REPORT TO THE GENERAL ASSEMBLY'S GENERAL LAW COMMITTEE

PURSUANT TO PUBLIC ACT 22-15, "AN ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING"

REFERRED TO AS THE CONNECTICUT DATA PRIVACY ACT ("CTDPA")

CODIFIED AS CONN. GEN. STAT. § 42-515 ET SEQ.

February 1, 2024

Executive Summary

Under the Connecticut Data Privacy Act, or "CTDPA," Conn. Gen. Stat. § 42-515 et seq., the Office of the Attorney General ("OAG") is mandated to make a report ("Report"), no later than February 1, 2024, which must include: (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.

In the six (6) months since the CTDPA took effect, the OAG has taken significant steps to prompt compliance with the new law. We have issued over a dozen notices of violation ("cure notices"), as well as a number of broader information requests, under the CTDPA. We have focused on key aspects of the law related to privacy policies, sensitive data and teens' data, among other areas. While many companies have taken prompt steps to address issues flagged in cure notices and/or have cooperated with information requests, all matters have resulted in additional follow-up to ensure that our concerns under the CTDPA are fully addressed. These matters are ongoing.

In addition to the specific requirements of this Report, we appreciate the opportunity to provide: an overview of the CTDPA; background on the OAG's Privacy Section and our efforts to prepare for implementation of the CTDPA, including a strong focus on outreach; a summary of the consumer complaints received under the CTDPA; and a discussion of our early enforcement efforts. The Report concludes with recommendations for strengthening or clarifying the CTDPA's protections.

I. The CTDPA

Consumer Rights

Access/obtain/ delete data businesses have collected about you

Opt out of targeted advertising, sale of personal data

Business Obligations

Limit use of, and be transparent about, data collection

Ensure data security

Obtain consent to process sensitive data

Connecticut was one of the first U.S. states to pass a comprehensive consumer data privacy law. The CTDPA was signed into law on May 10, 2022 and took effect on July 1, 2023. By enacting this legislation, we joined the ranks of a growing list of states taking innovative but necessary steps to protect consumer privacy. Now, a total of twelve (12) states have passed similar laws, with dozens of other states considering proposed legislation in this critical area.

The CTDPA empowers Connecticut residents with key rights over their personal data and establishes privacy protection standards for businesses that process personal data. More specifically, Connecticut residents have the right to: access data that companies are holding on them; have companies correct data that is inaccurate; request that companies delete such data; and opt-out of the processing of their personal data for sale, targeted advertising, or profiling.

Beginning January 1, 2025, businesses must also recognize universal opt-out preference signals indicating a consumer's intent to opt out of targeted advertising and sales of personal data. Throughout Connecticut's legislative process, our Office maintained that this mandatory requirement was critical to offset the heavy burden placed on consumers to exercise their rights under the law and we were pleased that universal opt-out was included in the law as enacted.

As for business obligations, the CTDPA imposes clear responsibilities on businesses to protect consumer privacy, including the duty to: minimize data collection; be transparent about what data is collected and why and to whom it is shared; limit use of personal data to the specific purposes disclosed to consumers; keep data secure; obtain consent for processing of sensitive data or before selling teens' personal data; and conduct data protection assessments for processing activities that present a heightened risk of harm to consumers.

The CTDPA lacks a private right of action and enforcement falls solely to the Attorney General. A violation of the CTDPA is considered an unfair trade practice under the Connecticut Unfair Trade Practices Act ("CUTPA"), Connecticut General Statutes § 42-110a et seq. As such, entities may face civil penalties up to $5,000 per willful violation of the law. The Attorney General may also seek to impose equitable remedies pursuant to CUTPA, including restitution, disgorgement, and injunctive relief.

Until December 31, 2024, the CTDPA provides that, prior to initiating an action, the Attorney General shall notify a business of an alleged violation if the Attorney General determines that a cure is possible. If the business fails to cure such violation within sixty (60) days of the notice, the Attorney General may bring an action. This "right to cure" sunsets on January 1, 2025.

II. Privacy Section

Even before passage of the CTDPA, Connecticut has long been recognized as a leader in the privacy space. In 2015, the Office established a standalone Privacy Section to handle all matters related to the protection of Connecticut residents' personal information, the first attorney general's office in the country to do so.[1] The Section advises the Attorney General regarding the enforcement of state and federal privacy laws, including Connecticut's data breach notification statute (Conn. Gen. Stat. §36a-701b), safeguards law (Conn. Gen. Stat. § 42-471), and CUTPA, as well as the federal Health Insurance Portability and Accountability Act, and the federal Children's Online Privacy Protection Act.

The Privacy Section undertakes a wide range of activities that protect the privacy of Connecticut consumers. Our team reviews all data breaches reported to the Office under Connecticut's breach notice statute. The number of breach notices received by the OAG has increased dramatically over the years— we received over 800 in 2019, 1,200 in 2020, over 1,500 both in 2021 and 2022, and approximately 1,800 in 2023.

We review each notification for compliance with our breach notice and data security laws. We frequently follow up with companies for further details concerning notice timelines, the privacy protections offered to affected residents, the safeguards in place at the time of the breach, and post-breach remedial measures. For example, our team responded quickly to a massive software supply chain attack involving Progress Software's file transfer software (MOVEit), which has generated hundreds of notices to our Office and Connecticut residents from Progress Software's customer companies. We also followed up with Prospect Medical Holdings immediately after learning of a ransomware attack that impacted hospital operations in Connecticut.

Further, over the past several months, our team has issued numerous "warning letters" to companies concerning lengthy breach notice timelines. Connecticut law requires that notice be provided both to our Office and Connecticut residents without unreasonable delay, but not later than sixty (60) days after breach discovery. See Conn. Gen. Stat. § 36a-701b(b)(1). More and more, we are seeing breach notice timelines stretch in contravention of the requisite period in Connecticut law, and we are focused on ensuring timely notices going forward.

In our warning letters, we have made clear that our Office views the statutory period to run from the date that a company becomes aware of the suspicious activity. While we understand that companies need time to investigate breaches and determine the full impact to personal information, lengthy notice timelines—absent clear justification— do not satisfy the requirements of state law. Connecticut residents must receive notice of a data breach as soon as possible so that they may take appropriate steps to protect themselves from the risk of identity theft.

1. The Section has its roots in a multidisciplinary "Privacy Task Force" formed by Attorney General Jepsen in 2011.

In addition to state-specific matters, the Section is currently leading or assisting with numerous multistate investigations of large-scale data breaches and other high-profile matters implicating consumer privacy.

In the past several years, working with multistate partners, the Section has negotiated and entered into a number of key settlements setting robust data security and privacy expectations, including in cases like Equifax, Uber, Anthem, Target and Home Depot, Experian/ TMobile, Google Location Tracking, and Easy Healthcare/ Premom. In the Fall of 2023 alone, the Section successfully resolved three separate multistate breach investigations involving ransomware (Blackbaud), improper device wiping (Morgan Stanley), and coding issues (Inmediata), all while pursuing early enforcement efforts under the CTDPA.

In addition to our enforcement work, the Section monitors federal and state privacy and data security initiatives and provides the Attorney General with counsel on proposed legislation. The Section participates in various National Association of Attorneys General ("NAAG") working groups involving data security and privacy issues, including co-leading a subgroup of states focused on consumer data privacy legislation. Further, the Section engages in extensive outreach to constituents, community groups, and businesses about data security and privacy in Connecticut.

III. CTDPA: Efforts to Prepare for Implementation

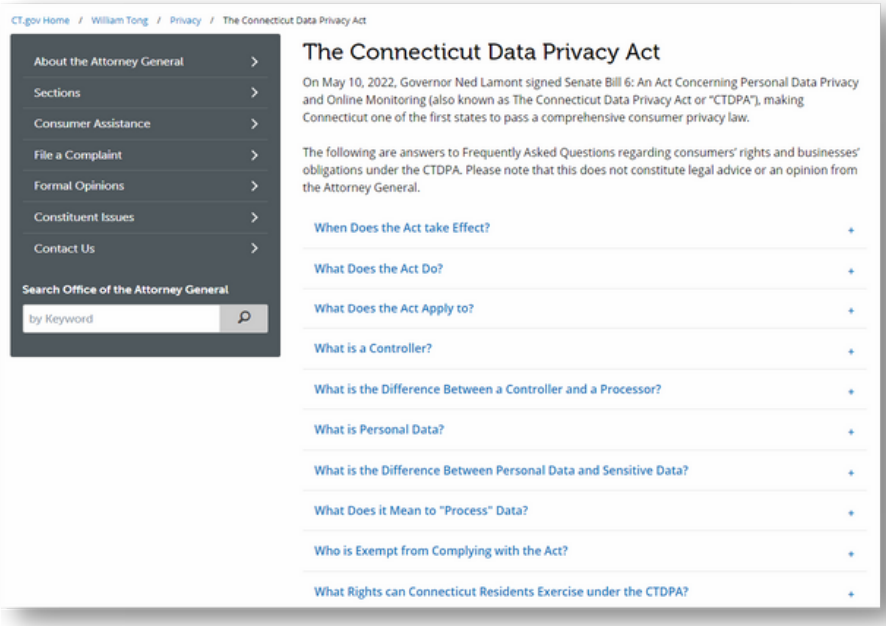
Against this backdrop, the CTDPA took effect on July 1, 2023, granting the Attorney General sole enforcement authority. Given the lack of a private right of action, we maintained during the legislative process that we would require additional resources to meaningfully implement the law's protections. Under the CTDPA, we were provided two additional attorney positions— as a result, we have since expanded our Privacy team from four to six full-time Assistant Attorneys General. In addition to the attorney positions, we were provided a position as part of our efforts to seek out in-house technical expertise (i.e., a technologist); however, it has been a challenge to do so under existing job classifications, including the position of a legal investigator.

When the CTDPA passed, we were also provided funding— limited to $250,000— to aid the OAG's efforts to prepare for implementation. With this funding, Privacy team members have participated in various trainings and are pursuing privacy credentials well-regarded in the field. Further, we engaged a privacy consultant to assist us in preparing for implementation. In order to continue these efforts, we recently issued a Request for Proposal seeking additional privacy and data security expertise as needed.

Importantly, when the CTDPA passed, the OAG immediately expanded outreach efforts to educate the public on the law, positioning our office as a resource for Connecticut businesses seeking to comply with the law's requirements and for Connecticut residents navigating their new data rights.

Attorney General Tong and our team have discussed the CTDPA at a number of events, including industry roundtables and events hosted by the National Association of Attorneys General, the Connecticut Bar Association and Boston Bar Association, and the Practicing Law Institute, as well as consumer education events.

We also published a CTDPA FAQ page on the OAG's website, distilling key components of the CTDPA. We view these FAQs as a foundation that we may supplement as the OAG becomes aware of common issues and questions raised under the law. Finally, in the weeks leading up to the CTDPA's effective date, the OAG issued a press release highlighting the law's effective date in order to ensure that Connecticut businesses and residents were on notice of this important development.



IV. CTDPA-related Inquiries & Consumer Complaints

30 Complaints Received by OAG in first 6 months of CTDPA

Soon after the CTDPA passed, we began receiving inquiries from businesses and consumers alike regarding the law's provisions. While the OAG is unable to provide formal legal advice, we respond to these inquiries to the fullest extent possible. In advance of the CTDPA taking effect, the OAG also updated our consumer complaint portal to ensure that Connecticut residents can appropriately flag that their complaints relate to the CTDPA and that our team would be able to sufficiently review and respond to these complaints. While the OAG does not represent private individuals, we seek to resolve consumer complaints on behalf of Connecticut residents.

From July 1, 2023 to mid-January 2024, the OAG received more than thirty (30) consumer complaints regarding the CTDPA. While the nature of these complaints varied, many involved consumers' attempts to exercise new data rights under the CTDPA, and primarily, the "right to delete."

These complaints highlight the limitations of the CTDPA's protections. Unfortunately, around one-third of these complaints involved data or entities that were exempt under the CTDPA. More specifically, at least six (6) consumer complaints related to issues excepted through data-level or entity-level exemptions. A handful of others were exempt for other reasons, including under the CTDPA's exemption for "publicly available information." For example, we received multiple complaints involving websites that post individual profiles, combining public records like contact information and addresses, property records, court documents, and public social media posts. While many individuals are understandably wary of this data being readily available to anyone online— all in one place— these companies allege that the profiles are pulled from publicly available information.

Despite not having access to the tools provided by the CTDPA, in most of these cases, the OAG reached out to the company involved in an effort to address the concerns raised in the consumer's complaint. Further, our team reviews all consumer complaints for issues or patterns indicative of CTDPA violations— even a single consumer complaint could ultimately lead us down a path to enforcement.

V. CTDPA—Early Enforcement Efforts (6 months from effective date)

Below we provide some highlights of our early enforcement efforts in several key areas. These include reviewing a cross-section of company privacy policies to determine compliance with the CTDPA, focusing on matters involving the collection of sensitive data and teens' data, and taking a closer look at the privacy practices of data brokers. We report on each of these areas in greater detail below.

a. Privacy Policies

Transparency requirements are a crucial component of the CTDPA— these provisions ensure that Connecticut residents have insight into the collection, use and sharing of their personal data, understand their new data rights, and are able to exercise those rights.

After the CTDPA took effect, the OAG began reviewing companies' privacy policies and the functionality of consumer rights mechanisms under the CTDPA. Based on that review, we have issued ten (10) cure notices aimed at addressing privacy policy deficiencies. Recipients spanned various industries, including retail, fitness, event services, career services, parenting technologies, and home improvement. Deficiencies identified in the notices included:

- **Lacking disclosures** (e.g., failure to incorporate notice of consumer rights under the CTDPA at all);
- **Inadequate disclosures** (e.g., failure to sufficiently inform Connecticut residents about their rights under the law and/ or how Connecticut residents may appeal denials);
- **Confusing disclosures** (e.g., statements creating an impression that consumers may be charged for rights requests as a default, as opposed to only for manifestly unfounded, excessive or repetitive requests);
- **Lacking rights mechanisms** (e.g., failure to include a clear and conspicuous link to a webpage enabling consumers to opt out of the targeted advertising or sale of their data);
- **Burdensome rights mechanisms** (e.g., rights mechanisms that did not take into account the ways consumers normally interact with the company); and
- **Broken/ inactive rights mechanisms** (e.g., non-working links or dead-end mechanisms).

Overall, the company responses we have received to date have been positive. Several companies updated privacy policies and/or consumer rights mechanisms quickly upon receiving cure notices. Notably, even where a company took the position that it does not currently meet the applicability threshold in the CTDPA (during the prior calendar year, having controlled or processed the personal data of at least (1) 100,000 consumers or (2) 25,000 consumers and derived over 25% of gross revenue from the sale of personal data), it made changes after receiving our notice because it hopes to meet that threshold in the future. Further, some companies strengthened their disclosures even beyond areas identified in the cure notices.

However, at this early stage, it is difficult to say with certainty how many companies have fully "cured" all deficiencies. While many companies have taken prompt steps to address issues flagged in cure notices and/or have cooperated with our requests, all matters have resulted in additional follow-up. For example, a number of companies made fixes that did not fully alleviate our concerns. Further, some of the privacy policies contained disclosures raising questions about compliance with other areas of the CTDPA (e.g., with respect to the collection of sensitive information or sale of personal data). This process is an iterative one and only time will tell which companies fully satisfy our concerns and which matters will ultimately require more formal enforcement action.

b. Sensitive Data

Another critical aspect of the law, the CTDPA established heightened protections for Connecticut residents' sensitive data, which is defined to include genetic or biometric data, and precise geolocation data, among other elements. The CTDPA requires that businesses obtain Connecticut residents' freely given, specific, informed and unambiguous consent before processing such data.

In the months since the CTDPA went into effect, the OAG has focused on matters raising concerns regarding the collection of sensitive data. For example, the OAG sent a cure notice to a local grocery store after becoming aware of media reports and receiving consumer complaints regarding the store's use of biometric software for purposes of preventing and/or detecting shoplifting.

The OAG also sent an inquiry letter to a major web service provider and retailer after the company issued press releases concerning its plans to widely deploy its palm recognition service for identification, age verification, payment, loyalty membership, and entry. At the time of our inquiry, the company had already deployed the service at hundreds of locations in the U.S., including at several locations in Connecticut, and disclosed plans to expand its availability rapidly.

The OAG sent a cure notice to a popular car brand after the Mozilla Foundation published a report raising serious privacy concerns regarding connected vehicles. In its study, the Foundation called out connected vehicles for collecting and sharing a broad range of highly personal data about consumers. The cure notice included inquiries into the companies' broader data collection and sharing practices.

In addition, in a recent press release, the OAG announced that it sent an inquiry letter to a genetic testing and ancestry company, seeking details related to a data security incident that exposed sensitive records for over five million users, including specifically those of Ashkenazi Jewish and Chinese heritage. In the letter, in addition to seeking information on the data security incident itself, we included questions focused on the company's compliance with the CTDPA.

c. Teens' Data

In addition to sensitive data, the CTDPA established heightened protections for teens' data. In particular, the CTDPA provides that businesses shall not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a business has actual knowledge, and wilfully disregards, that the consumer is at least thirteen but younger than sixteen years of age.

The OAG sent a cure notice to an app company in connection with its an anonymous peer messaging app directed at teens. In October 2023, children's advocacy and tech accountability group Fairplay filed a complaint with the Federal Trade Commission alleging that the app is inherently harmful to kids. This complaint prompted us to review the company's Privacy Policy under the CTDPA. The cure notice included inquiries aimed at learning more about the company's information collection and sharing practices as well as the nature and extent of its targeted advertising efforts directed towards teens.

d. Data Brokers

Under the CTDPA, Connecticut residents have the right to "delete personal data provided by, or obtained about, the consumer." The OAG advocated for the inclusion of this specific language in order to ensure that data brokers are appropriately covered under the law, especially given the broad swaths of information that data brokers collect and collate on behalf of Connecticut residents.

The OAG sent an inquiry letter to a national cremation services company, after receiving a complaint from a Connecticut resident who received an advertisement in the mail for cremation services after recently completing chemotherapy. After reviewing the company's responses, we issued a cure notice to the company as well as an inquiry letter to the data broker that identified the individual for the marketing list. This matter has brought to light the close interplay between data brokers and data analytics firms in the digital marketing landscape.

VI. CTDPA Legislative Recommendations

Through our early enforcement efforts, as well as our collaboration with other states who have recently passed consumer privacy laws, we have identified several areas where legislative changes would strengthen or clarify privacy protections under the CTDPA. These explain our recommendations for future revisions to the law in detail below.

a. Scale Back Entity-Level Exemptions

The CTDPA contains a myriad of exemptions carving out entities from its requirements. Several states have passed comprehensive consumer data privacy laws without these entity-level exemptions. For example, while Connecticut's law flatly exempts all non-profits—despite the fact that many non-profits collect an extensive amount of sensitive personal data—other state privacy laws, such as in California, Colorado, and Delaware, apply to non-profits. Further, while Connecticut's law creates blanket exemptions for entities covered by the federal Gramm-Leach-Bliley and Health Insurance Portability and Accountability Acts, irrespective of the data involved, California and Oregon's laws are appropriately limited to data covered under these laws.

The legislature should scale back the entity-level exemptions in the CTDPA. These sweeping exemptions not only put Connecticut residents at a disadvantage, but they further impact the OAG's ability to uphold the CTDPA's protections and join forces with our sister states in their efforts to enforce consumer data privacy laws against large national entities.

b. Enact One-Stop-Shop Deletion Mechanism

We continue to monitor legislative efforts by other states and believe that Connecticut should enact a "one-stop-shop" deletion mechanism such as that contained in California's Delete Act. Importantly, the Delete Act will allow Californians to delete their personal information held by data brokers through a single, verified request. As with the global-opt out requirement, mechanisms that allow Connecticut residents to exercise deletion rights at scale are sorely needed.

c. Add "Right to Know" Specific Third Parties

Since passage of the CTDPA, other states have built upon Connecticut's framework to strengthen required disclosures concerning information sharing with third parties. For example, Oregon created a "right-to-know" the specific third parties who receive personal data from covered businesses. In addition, Delaware's law allows consumers to obtain a list of the categories of third parties to which the controller has disclosed *that particular consumer's personal data*. Currently, the CTDPA requires only that controllers identify the "categories" of data that they provide to third parties and the "categories" of third parties that they disclose the data to.

The legislature should seek to enhance the required disclosures in the CTDPA related to information sharing with third parties to bring it in line with the protections afforded under other state statutes. Connecticut residents must have insight into the third parties that gain access to their data so that they can track their data downstream and effectively exercise their rights under the CTDPA.

d. Expand Biometric Data Definition

The CTDPA currently defines biometric data to mean "generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual." Under Oregon's newly passed law, the definition of biometric data is not limited only to data used to identify an individual; it covers all biometric data that is capable of doing so. This is an important distinction—biometric data is extremely sensitive and consumers may wish to keep this information private, regardless of whether it is used for identification purposes. Further, even in the circumstance where a controller does not currently use such data for identification, once it is collected, it could easily be used for that purpose in the future and/or by a third party who obtains it.

The legislature should similarly expand Connecticut's definition of biometric data to include data that is capable of being linked to the consumer. The collection, sale, and use of biometric data raises serious privacy concerns for consumers that should trigger elevated protections.

e. Clarify Protections for Teens' Data

The CTDPA states that businesses shall not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where the business has actual knowledge, and willfully disregards, that the consumer is at least thirteen years of age but younger than sixteen years of age. The OAG is aware that this language has generated some confusion among industry participants. Due to the comma placement, the consent language qualifies whether a controller can sell teens' personal data, whereas the law appears to set an absolute prohibition on targeting advertising to teens regardless of consent. This language was subject to several iterations during the legislative process, and in prior versions, the opt-in consent qualifier applied both to sale and targeted advertising, consistent with California's law.

The CTDPA's protections for teens' data are a key aspect of the law. The legislature should clarify whether it intended to ban targeted advertising to teens wholesale, or whether it intended that the opt-consent qualifier apply to both sale and targeted advertising.

f. Address "Publicly Available Information" Language

The CTDPA's definition of "personal data" explicitly excludes publicly available information, which is defined to mean "information that (A) is lawfully made available through … government records or widely distributed media, and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public."

This is another area that has generated confusion among stakeholders— we believe that the inclusion of the "and" was a scrivener's error and that the legislature may have intended to include the word "or", which would comport with the definitions in other state privacy laws.

The legislature should review this language and make any necessary updates.

Conclusion

There is much yet to be done in the balancing act of privacy of consumer information and the need to use and maintain that same information in our global economy. We remain ready to do our part, encouraging and guiding compliance, but prepared to undertake enforcement when necessary.

In that vein, we provide this Report not just to meet the specific requirements in the CTDPA but to continue the conversation in this expanding, and critically important, area of the law.