May 13, 2022

Mystic Privacy: Connecticut's New Law Makes it Clearer

by Jon Neiditz , John M. Brigagliano

Connecticut's new privacy law, an Act Concerning Personal Data Privacy and Online Monitoring, also known as the Connecticut Data Privacy Act ("CTDPA"), generally continues the pattern of non-California states enacting comprehensive privacy laws of evolving rights and obligations without a private right of action, but some of the differences are interesting. Like the Colorado Privacy Act, the CTDPA will go into effect on July 1, 2023.

1. Not How Big You Are, But What You Do with Data

While California and Utah use revenue numbers to bring in all large entities or exclude small businesses, the CTDPA covers individuals and entities of any size that conduct business in Connecticut, or produce products or services that are targeted to Connecticut residents, as long as in the preceding calendar year they either:

a. controlled or processed the personal data of at least 100,000 consumers (excluding for the purpose of completing a payment transaction), or
b. controlled or processed the personal data of at least 25,000 consumers and derived more than 25% of their gross revenue from the sale of personal data.

Virginia and Colorado's privacy laws similarly lack revenue targets, although the states differ slightly in terms of revenue thresholds derived from data sales. In addition to excluding pure payment processing, the CTDPA excludes state and local government entities, nonprofits, higher education institutions, financial institutions subject to the GLBA and covered entities and business associates subject to HIPAA.

2. Lots of Rights and Wrongs, But No Rules

The CTDPA gives many rights to consumers and imposes many requirements on controllers, but it is unusual as it does not contemplate Connecticut's Attorney General issuing rules and (unlike Colorado) may anticipate that no rules will be issued. Might somebody be tired out by California?

Consumers (which as in other states except (soon) California, excludes employees and B2B contacts) have rights to:

a. confirm whether a controller is processing the consumer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret (whether companies may withhold information that might reveal trade secrets in response to access requests has been a major point of debate under California privacy law, leading the California Attorney General to issue an advisory opinion on the matter, available here);
b. correct inaccuracies in the consumer's personal data;
c. delete personal data provided by, or obtained about, the consumer;
d. obtain a copy of the consumer's personal data processed by a controller, in a portable and – to the extent technically feasible – readily usable format, provided the controller is not required to reveal any trade secret; and
e. opt out of the processing of their personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning

the consumer.

Data controllers will be required to:

a. limit the collection of personal data to “what is adequate, relevant and reasonably necessary” to the purposes for processing, as disclosed to the consumer;
b. process personal data only for purposes that are reasonably necessary to and compatible with the purposes for processing, as disclosed to the consumer (unless the controller obtains the consumer’s consent);
c. establish, implement and maintain reasonable administrative, technical and physical data security practices;
d. not process sensitive data (e.g., certain demographic categories like race and sexual orientation, biometrics, and precise geolocation) concerning a consumer without obtaining the consumer’s consent and consent must be an affirmative opt-in process rather than agreement to bundled terms;
e. not process personal data in violation of federal and state antidiscrimination laws;
f. provide an effective mechanism for a consumer to revoke consent and cease processing the data within 15 days of receiving a revocation request; and
g. not process personal data of a consumer for purposes of targeted advertising, or sell the consumer’s personal data without the consumer’s consent, where a controller has actual knowledge and willfully disregards that a consumer is 13-15 years old;
h. treat all sharing for any non-monetary consideration as a “sale” (as pioneered by California);
i. adopt a universal opt-out mechanism (like Colorado), but in this case not until 2025;
j. offer opt-outs without the authentication processes required for exercise of other consumer rights (an enforcement favorite of the California Attorney General);
k. use no “dark patterns” to obtain consents (more work for the pattern lighteners you hired for California and Colorado);
l. obtain parental consent for the collection of personal data from children under 13; and
m. do data protection assessments prior to engaging in data processing activities that present a heightened risk of harm to consumers (like the GDPR and three states; DPIAs are here to stay).

Note that “sensitive data” includes personal data knowingly collected from children under 13 years old. Connecticut appears to have focused on increased protections for children’s data, a trend also reemerging at the federal level. Companies should anticipate possible enforcement in this area at both the state and federal levels.

The CTDPA offers the right to cure violations that we love in California, but as in Colorado and under California’s CPRA, it sunsets, in Connecticut’s case on December 31, 2024.

We end with a warning to FTC commissioners and staffers to be sure to make appropriate disclaimers in fabric stores and at parties, lest you inadvertently make drapery illegal in Connecticut, where “dark pattern” now includes anything the FTC “refers to” as such.