State AGs and Consumer Protection: What We Learned from . . . Connecticut Part I

Paul L. Singer, Abigail Stempson, Beth Bolen Chun

May 11, 2023

Our State AG webinar series continues with Connecticut Attorney General William Tong and Chief of the Privacy Consumer Protection Section Michele Lucan. During our webinar, the Connecticut AG's office described their structure and the tools available to them to enforce the state's consumer protection laws. In particular, as the fifth state to pass comprehensive privacy legislation, AG Tong highlighted the AG office's privacy priorities and agenda which we will focus on here in Part I. We will explore the more general consumer protection topics in Part II. In case you missed it, here is a recording of the webinar.

While the Connecticut Unfair Trade Practices Act (CUTPA - Connecticut's UDAP law) is broad and robust, in the privacy and cybersecurity space, the AG has additional authority derived from specific state laws such as the Data Breach Notification law and Connecticut's Data Privacy Act (CTDPA). General Tong noted Connecticut's dedication to enforcing consumer protection, as it relates to privacy, traces back to at least 2011 when it was the first state to create the Privacy Task Force and eventually a standalone Privacy Section in 2015.

Enforcing the CTDPA

AG Tong noted that the CTDPA reflects a "philosophical judgment of Connecticut to return rights and power of authority to consumers regarding their Personal Information." As we have previously reported, the CTDPA provides for several rights such as the right to access, right to portability, right to correct mistakes, right to deletion, and the right to opt out of targeted advertising, sale, and profiling of personal data.

The CTDPA also creates obligations for "controllers" which are entities that alone or jointly determine the purpose and means of processing of personal data. Some of these obligations include: minimizing data collection and storage, providing transparency about the types of data collected and why, ensuring that data is secure, and obtaining consent to process sensitive data. Notably, the CTDPA also provides heightened protections for data related to teenagers, a hot topic for State AGs. Controllers must obtain consent to sell teens' data or conduct targeted advertising to teens.

The Connecticut AG has the exclusive authority to enforce the CTDPA's provisions, making their insights all the more valuable. However, the law provides for a cure period. This means that if the AG's office is aware of a potential violation, the office will reach out to the entity and issue a notice of violation if the AG determines that a cure is possible. If the controller fails to cure within sixty (60) days, then the AG may bring an action against the entity. Similar to the data breach notification law discussed below, a violation is a per se violation of CUTPA.

Connecticut AG's Advice: How to Prepare for Compliance with the CTDPA

With the CTDPA's effective date quickly arriving on July 1, 2023, the Connecticut AG's office provided their own recommendations on how to take steps and prepare for compliance with the new law:

- **Applicability**. Entities should determine whether they meet the thresholds to trigger CTDPA obligations.
- **Data Inventory**. Entities should understand what data they are collecting and where it lives, while also thinking about how to minimize data collection if possible.
- **Consumer Facing Updates**. Entities should review their privacy policies to ensure they are up to date, and that entities are prepared to operationalize and effectuate the mechanisms for consumers to take advantage of their privacy rights (i.e. ensure links work).
- **Internal Updates**. Entities should review and update their vendor contracts to address CTDPA requirements and conduct employee training to minimize data security risks.

Safeguards and Data Breach Notice Laws

The Connecticut Safeguards Law, referred to by the office as the basic building blocks for Connecticut's privacy infrastructure, requires any person in possession of Personal Information (PI) to safeguard data against misuse by third parties, and destroy, erase, or make unreadable the data prior to disposal. Penalties under the Safeguards law can be significant—up to $500 per intentional violation and up to $500,000 for a single event.

Connecticut defines PI as information capable of being associated with a particular individual through one or more identifiers. The AG's office noted that PI is broadly defined. For instance, PI includes a person's name, but also covers other identifiers including social security numbers, driver's license numbers, credit/debit card numbers, passport numbers, biometric information, online account credentials, and certain medical information.

Connecticut's Breach Notification Law requires that an entity that experiences a data breach provide notice to the Connecticut AG without "unreasonable delay" within a 60-day limit. The law also requires that the entity provide two years of ID theft prevention services if social security numbers and taxpayer numbers (ITINs) are compromised. A violation of this law is a per se violation of CUTPA. Last year, Connecticut received over 1,500 data breach notifications, and the office is experienced in reviewing all types of data breaches and determining which ones to pay attention to.

Our Take

Connecticut has consistently been a leader in data security and privacy issues over the last decade, and with the passage of the CTDPA we expect to see the office double down on enforcement efforts. Businesses should pay particular attention to the compliance tips highlighted above by Ms. Lucan and General Tong, as there is little doubt the office will be actively looking for targets right out the gate on July 1. In General Tong's words, "data privacy and the law of data privacy are here. Its obligations are here, present, and they are demanding." Privacy laws can't be approached as "optional" or "too cumbersome" to take precautions and manage the risks of collecting data. Law enforcement will take action where we believe people have failed to meet their obligations under the law" as that is what people in the state of Connecticut "expect and demand."

Given Connecticut's leadership in the multistate Attorney General community, we would not be

surprised to see other states joining Connecticut in enforcement efforts, even without a comprehensive privacy law (relying on their UDAP authority as states have done for decades). Understanding your data collection and security practices is more important than ever.

***

Be sure to look out for Part II of this blogpost where we will talk about Connecticut's UDAP law in more detail as well as priorities and more tools that the Connecticut AG's office uses to enforce consumer protection laws. We also have an exciting blogpost recapping our conversation with the Nebraska Attorney General just around the bend. Stay tuned.