Updates

Connecticut was one of the first U.S. states to pass a comprehensive data privacy law back in May 2022.

Today, a total of 13 states have passed similar laws, and dozens of other states are proposing legislation to do so as well. A unique element of Connecticut's law, the Connecticut Data Privacy Act (CTDPA), requires the attorney general's office (the Office) to issue a privacy report (the Report) no later than February 1, 2024, including (1) the number of notices of violation the attorney general has issued; (2) the nature of each violation; (3) the number of violations cured; and (4) any other matter the attorney general deems relevant.

Per the Report, the Office indicated that since the CTDPA went into effect on July 1, 2023, it has issued over a dozen notices of violations (generally referred to in the Report as "cure notices" since recipients have a 60-day

cure period to address any alleged violations) and other information requests focusing on privacy policy disclosures, privacy rights responses, use of sensitive data (including biometrics and teen data), and more. The recipients of these cure notices span multiple industries—from retail and fitness to home improvement and parenting technologies—with several investigations still ongoing. Notably, many of the companies receiving cure notices appear to have leveraged the cure period in some capacity and with varying degrees of reported success. This Update discusses the compliance areas on which the Office focused, as well the Office's response to certain data breach notification processes and recent investigations.

Privacy Issues Prioritized in the First Seven Months of CTDPA Enforcement

Privacy Policies and Consumer Privacy Rights

After reviewing privacy policies and consumer privacy rights mechanisms, the Office issued 10 cure notices addressing privacy policy or rights program deficiencies, which alleged the following:

- Failure to provide notice or insufficient notice of consumer rights under the CTDPA, including insufficient notices concerning how Connecticut residents can appeal request denials. Interestingly, in response to several consumer complaints alleging that businesses had improperly denied deletion requests, the Office determined that the businesses or the flagged data were either out of the scope of the CTDPA or subject to a permissible exemption from the request process. This should give businesses some comfort in their reliance on statutory exemptions, assuming that they or the data at issue qualify for such an exemption.
- Creating the improper impression that consumers would be charged for consumer requests as a default, rather than only for unfounded or repetitive requests.
- Failure to provide a clear and conspicuous opt-out link on websites from the sale, sharing, or use of personal data for targeted advertising. The Office noted that in some instances, the rights mechanisms existed but appeared broken or inactive. The Office also noted that the rights mechanisms failed to account for how consumers normally interact with the company.

Sensitive Data (Biometrics and Teen Data)

The Office also issued several cure notices and/or inquiry letters regarding the use of sensitive data, such as biometrics and data collected from teens between the ages of 13 and 16, alleging that the data was collected, processed, and/or shared without sufficient consent mechanisms. The Report also suggested that the current definition of "biometrics" (only applicable when used for "identification purposes") was too restrictive and urged the legislature to adopt a more expansive definition of "biometrics"—as used in other state consumer privacy laws. Additionally, the Report asked the legislature to clarify whether teen data could be used with "consent" for targeted advertising, as it read the law to presently restrict all targeted advertising to teens, even with consent.

Data Brokers

The Office also issued cure notices and inquiries to companies, including a data broker, around the use of certain personal data. In a macabre example of targeted advertising, it investigated a company's mailing of a cremation advertisement to a Connecticut resident after they had recently completed chemotherapy, drilling down on the role played in that instance by a data broker selling marketing lists. The Report urged the legislature to consider more sweeping solutions for data deletion and the ability to opt out of the sale of personal data by data brokers and third parties, asking the legislature to consider passing laws akin to California's Delete Act, which will establish a universal opt-out mechanism for California residents from data broker sales.

Data Breaches

The Office also handles data breaches affecting Connecticut residents under Connecticut's data breach notification statute (Conn. Gen. Stat. §36a-701b) and is actively involved in several multistate breach investigations. In 2023, the Office received approximately 1,800 data breach notices—an increase of about 300 from the two prior years. The Report indicated that the Office has issued "warning letters" to companies concerning breach notification timelines that they found to unjustifiably exceed the required 60-day reporting period. In particular, the Office emphasized its view that the statutory period starts running on the date that the company becomes *aware* of "suspicious activity."

Conclusion and Takeaways

The Report demonstrates the Office's active enforcement of the CTDPA since it went into effect a little more than seven months ago. It also highlights the Office's priorities, particularly regarding companies' handling of sensitive data, transparency in their privacy policies, consent practices, honoring privacy rights, standing up effective tools that reflect the user experience, and actively regulating data brokers.

The CTDPA's "right to cure"—which allows businesses receiving inquiries or complaints from the Office to cure alleged privacy compliance deficiencies within 60 days—sunsets on January 1, 2025. The Report demonstrates that the Office's Privacy Section is active in CTDPA enforcement, as well as its current priorities and receptiveness to companies' attempts to cure. Businesses should take note of these enforcement activities to date, as they provide helpful insights into how the Office is likely to apply the law in practice going forward. Also, the Office's focus on data breach response timeliness suggests that companies that have experienced a security breach should not be cavalier with reporting obligations.

Authors

Gabriella Gallego

Associate
GGallego@perkinscoie.com 650.838.4815

Saba Chinian

Associate
SChinian@perkinscoie.com

Explore more in

Privacy & Security

Related insights

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights

Update

FDA Food Import and Export Updates for Industry