA, in addition to those scheduled to go into effect on July 1, 2026. We summarize the Report below.

1. Privacy-Related Consumer Complaints

The Report begins by identifying several common categories of consumer complaints from 2025, including:

- **Unfulfilled Consumer Data Rights Requests.** The Report notes that Connecticut continues to receive complaints about businesses failing to timely honor consumers’ access, deletion, and opt-out requests. Connecticut emphasizes that simply providing a submission channel is not enough. Companies must implement operational processes for identity verification, request tracking, and fulfillment that comply with statutory deadlines.
- **Data Breaches.** The Report indicates that Connecticut received a number of complaints relating to data security incidents and breach notifications, with a particular focus on whether notices were easy to understand and contained all statutorily required information. Connecticut also examined companies’ internal incident response documentation and decision-making processes, signaling that the state expects organizations to maintain clear records demonstrating how and when breach determinations and notification obligations were assessed.
- **People Search Websites & “Publicly Available” Data.** The Report states that nearly one-third of the complaints received this year involved entities or data potentially exempt under the CTDPA, including people search sites and data brokers relying on the statute’s broad definition of “publicly available information.” In the Report, Connecticut reiterates its recommendation that the legislature narrow that definition to ensure such entities are fully covered and again urges removal of certain entity-level exemptions.

2. Enforcement Efforts

The Report details Connecticut's recent enforcement areas and trends, including:

- **Privacy Notices.** Connecticut continues to proactively review privacy notices for substantive compliance with the CTDPA and to issue notices of violation where disclosures are incomplete, inaccurate, or inconsistent with actual data practices. The Report makes clear that Connecticut is not simply checking for the existence of a privacy policy, but is assessing whether notices clearly describe the categories of personal data collected, the purposes of processing, categories of third parties with whom data is shared, consumers' rights and how to exercise them, and whether sensitive data processing is supported by valid opt-in consent.
- **Dark Patterns and Cookie Banner Sweeps.** The Report describes targeted sweeps examining cookie banners and user interfaces for the use of "dark patterns" that may subvert consumers' privacy choices. The AG emphasizes that companies must ensure their consent mechanisms and privacy disclosures accurately reflect actual data practices. Interfaces that make opting out more difficult than opting in, obscure key disclosures, or present misleading choice architecture may draw enforcement scrutiny.
- **Opt-out Preference Signals (OOPS).** The CTDPA requires controllers to recognize and honor universal opt-out preference signals that communicate a Connecticut resident's choice to opt out of the sale of personal data and targeted advertising. The Report notes that the AG is actively working with technologists to test whether businesses are properly detecting and effectuating these signals and makes clear that failure to do so may result in enforcement action. It also recommends legislative amendments that would shift more responsibility upstream—requiring browser vendors, and eventually mobile operating systems, to enable opt-out signals by default rather than placing the burden on consumers to install extensions to transmit Global Privacy Control (GPC) signals.
- **Genetic Data.** The Report notes that the AG issued an inquiry letter to a genetic testing and ancestry company following a data security incident involving sensitive records. The Report urges the adoption of standalone genetic privacy legislation to ensure consistent protections.
- **Consumer Health Data.** The Report indicates that Connecticut began investigating a hormonal fertility tracking app after determining that its privacy notice failed to recognize Connecticut's heightened consumer health data protections.

3. Children's Privacy

The Report makes clear that protecting minors online remains a top priority for Connecticut. Although the Report notes that only two formal violation notices were issued under the CTDPA's expanded minors' provisions, it appears the office has relied heavily on information requests and broader investigations to assess compliance, as highlighted below.

- **Social Media Outreach & DPAs.** Connecticut's early investigatory efforts have included inquiry letters to three popular social media companies regarding their compliance with the CTDPA's minors' provisions. The Report notes that these efforts reinforced the importance of Data Protection Assessments (DPAs), as the state has requested and will continue to request DPAs as part of investigations.
- **Messaging Platforms and Geolocation Data.** The Report explains that Connecticut issued a notice of violation and inquiry letter to a messaging platform popular with children and teens, citing deficiencies in privacy notice disclosures and opt-out practices. It further notes that the

state's investigations increasingly focus on whether platforms know—or willfully disregard—the presence of minors, how they limit unsolicited adult contact, and how they obtain consent for collecting and using minors' precise geolocation data.

- **Gaming Platforms.** The Report explains that Connecticut sent an inquiry letter to a popular game provider regarding potential use of children's personal data for sale and targeted advertising. It further emphasizes that companies may not willfully blind themselves to users' ages and must adjust tracking technologies to account for heightened protections afforded to minors. Connecticut also joined several states in sending a joint letter to a gaming studio regarding deficiencies in privacy disclosures and consent processes and is investigating a data broker offering advertising-related SDKs.
- **Chatbots**. The Report notes that the state continues to investigate a chatbot platform provider regarding alleged harm to minors tied to certain design features. Attorney General Tong joined a bipartisan coalition of 42 attorneys general in urging major AI software companies to implement stronger safeguards and quality controls for chatbot products.

* * *

In short, the Report serves as a clear signal that Connecticut expects mature, operational privacy compliance programs, and provides a roadmap of where Connecticut is focusing its attention. Businesses should:

- Operationalize consumer rights request processes and monitor performance.
- Review privacy notices for accuracy, specificity, and alignment with actual data practices.
- Audit cookie banners and eliminate deceptive designs.
- Confirm detection and honoring of universal opt-out preference signals.
- Ensure sensitive data consent mechanisms are specific, separate, and easily revocable.
- Conduct and document substantive Data Protection Assessments for minors' services.
- Review SDK integrations and tracking technologies in apps used by children.