CTDPA ENFORCEMENT REPORT

2025

ATTORNEY GENERAL
LEX ET JUSTITIA
STATE OF CONNECTICUT

Introduction

The Office of the Attorney General ("OAG" or "Office") is issuing this 2025 Enforcement Report under the Connecticut Data Privacy Act ("CTDPA" or "Act"), Conn. Gen. Stat. § 42-515, et seq., as part of our ongoing effort to be transparent about our compliance expectations and enforcement priorities under the CTDPA. This is the third annual report that we have issued since the CTDPA's July 1, 2023 effective date— we issued an Initial CTDPA Enforcement Report highlighting our early enforcement efforts in the first six months after the law took effect, and then issued our 2024 CTDPA Enforcement Report the following year. Throughout 2025, the OAG continued to take significant steps to prompt compliance with the CTDPA and address privacy concerns that have come to light.

We are also reporting on our enforcement efforts aimed at protecting kids online. More specifically, after the CTDPA passed but before its effective date, the law was amended through 2023's Public Act 23-56 ("P.A. 23-56") to, among other things, expand privacy protections for minors. These provisions took effect on October 1, 2024. Through P.A. 23-56, the legislature required our Office to report, no later than February 1, 2026, on: (1) the number of notices of violation issued related to minors' privacy; (2) the number of violations cured; and (3) any other matter the Attorney General deems relevant.

In this 2025 CTDPA Enforcement Report, we provide an update on: (i) the OAG's broader privacy and data security efforts; (ii) privacy-related consumer complaints received this year; (iii) our data breach notice review and enforcement efforts; and (iv) our CTDPA enforcement efforts and priorities, including those related to minors' privacy. The Report concludes with a summary of recent amendments to the CTDPA and corresponding takeaways for businesses.

In 2025, data breaches remained a pressing concern— we took action to address breach notice delays and set strong data security expectations, including in our first breach settlement involving Connecticut's Student Privacy Act. We directly assisted many Connecticut residents with their privacy concerns, conducted various investigative sweeps under the CTDPA, and resolved our first CTDPA enforcement action. Looking forward, we will remain focused on addressing data security and privacy violations impacting Connecticut residents, and especially Connecticut minors.

Broader Privacy Efforts

Even before passage of the CTDPA, Connecticut has long been recognized as a leader in the privacy space— the OAG was the first office in the country to create a standalone Privacy Section. In addition to enforcing the CTDPA, the Privacy Section advises the Attorney General regarding the enforcement of various other 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 the Connecticut Unfair Trade Practices Act ("CUTPA"), as well as the federal Health Insurance Portability and Accountability Act ("HIPAA") and Children's Online Privacy Protection Act ("COPPA"). The Privacy Section undertakes a wide range of efforts to protect the privacy of Connecticut consumers.

Along with our enforcement work, the Privacy 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 continues to engage in extensive outreach to constituents, community groups, and businesses about data security and privacy in Connecticut, including specific education efforts focused on the CTDPA. In particular, we maintain and regularly update an FAQ page on our website to highlight the CTDPA's requirements.

Privacy-Related Consumer Complaints

The Privacy Section continues to field privacy-related consumer complaints. Since our prior reports, the OAG has received almost seventy (70) new complaints under the CTDPA. We assist Connecticut residents with these complaints, which in turn drive our enforcement efforts and priorities.

The CTDPA has been in effect for two years, but many complaints *still* involve consumers' unsuccessful attempts to exercise data rights, including the right to delete. While we seek to help Connecticut residents with these complaints, our efforts are sometimes frustrated by businesses' failure to maintain an active privacy email address or other mechanism to respond promptly to consumer issues. Businesses must ensure that they are timely and properly handling consumer rights requests as well as any consumer issues or regulator outreach. Businesses must also ensure that privacy email inboxes are staffed and reviewed regularly.

This year, of the consumer complaints we received, nearly one third— twenty-two (22) complaints— involved entities or data potentially exempt under the CTDPA. For example, many of these complaints involved people search websites that purportedly combine "publicly available" records and post individual profiles online. These profiles, which are often extensive, unwanted and inaccurate, are a far cry from public information and should not be carved out from the reach of the CTDPA.

We continue to recommend that the legislature narrow the too-broad definition of "publicly available information" to ensure that people search sites and data brokers are fully covered under the CTDPA. Further, we again urge the legislature omit the entity-level exemptions that do not appear in other states' consumer data privacy laws, including for HIPAA-covered entities and non-profits.

In addition to complaints related to the CTDPA, our Office has received over sixty (60) complaints related to data breaches this year alone. Frequently, companies send data breach notices that are vague and do not sufficiently explain to Connecticut residents why they are receiving the notice. Data breach letters sent to Connecticut residents must make clear why the company has the impacted individual's data and what specific personal information was compromised. In circumstances where notice letters are sent by an entity that does not have a direct relationship with the consumer, the notice must clearly identify how the notifying entity relates to the entity that has a direct relationship with the consumer.

Data Breach Notice Review & Notice Delay Settlements

The Privacy team reviews all data breaches reported to the Office under Connecticut's breach notice statute. The number of breach notices received by the Office remains significant— in 2025, the OAG received over 1,830 breach notifications. [1] We review each notification for compliance with our breach notice and data security laws and frequently follow up with companies for further details concerning notice timelines, the privacy protections offered to affected Connecticut residents, the safeguards in place at the time of the breach, and post-breach remedial measures.

In the past year alone, our Privacy team issued sixty-three (63) warning letters regarding notice delays. Connecticut law requires that notice be provided both to the OAG and Connecticut residents without unreasonable delay, but not later than sixty (60) days after breach discovery. See Conn. Gen. Stat. § 36a-701b(b)(1). In these letters, we continue to stress that we view the statutory notice period to run from the date that a company *becomes aware of suspicious activity,* not the date it determines the full impact to personal information. [2] Connecticut residents must receive notice of a data breach as soon as possible so that they may take appropriate steps to protect themselves from identity theft.

1 The Office received over 800 data breach notifications in 2019, 1,200 in 2020, over 1,500 both in 2021 and 2022, 1,800 in 2023, and 1,900 in 2024

2 *See also* 2022 Office of Civil Rights Cybersecurity Newsletter ("'the time period [for reporting] begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in the rule.'") (quoting Modifications to HIPAA Rules, 1/25/13).

In our 2024 Report, we highlighted that we have pursued several breaches involving egregious notice timelines, that were resolved through Assurances of Voluntary Compliance ("AVCs") from the reporting companies. These AVCs, among other things, require the companies to implement clear incident response and notification plans as well as address certain data security failures that led to the breach. The AVCs also require payments to the State reflective of the companies' failure to comply with Connecticut law and the resulting impact to Connecticut residents.

For example, in April 2024, we finalized an AVC with voice-over internet protocol provider, **Nextiva Servicing LLC**, regarding a January 2020 data breach that impacted a small number of residents. Nextiva did not notify impacted individuals about the breach until September 2023— almost *four* (4) *years* after the breach occurred. In addition to the injunctive relief afforded under the AVC, Nextiva made a $15,000 payment to the State for its failure to provide timely breach notice.

In November 2024, we finalized an AVC with professional services firm **Horne LLP** regarding a December 2021 data breach that impacted a small number of Connecticut residents. In that case, Horne did not notify impacted individuals about the breach until January 2024—more than two (2) years after the breach occurred. Like Nextiva, Horne made a $15,000 payment to the State in addition to agreeing to injunctive relief aimed at ensuring prompt notice going forward.

Our Office has continued to build upon these efforts this year. Most recently, in November 2025, we finalized an AVC with **Omni Healthcare** over a January 19, 2024 ransomware attack that Omni did not report to our Office until April 9, 2025– more than fourteen months later. The breach involved the exfiltration of 330 Connecticut residents' personal information, including Social Security numbers and driver's license numbers. In addition to injunctive relief, Omni made a **$105,000** payment to the State to reflect its untimely notice. Our Office will continue to take this approach, as well as consider more formal action, to address notice delays going forward.

Data Breach Investigations & Recent Settlements

In addition to our broader breach notice review efforts, the Privacy Section is currently leading or assisting with numerous state-specific or multistate investigations of large-scale data breaches and other high-profile matters implicating consumer privacy.[3] The targets of these investigations span multiple industries— including healthcare, pharmaceutical services, telecommunications, education technology, and software providers— and the fact patterns vary (ransomware attacks, credential stuffing[4] etc.). No industry is immune, and companies must guard against these foreseeable attacks.

In 2025, the Section negotiated and entered into a number of important settlements setting robust data security and privacy expectations. For example, in August 2025, we finalized an AVC with dialysis provider **Fresenius Medical Care Holdings, Inc**. to resolve our concerns over a September 2023 data breach experienced by the company. Approximately 348,000 individuals were impacted by the breach, including 9,483 Connecticut residents who had their Social Security numbers and health information exposed. Under the AVC, Fresenius must implement a stringent information security program with new training and reporting obligations and made a $116,085.30 payment to the State. This matter was a priority for our Office given the company's large presence in the dialysis field and the highly sensitive data that the company maintains on behalf of a vulnerable population.

3 In the past several years, working with multistate partners, the Section has 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, Easy Healthcare/ Premium, Inmediata, Blackbaud, Morgan Stanley, Enzo Biochem, Guardian Analytics, and Marriott.

4 Credential stuffing is the automated injection of stolen username and password pairs into website login forms to fraudulently gain access to user accounts.

The same month, we finalized an AVC with benefits administrator **WebTPA Employer Services, LLC** to resolve our concerns regarding a data breach reported by the company in May 2024. As a result of the breach, 49,855 Connecticut residents had their sensitive personal information compromised. The AVC requires WebTPA to maintain a comprehensive information security program and implement specific security safeguards, including related to enforcement of multi-factor authentication, access controls, logging and monitoring, and risk assessment and mediation. WebTPA also made a $200,000 payment to the State. This matter illustrates the importance of ensuring that information security policies are enforced and fully effectuated.

In October 2025, we finalized an AVC with **PharMerica Corporation** and its parent company BrightSpring Health Services ("Companies") to resolve over concerns over a May 2023 data breach that impacted over 5.8 million individuals nationwide, including 105,057 Connecticut residents. Given that PharMerica primarily provides pharmacy services to assisted living facilities, nursing homes, and hospice providers, many impacted Connecticut residents were deceased at the time of the breach. In addition to various data security failures, we found that the Companies' notice was untimely and insufficient— after hearing concerns from medical facilities that received numerous letters on behalf of residents, the Companies chose to cease sending notice to any deceased individual, or their next of kin, if the only address they had on file was a medical facility. Under the AVC, the Companies must strengthen their data security practices and maintain a comprehensive incident response plan that includes appropriate notification to next of kin when an impacted individual is deceased. The Companies also made a $200,000 payment to the state. This matter underscores the importance of providing direct notice when possible given that decedents remain vulnerable to identity theft or fraud and their next of kin are vulnerable to obituary or bereavement scams.

In November 2025, we finalized an AVC with education technology provider **Illuminate Education**, a wholly owned subsidiary of Renaissance Learning, Inc., to resolve our concerns regarding a December 2021 data breach that impacted 26,680 Connecticut students. Our investigation found that Illuminate failed to implement basic security measures to protect students' data. The AVC requires Illuminate to strengthen its cybersecurity practices. Illuminate was also required to pay $5.1 million to Connecticut, New York and California. Connecticut received $150,000 where 28,610 students were impacted; New York received $1.7 million where 1.7 million students were impacted; and California receives $3.25 million where 3 million students were impacted. This was our Office's first settlement involving the Student Data Privacy law and emphasizes the importance of protecting student data.

CTDPA Enforcement Efforts & Takeaways

While several matters highlighted in our Initial Report and 2024 Report remain ongoing, including investigations related to connected vehicles and geolocation data, we wanted to highlight several key takeaways from our enforcement efforts that we hope will provide insight regarding our Office's compliance expectations going forward.

Privacy Notices

The OAG has continued to review companies' privacy notices and the functionality of consumer rights mechanisms under the CTDPA. We have now issued five "privacy notice sweeps," all aimed at addressing deficiencies that keep Connecticut residents in the dark about their data rights or hamper their ability to effectuate those rights.

Notably, we recently announced our first settlement under the CTDPA with **TicketNetwork, Inc**. to address its failure to bring its privacy notice into compliance after receiving a cure notice from our Office. More specifically, we issued a cure notice to TicketNetwork in November 2023 flagging that its privacy notice was inordinately unreadable, missing key data rights, and contained inoperable rights mechanisms. Under the CTDPA, TicketNetwork had 60 days to cure the deficiencies. However, TicketNetwork did not resolve those deficiencies until December 2024— well beyond the statutory cure period. Under the AVC, TicketNetwork must review its privacy notice for compliance with the CTDPA on at least an annual basis and upon any material change in its privacy practices. The AVC also requires that TicketNetwork document data rights requests from Connecticut consumers and provide a report to our Office. TicketNetwork also paid $85,000 to the State.

The OAG has continued to review privacy notices for compliance and issue violation notices where deficiencies have been found. We are prepared to use the full weight of our enforcement authority to address continued non-compliance going forward, especially as we move further away from the cure window.

Opt-Out Rights/Deceptive Patterns

Building upon our privacy notice sweeps, we broadened our enforcement efforts to address problematic cookie banners and deceptive patterns that trick consumers. As noted in our 2024 Report, we have now conducted several sweeps flagging cookie banners that undermine or override consumers' ability to make important privacy choices, by making the path to "opt-out" of targeted advertising or sale (the more privacy-protective option) more difficult or time-consuming than the path to "opt-in" (the less privacy-protective option). We made clear that, to comply with the CTDPA, companies that utilize cookie banners that provide consumers with the option to accept all cookies, should also offer a *symmetrical* option to reject all cookies.

Connecticut residents must be able to exercise their rights without undue burden or confusion. While the CTDPA expressly prohibits deceptive patterns in the context of consent mechanisms, deceptive patterns also violate Connecticut's Unfair Trade Practices Act. Companies will similarly be held accountable for deceptive patterns within, *e.g.*, opt-*out* processes and the layout of consumer rights mechanisms. Businesses must not present consumer choices in a way that is buried or misleading.

Companies must do more than the bare minimum in terms of complying with the CTDPA. They should seek to implement best practices that promote transparency and user control. This means designing choice frameworks that make it simple and easy for consumers to understand and effectuate their data rights. For example, companies should configure consent management pop-ups so that the toggle for cookies that facilitate targeted advertising or data sales is off by default, as the most privacy protective option.

We are also focused on the CTDPA's broader requirements around opt-out rights. More specifically, under the CTDPA, if a controller engages in targeted advertising or sale, the controller must "clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt-out of such processing."[5] Further, a controller must "provid[e] a clear and conspicuous link on the controller's Internet web site to an Internet web page that enables a consumer, or an agent of the consumer, to opt-out of the targeted advertising or sale of the consumer's personal data."[6]

While the CTDPA does not define the term "clear and conspicuous," we can look to analogous federal law for guidance.[7] For example, in the Federal Trade Commission ("FTC") Guides Concerning the Use of Endorsements and Testimonials in Advertising, the FTC defines "clear and conspicuous" to mean:

[5] Conn. Gen. Stat. § 42-520(d).
[6] Conn. Gen. Stat. § 42-520(e).
[7] *See* Conn. Gen. Stat. § 42-525(e) (noting that a violation of the CTDPA is a *per se* violation of the Connecticut Unfair Trade Practices Act ("CUTPA"); Conn. Gen. Stat. § 42-110b(b) (noting that when construing CUTPA, courts should be guided by interpretations given by the FTC and the federal courts to Section 5 of the FTC Act.); *see also* Conn. Gen. Stat. § 42-524(a)(1) ("Nothing in [the statute] shall be construed to restrict a controller's . . . ability to: (1) Comply with federal, state or municipal ordinances or regulations.").

> that a disclosure is *difficult to miss (i.e., easily noticeable)* and easily understandable by ordinary consumers. … A visual disclosure, by its size, contrast, *location,* the length of time it appears, and other characteristics, *should stand out* from any accompanying text or other visual elements so *that it is easily noticed, read, and understood.* … In any communication using an interactive electronic medium, such as social media or the internet, the disclosure *should be unavoidable.* [8]

Similarly, in the FTC's "Dot Com Disclosures"– which provide guidance to online advertisers regarding how to make required disclosures "clear and conspicuous" to avoid deception – the FTC states that companies should consider, among other factors: "the prominence of the disclosure; whether it is unavoidable; whether other parts of the ad distract attention from the disclosure; [and] whether the disclosure needs to be repeated at different places on a website. . . . [9]

Further, the guidance dictates that when using a hyperlink to lead to a disclosure, companies should "make the link obvious" and "place the hyperlink as close as possible to the relevant information it qualifies and make it noticeable." [10] The Guidance also recommends that companies "design advertisements so that 'scrolling' is not necessary in order to find a disclosure. [11] When scrolling is necessary, use text or visual cues to encourage consumers to scroll to view the disclosure." Ultimately, the Guidance concludes that "[t]here is no litmus test for determining whether a disclosure is clear and conspicuous. … [T]he best practice would be to select the method more likely to effectively communicate the information in question."[12]

Applying these principles here, while it has become a common practice to embed opt-out links in the website footer, we question whether these opt-out links are "obvious and on the front page," "difficult to miss," "easily noticeable," or "unavoidable." Consumers must often scroll all the way down to the bottom of the lengthy webpage to locate the link to exercise their opt-out rights. This link is not "obvious" and there are no visual clues that encourage consumers to scroll down to the footer to exercise their rights.

Connecticut residents' right to opt-out of the processing of their data for targeted advertising, sale, or profiling is a key component of the law. As a best practice, companies should ensure meaningful and prominent notice of these opt-out rights, as well as provide obvious opt-out mechanisms.

Universal Opt-Out Preference Signals

Our Office remains focused on ensuring that businesses honor the CTDPA's universal opt-out provisions ("OOPS"). Effective January 1, 2025, the CTDPA requires that businesses recognize universal opt-out preference signals indicating Connecticut residents' intent to opt-out of targeted advertising and the sale of their personal data across *all* website-based activities. In our 2024 Report, we highlighted our Data Privacy Day educational efforts related to OOPS signals. We worked with California and Colorado to develop resources for consumers to learn how to send their OOPS signal, and for businesses seeking to honor the Global Privacy Control ("GPC").[13] We signaled that after conducting this outreach, we would turn towards enforcement.

To this end, in August 2025, we announced an investigative sweep with California and Colorado flagging potential noncompliance with the OOPS provisions. As part of the sweep, we issued letters to businesses that did not appear to be processing consumer requests to opt-out of targeted advertising and the sale of their personal data submitted via the GPC and requested that those businesses come into immediate compliance. While these matters are ongoing, companies should note that GPC signals should trigger an opt-out across all personal data— not just data collected and shared via tracking technologies such as cookies or software development kits (SDKs). In addition, this opt-out must apply to all devices which a consumer uses to log into an account maintained by the controller, including on mobile apps.

---

8 16 CFR 255.0(f) (emphasis added); *see also Longbridge Fin., LLC v. Mut. Of Omaha Mortg., Inc.*, No.: 24-cv-1730-DMS-VET, 2025 U.S. Dist. LEXIS 91179, at *19-20 (S.D. Cal. May 13, 2025) (finding defendant's disclosures were "confusing and misleading to consumers" where "landing page lacked a banner disclosure or a hyperlink to its disclosures at the top of the page" and where a consumer needed "to scroll to the very bottom of the landing page and click on a "Disclaimer" hyperlink to reach defendant's full-form disclaimers.").

9 FTC Dot Com Disclosures, March 2013 at ii (the "Dot Com Disclosures").

10 *Id.*

11 *Id.*

12 *Id. at iii.*

13 *See* The Connecticut Data Privacy Act FAQ page, *CTDPA Universal Opt Out Resources* (updated Jan. 29, 2025), https://portal.ct.gov/ag/sections/privacy/the-connecticut-data-privacy-act.

Much like the OAG's work enforcing compliance with the CTDPA's privacy notice and opt-out requirements, we will continue to use our resources to ensure that companies are complying with the OOPS provisions. We are working with a robust team of experts and technologists to examine compliance and are prepared to pursue violations. We also recommend that the legislature expand the utility of the CTDPA's OOPS provisions by joining California in requiring all browser vendors, and eventually mobile operating systems, to enable users to affirmatively send opt out preference signals. Currently, consumers that use major browsers, like Chrome and Safari, must download an extension to send the GPC signal – an extra hurdle for consumers seeking to exercise their rights.

Genetic Data

In our prior reports, we noted that the OAG had issued an inquiry letter to a genetic testing and ancestry company, seeking details related to a data security incident that exposed sensitive records for over seven million users as well as the company's compliance with applicable privacy laws, including the CTDPA. More recently, that company, 23andMe, filed for bankruptcy, and we intervened in the bankruptcy to ensure that genetic data would be protected and data rights would be honored. We also filed a proof of claim on behalf of Connecticut residents. Based on our experience in that matter, we urge the legislature to adopt a standalone genetic data privacy law to ensure that Connecticut residents have the same protections as residents of other states that have enacted such laws.

Consumer Health Data

Consumer health data privacy continues to be a priority for the OAG. Under the CTDPA, "consumer health data" constitutes "sensitive data" requiring that a controller obtain a consumer's opt-in consent before processing such data.[14] Further, the law prohibits companies from (1) selling, or offering to sell, consumer health data without first obtaining the consumer's consent;[15] and (2) providing any processor with access to consumer health data without proper contracts in place, including requiring that the processor keep the data confidential.[16] Notably, these provisions apply to all consumer health data controllers who do business in Connecticut, regardless of their size or the nature of their data processing activities.[17]

Earlier this year, we began an investigation into a hormonal fertility tracker app/service based on our findings that its privacy notice failed to recognize Connecticut's heightened consumer health data protections. Based on the personal nature of the company's data processing, we tested their app on both iOS and Android devices to review data flows. While our investigation is ongoing, we note that processing sensitive data, including voluntarily shared consumer health data, is unlawful when companies do not inform consumers about the heightened risks of harm inherent to such processing.[18]

We also sent a notice of violation and inquiry letter to a large data broker highlighting concerns regarding its sensitive data processing disclosures and consent processes. The data broker processes several categories of "sensitive data" under the CTDPA, including consumer health data. To process sensitive data, a controller must first obtain opt-in "consent" which means "a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer."[19] Importantly, "'consent' does not include … acceptance of general or broad terms of use or a similar document that contains descriptions of personal data processing along with other, unrelated information…."[20]

Consent disclosures are intended to enable consumers to provide their freely given, specific, informed and unambiguous agreement to process his/her sensitive data. Such disclosure must identify what categories of sensitive data are collected, who it is shared with, and for what specific purposes. Further, it is especially important that companies provide consumers with a mechanism to revoke their consent "that is at least as easy as" the mechanism by which the consumer provided consent.[21]

14 Conn. Gen. Stat. §§ 42-515(9)(38), 42-520(a)(4).
15 Conn. Gen. Stat. § 42-526(a)(1)(D).
16 Conn. Gen. Stat. § 42-526(a)(1)(B), 42-521
17 Conn. Gen. Stat. § 42-526(a)(2) (citing Conn. Gen. Stat. § 42-516).
18 Conn. Gen. Stat. § 42-522(a).
19 Conn. Gen. Stat. § 42-515(7).
20 Conn. Gen. Stat. § 42-515(7)(A).
21 Conn. Gen. Stat. § 42-520(a)(6).

CTDPA Enforcement Efforts— Minors' Privacy

Effective October 1, 2024, the CTDPA imposes important obligations on companies that offer online services, products or features to minors, which is defined to mean any consumer younger than eighteen years of age.[22] The minors' privacy provisions require that covered entities use reasonable care to avoid a heightened risk of harm to minors. Further, these provisions currently prohibit: (1) the processing of a minor's personal data for targeted advertising, profiling, or sale without consent; (2) using a system design feature to significantly increase, sustain, or extend a minor's time online without consent; and (3) collecting a minor's precise geolocation data without consent. The minors' privacy provisions also require that covered entities put specific safeguards in place for direct messaging tools and provide a signal to minors while collecting their precise geolocation data. Lastly, covered entities must conduct data protection assessments ("DPAs") addressing the potential risks of harm to minors.

Protecting kids online remains a topmost priority for our Office. In the year since the CTDPA's expanded minors' privacy provisions took effect, the OAG issued two violation notices but relied more heavily on information requests since many of these issues are complex, do not involve facial deficiencies, and are not easily "fixed." To this end, we opened several broader investigations focused on the minors' privacy provisions. Some examples of these matters, all of which are ongoing, are discussed below.

Early Outreach and Investigatory Efforts

Early on, we issued inquiry letters to three popular social media companies seeking to understand the steps that the companies were taking to comply with the CTDPA's minors' privacy provisions. While the companies reported taking steps to comply with the CTDPA, it is clear there is still more work to be done to increase the safety and privacy of minors online.

Based on these early efforts, we advocated for legislative fixes to enhance the minors' privacy provisions. The legislature amended the CTDPA to expand these protections, including by prohibiting addictive design features outright and banning the processing of minors' personal data for targeted advertising and sale (removing the consent structure currently in the law), as well as prohibiting controllers from collecting minors' precise geolocation unless strictly necessary. In addition to these legislative updates, we also advocated for standalone legislation that would protect Connecticut minors from the harms of addictive feeds.

These early efforts also reinforced the importance of the CTDPA's data protection assessment ("DPA") requirements, especially for minors' data. Under the minors' privacy provisions, entities must conduct DPAs to determine whether their online services, products, or features offered to minors pose a heightened risk of harm, and if so, to establish and implement a plan to mitigate or eliminates such risks.[23] Our Office has requested and will continue to request DPAs as part of our investigations, and covered businesses are expressly *required* to turn those DPAs over to our Office. These DPAs should be conducted before a covered business engages in an activity that presents a heightened risk of harm— these should not be done after the fact. DPAs should be comprehensive and detailed, and timely provided to our Office upon request.

Messaging Apps

We sent a notice of violation and inquiry letter to a messaging platform provider that is popular with kids and teens, highlighting multiple deficiencies with its privacy notice disclosures and opt-out practices. Our investigations have increasingly focused on whether platforms know about, or willfully disregard, the presence of minors on their platform, how the platforms restrict the ability of adults to send unsolicited messages to minors, and how they receive consent for the collection and use of minors' precise geolocation data.

[22] Conn. Gen. Stat. §§ 42-529, *et seq.*
[23] Conn. Gen. Stat. 42-529b.

Gaming Platforms

We sent an inquiry letter to a popular game provider in May focused on the potential use of children's personal data for sale and targeted advertising. Based on testing done using the provider's iOS and Android apps, we discovered the use of software development kits ("SDKs") that are commonly used for targeted advertising. While our investigation is ongoing, this effort indicates the complex nature of regulating data processing to protect children's privacy. Companies may not willfully blind themselves to users' age and must adjust their tracking technologies to account for the heightened protections afforded to minors under the CTDPA.

We also sent a joint letter with several of our sister states to a popular gaming studio and its subsidiaries highlighting deficiencies in the gaming studios' privacy notice disclosures and consent processes, including relating to their processing of minors' data. Further, we are investigating a data broker in the digital advertising space that offers SDKs to app developers – including those targeted at minors – for potential violations of the CTDPA and CUTPA.

Chatbots

AArtificial intelligence (AI) has progressed to the point where interaction with a chatbot can be indistinguishable from interaction with a human. Chatbots are designed to maximize user retention, and as a result they are prone to manipulation, sycophancy, and the reinforcement of delusional thought patterns. This technology comes with great risks, particularly to children.

Our Office continues to investigate a technology company that provides a chatbot platform regarding alleged harm to minors due to certain design features. Attorney General Tong also recently joined a bi-partisan coalition of 42 Attorneys General in sending a letter to major artificial intelligence software production and distribution companies demanding more quality control and other safeguards over chatbot products. The letters highlight that chatbot developers' race to be "first'" is putting children's health at risk.

The Georgetown Law Institute for Technology Law & Policy recently released a Report noting that nearly 3 in 4 teens are using AI chatbots— an alarming statistic given the serious and potentially life-threatening risks involved to a vulnerable population. The Report correctly highlights that AI is not exempt from the law— existing federal and state privacy, data breach, and unfair and deceptive acts apply in this space and can and will be used to tackle chatbot-related harms. We echo the authors in stressing that new AI products and services *do not erase* existing obligations, and that longstanding precedent can be used to tackle these unprecedented harms.

While the CTDPA, Connecticut's unfair trade practices act, and other state data breach and privacy laws apply to chatbot providers, given the serious harms at issue, we strongly believe that standalone, specific chatbot legislation is necessary to protect Connecticut residents and especially minors.

CTDPA Legislative Updates

As set forth above, the legislature amended the CTDPA soon after its passage to add and enhance protections for minors' and consumer health data. In 2025, the legislature again passed a broad set of amendments aimed at strengthening existing protections for Connecticut residents. Many of these 2025 amendments were made at our Office's urging— in our prior reports, we flagged certain weaknesses in the law and called for fixes to those provisions.

These amendments, which will take effect on July 1, 2026, made several notable changes to the CTDPA, including the following:

- The law's applicability threshold was expanded to include businesses that: (i) process the data of more than 35,000 residents (down from 100,000); (ii) sell any personal data; or (iii) that process *any* sensitive data. While other smaller states have similarly lowered applicability thresholds for personal data processing, expansion of the CTDPA to all processing of sensitive data and all sales of such data is unique to Connecticut.

- The entity-level exemption for businesses covered under the Gramm-Leach-Bliley Act ("GLBA") was removed, whereas the law retains a GLBA data-level carveout.
- The definition of "sensitive data" in the law was expanded to include additional categories of data, including disability or treatment, status as non-binary or transgender, certain financial and government identifier information, and "neural" data.
- Controllers will be expressly required to disclose in their privacy notices whether they collect, use or sell personal data for the purpose of training large language models.
- Connecticut residents' right to opt out of profiling was expanded to include *any* automated processing (as opposed to "solely" automated processing) that produces legal or similarly significant effects.
- Connecticut residents will be afforded a right to contest the result of profiling decisions.
- Controllers that engage in profiling must conduct impact assessments, which shall consider specific factors listed in the law.
- Connecticut residents will now have the right to access a list of specific third parties to whom a controller sells personal data. The amendments also make explicit that Connecticut residents have the right to access inferences about the consumer derived from personal data.
- Controllers will be prohibited from processing minors' personal data for targeted advertising or sale (removing these protections from the prior consent framework).
- Controllers will be prohibited from using any system design feature to significantly increase, sustain or extend any minor's use of such online service, product or feature (removing this protection from the consent framework).
- Controllers are prohibited from collecting minors' precise geolocation unless "strictly necessary" for the controller to provide the relevant online service, product, or feature.
- Controllers must conduct privacy impact assessments for minors' data processing in addition to data protection assessments.
- With respect to controllers' duty to avoid a heightened risk of harm to minors, the law makes clear that covered harms include, among other things, physical violence against minors, any material harassment of minors, and any sexual abuse or sexual exploitation of minors.

Businesses can expect that our Office's enforcement priorities will align with updates to the law. For example, we will continue to focus on sensitive data especially with the removal of the problematic threshold, we will seek to ensure companies are honoring Connecticut residents' expanded data rights, and we will continue to focus on minors' privacy, among other areas.

Conclusion

Companies must be responsible corporate citizens and stewards of our personal data, including that of our most vulnerable populations, especially children, and our most sensitive data such as health information, location data and genetic data. Companies must design and implement privacy and safety into technological advances. Privacy and data security is not only paramount, but a competitive edge for companies that are the most successful in innovating. This Office will continue to be transparent in its privacy and cybersecurity efforts as well as work with the legislature to further develop the law for the benefit of all Connecticut residents, and especially our children.