New Connecticut law takes its place in the U.S. data privacy framework

By Jeff Mann, Esq., and Gilana Keller, Esq., Stroock & Stroock & Lavan LLP

JULY 5, 2022

In May, the State of Connecticut enacted the Personal Data Privacy and Online Monitoring Act (the "CTDPA") which includes a broad array of privacy regulations that will go into effect on July 1, 2023. (S.B. 6, Gen. Assemb., Reg. Sess. (Conn. 2022)). Connecticut joins four other states -- California, Virginia, Colorado and Utah -- that have enacted privacy laws over the last few years.

While the CTDPA contains many similarities to the existing four U.S. state privacy statutes, it also possesses its own unique differences, thus adding to the growing patchwork of state privacy laws that has been forming absent a federal rule.

Applicability

The CTDPA is applicable to individuals who conduct business in Connecticut or "produce products or services that are targeted to residents [of Connecticut]." The law governs those who during the preceding calendar year controlled or processed the personal data of (1) at least 100,000 consumers, excluding personal data used solely for the purpose of completing a payment transaction or (2) at least 25,000 consumers and derived more than 25 percent of their gross revenue from the sale of personal data. (§ 2).

While the CTDPA contains many similarities to the existing four U.S. state privacy statutes, it also possesses its own unique differences, thus adding to the growing patchwork of state privacy laws that has been forming absent a federal rule.

The CTDPA's scope of applicability is narrower than some of the existing state regulations, but broader than others.

For example, the gross revenue amount required by the CTDPA is smaller than that in Virginia and Utah which require at least 50 percent of gross revenue to be from the sale of personal data, but greater than in Colorado which does not have a threshold amount at all. (VCDPA § 59.1-572; UCPA § 13-61-102).

Additionally, unlike California's Consumer Privacy Act (CCPA) and Privacy Rights Act (CPRA), the CTDPA does not have an independent overriding revenue threshold, and thus, even large revenue generating companies will not be subject to the regulations absent satisfying the minimum consumer requirements (CCPA § 1798.140(c)(1); CPRA § 14(d))). The CTDPA is also unique in that it narrows its reach by not covering data collected solely for the purposes of payment transactions.

The CTDPA's definition of "sale of personal data" includes "the exchange of personal data for monetary or other valuable consideration" to a third party. This definition is similar to the Colorado Privacy Act (CPA) as well as California's CCPA and CPRA, but it is broader than the Utah Consumer Privacy Act (UCPA) and the Virginia Consumer Data Protection Act (VCDPA) which do not include "valuable consideration" as part of the definition of sale of personal data. (CTDPA § 1(18); CCPA § 1798.140(t); CPRA § 14; CPA § 6-1-1303(23(a)); VCDPA § 59.1-571; UCPA § 13-61-101(31)(a)).

There are also groups or organizations that are not covered by the CTDPA, including government bodies, nonprofit organizations and higher education institutions. Similarly excepted are covered entities or business associates as defined in 45 CFR 160.103, such as a person who offers a personal health record to individuals on behalf of a health plan, health care clearinghouse or health care provider; national security associations registered under the Securities Exchange Act of 1934; and financial institutions or data subject to Title V of the federal Gramm-Leach-Bliley Act ("GLBA"). (§ 3(a)).

The GLBA requires certain agencies and regulators to issue regulations ensuring that financial institutions protect the privacy of consumers' personal information by developing and giving notice of their privacy policies to their customers at least annually, before disclosing any consumer's personal financial information to an unaffiliated party. The CTDPA also exempts 16 types of information and data, including, for example, protected health information under HIPAA (Health Insurance Portability and Accountability Act). (§ 3(b)).

Consumer rights

Similar to many of the other state privacy statutes that preceded the CTDPA as well as certain other regulations across the globe such as the GDPR (General Data Protection Regulation) in Europe,

Connecticut employs the concept of a "Controller" to refer to an entity or individual determining the purpose and means of data processing and a "Processor" for the entity or individual that processes personal data on behalf of the Controller. (§ 1(8), (21). The Connecticut CTDPA provides certain rights to Connecticut residents, or "Consumers," which largely track those in the Virginia and Colorado laws with some notable differences.

For example, under the CTDPA, the Consumer has the right to confirm whether a Controller is processing the Consumer's personal data and access such personal data. This language mirrors the language in Virginia's privacy statute. However, the protection is slightly more narrow than that provided by Virginia because the CTDPA creates an exception to providing such information if it would require the Controller to reveal a trade secret. (CTDPA § 4(a)(1); VCDPA § 59.1-573(A)(1)). The Virginia privacy statute has no such exception.

The Connecticut CTDPA provides certain rights to Connecticut residents, or "Consumers," which largely track those in the Virginia and Colorado laws with some notable differences.

Additionally, a Consumer has the right to correct inaccuracies and request the deletion of personal data. Further, a Consumer can "obtain a copy of the Consumer's personal data *processed by the Controller*, in a portable" and "readily usable" format. (§ 4(4)). This is broader than Utah's and Virginia's privacy statutes in which Consumers are only entitled to their previously provided personal data. (UCPA § 13-61-201; VCDPA § 59.1-573(4)).

The CTDPA's provisions regarding the right to opt-out are broad. Similar to the Virginia and Colorado statutes, in Connecticut a Consumer can opt-out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or "profiling in furtherance of solely automated decisions that produce legally or significant effects concerning the consumer." (CTDPA § 4(a); VCDPA § 59.1-573(A)(5); CPA § 6-1-1306).

Under the CTDPA, the Controller must provide a "clear and conspicuous" link on the Controller's website to a webpage that enables a Consumer to opt out of targeted advertising or the sale of personal data. (§ 6(e)(1)(A)(i)). By Jan. 1, 2025, the CTDPA expands the opt-out requirements by mandating that Controllers enable Consumers to opt out "through an opt-out preference signal" which "indicat[es] such consumer's intent to opt out of any such processing or sale." (§ 6(e)(1)(A)(ii)). Similar to California, the Controller is not required to authenticate an opt-out request, which likely will increase the number of requests that are made once the CTDPA goes into effect. (CTDPA § (4)(c)(4); CCPA).

Data protection

The CTDPA also creates certain standardized data protection requirements.

For example, a Controller must conduct and document a data protection assessment for each of the Controller's processing activities that presents a heightened risk of harm to a Consumer. (§ 8). The CTDPA also requires the creation of "reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data." (§ 6) Further, any Controller in possession of de-identified data is required to "take reasonable measures to ensure that the data cannot be associated with an individual" and "publicly commit" to not attempt to re-identify the data. (§ 9).

Moreover, under the CTDPA the Controller must "provide an effective mechanism" for the Consumer to revoke consent "that is at least as easy as the mechanism" provided to give consent. (§ 6). Similar to the Virginia and Colorado statutes, the CTDPA prohibits a Controller from processing sensitive data concerning a Consumer without obtaining the Consumer's consent. (CTDPA § 6; VCDPA § 59.1-574(5); CPA § 6-1-1308)(7)).

Data of minors

The CTDPA also contains strict protections for data of minors.

Processing of data for children under 13 must be done in accordance with the Children's Online Privacy Protection Rule ("COPPA"). The Controller cannot process personal data for purposes of selling or targeted advertising, without the Consumer's consent when knowing the Consumer is between 13 and 16 years old. (§ 6).

The CTDPA also mandates that by Sept. 1, 2022, the General Assembly will convene a task force to study available ways to "verify the age of a child who creates a social media account." (§ 12).

Privacy notice

Similar to other privacy regulations, the CTDPA requires that the Controller must provide Consumers with a "reasonably accessible, clear and meaningful privacy notice" which includes, the categories of personal data processed, the purposes of processing it, how Consumers may exercise their rights, categories of personal data that the controller shares with third parties, and the categories of third parties. It also must include an online mechanism that the Consumer may use to contact the Controller. (§ 6(c)).

Enforcement

A violation of the CTDPA constitutes an unfair trade practice and will be enforced by the Attorney General. This is similar to other state regulations, leaving California as the only state that provides for a private right of action.

When the CTDPA goes into effect in 2023, the Connecticut Attorney General can issue a notice of the violation and allow 60 days to cure. Beginning January 2025, the Attorney General may bring an action without providing an opportunity to cure. (§ 11).

Conclusion

The CTDPA has many similarities to certain of the existing state privacy laws. Still, variations, particularly in its applicability, opt-out provisions, and consumer rights will necessitate close scrutiny of the law to ensure compliance. Without a federal statute, as more states enact privacy laws, the privacy framework will likely continue to only grow more diverse and complex.

Ayanna Thompson, a summer associate at Stroock & Stroock & Lavan LLP, assisted in the preparation of this article.

About the authors

Jeff Mann (L) is a partner in **Stroock & Stroock & Lavan**'s Intellectual Property and Technology Group and a Certified Information Privacy Professional (CIPP/US). He advises clients on data privacy, cybersecurity and technology matters, including data licensing, cloud services and outsourcing issues. He can be reached at jmann@stroock.com. **Gilana Keller** (R) is an associate in the firm's Litigation Group specializing in commercial litigation, government investigation matters, as well as reinsurance arbitrations. She can be reached at gkeller@stroock.com. The authors are based in New York.

This article was first published on Reuters Legal News and Westlaw Today on July 5, 2022.