CLIENT ALERTS & INSIGHTS

As Connecticut Data Protection Law Comes into Effect, New Law Amends-and Adds-Key Provisions

AUGUST 7, 2023

A recently passed law in Connecticut adds in specific protections on sub-sets of consumer health data, creates new rights related to social media, and clarifies requirements related to children's data.

This year has seen a flurry of new data protection laws and regulations-especially at the state level, which continued as the calendar flipped from June to July as Colorado and Connecticut's data protection laws are now in effect and enforceable.

In June, however, just prior to the Connecticut data protection law's effective and enforcement date, the Connecticut state legislature passed, and the governor signed, an amendment expanding the law.

While the previous, unamended version of Connecticut's data protection law included "health data" in its definition of what it considered "sensitive" and subject to prior, opt-in consent requirements, the law was sparse on details related to health data. Pushing health data into the "sensitive" category is how the other U.S. state data protection laws have handled the issue. However, the amendment creates a new, separate category of "consumer health data", while retaining "consumer health data" as a subcategory of "sensitive" data more generally.

The amendment also introduces specific requirements regarding the online activity of children-those under the age of 18.

Consumer Health Data

Where U.S. state data protection laws had largely avoided providing businesses specificity, the amendment to Connecticut's data protection law now includes a specific definition for "consumer health data". Consumer health data is considered any personal data that a business "uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data."

With consumer health data now a sub-set of "sensitive personal data" as defined under the Connecticut data protection law, any business that aims to collect and process such consumer health data is required to obtain each consumer's prior, opt-in, express consent before such collection and processing.

Also specific to health data and access to health care, the amended Connecticut data protection law prohibits businesses from establishing a "geofence" that would establish boundary within 1,750 feet of any mental, reproductive, or sexual health facility for the purpose of "identifying, tracking, collecting data from or sending any notification to a consumer regarding that consumer's health data. Geofences include, for example, "any technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, wireless fidelity technology data or

any other form of location detection, or any combination of such coordinates, connectivity, data, identification or other form of location detection, to establish a virtual boundary."

The amended Connecticut data protection law also puts obligations on businesses to ensure their personnel and employees are properly handling consumer health data. Businesses subject to Connecticut's data protection law are prohibited from allowing any employee or personnel to access consumer health data without first requiring such employee or personnel to sign a confidentiality agreement (or ensuring they are subject to a statutory duty of confidentiality.

Social Media Provisions

In line with other recent state law activity implementing further regulations on social media companies, the amended Connecticut data protection law includes provisions designed to protect the data and health of those individuals under the age of 18.

Specifically, the amended Connecticut data protection law requires social media platforms to allow minors or their legal guardians to request the deletion or unpublishing of any and all social media accounts or posts-with very few exceptions. Upon such a deletion request, the social media platform must cease all processing of that minor's personal data as well.

This is a novel approach to dealing with the issue of children's online safety-essentially extending the popular data protection principle of a right to deletion or right to be forgotten, but broader to social media accounts and minor's personal data. The reason it is broader is due to the "unpublish" requirement that goes along with the deletion. Social media platforms must remove the account and posts from public visibility, something that may be technically difficult.

"Social media platforms" are defined as public or semi-public services used by consumers that are primarily intended to connect and allow users to socially interact within a service or applicable. To qualify as a social media platform, it must enable the users to (i) construct a profile; (ii) populate a list of other users they interact with (e.g., a friends list); and (iii) create or post content viewable by other uses of the services.

The social media platform requirements go into effect on July 1, 2024.

As more states continue to implement their own variations of data protection laws and business juggle the various requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.