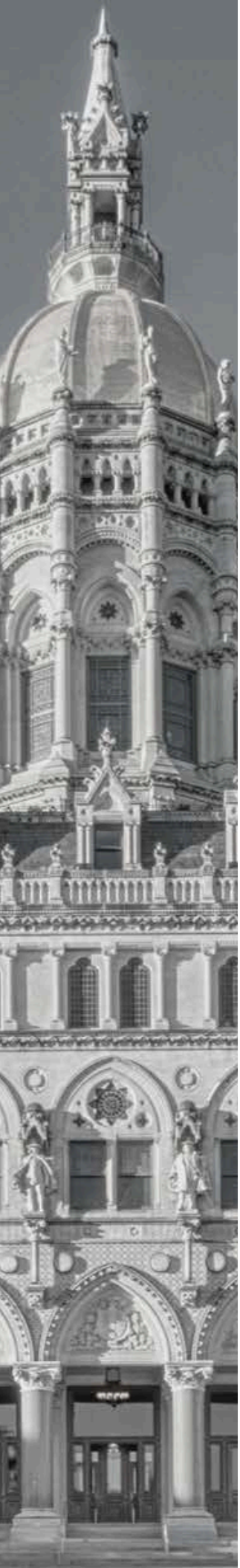
UPDATED ENFORCEMENT REPORT PURSUANT TO CONNECTICUT DATA PRIVACY ACT, CONN. GEN. STAT. § 42-515, ET SEQ.

April 17, 2025



Introduction

The Office of the Attorney General ("OAG" or "Office") is issuing this updated enforcement report ("Updated Report") under the Connecticut Data Privacy Act ("CTDPA" or "Act"), Conn. Gen. Stat. § 42-515, et seq., to highlight common deficiencies and problematic privacy practices that we are investigating and/or addressing under the Act. The OAG issued our initial CTDPA Enforcement Report ("Initial Report") on February 1, 2024,[1] which covered the first six months of enforcement. Now that the CTDPA has been in effect for over a year, we issue this Updated Report covering calendar year 2024 as part of our ongoing efforts to be transparent about our compliance expectations and enforcement priorities.

Since our Initial Report, the OAG has continued to take significant steps to prompt compliance with the CTDPA. We have now issued dozens of notices of violation ("cure notices"), as well as a number of broader information requests, under the Act. We remain focused on key aspects of the CTDPA related to transparency in public-facing privacy notices and sensitive data processing, among other areas, but have also broadened our efforts to address problematic cookie use banners and dark patterns that trick consumers. Our priorities have also expanded as new legislation related to minors' privacy and consumer health data took effect, and as our universal opt-out provisions came online.

In this Updated Report, we provide an update on (1) the OAG's broader privacy and data security efforts; (2) consumer complaints received under the CTDPA to date; (3) several enforcement efforts highlighted in our Initial Report; and (4) our expanded enforcement priorities. As in our Initial Report, this Updated Report concludes with recommendations for strengthening the CTDPA's protections.

Broader Privacy Efforts

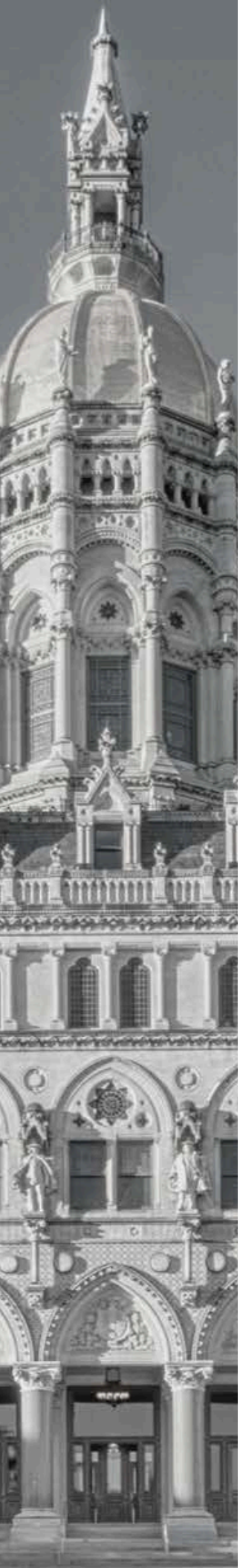
Even before passage of the CTDPA, Connecticut has long been recognized as a leader in the privacy space— the OAG was the first office in the country to create a standalone Privacy Section. In addition to enforcing the CTDPA, the Privacy Section also advises the Attorney General regarding the enforcement 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 activities that protect the privacy of Connecticut consumers.

Breach Notice Review

As noted in our Initial Report, 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 OAG has increased dramatically over the years— in 2024, the OAG received 1,900 breach notifications.[2] 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 residents, the safeguards in place at the time of the breach, and post-breach remedial measures.

In our Initial Report, we highlighted that we had begun issuing "warning letters" to companies concerning lengthy breach notice timelines. 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). Our warning letters are aimed at addressing a troubling trend of breach notice timelines stretching out many months from breach discovery in violation of Connecticut law.

[1] Under the CTDPA, the OAG was mandated to make a report ("Initial Report"), no later than February 1, 2024, to 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 deemed relevant.
[2] The Office received over 800 data breach notifications in 2019, 1,200 in 2020, over 1,500 both in 2021 and 2022, and approximately 1,800 in 2023.



In the past year, our Privacy team has issued dozens of warning letters regarding notice delays. 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.[3] Further, we underscore that 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.

More recently, we have taken these efforts a step further, pursuing several breaches involving egregious notice timelines and requiring 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, and provide timely notice of data breaches going forward. The AVCs also require payments to the State reflective of the impact to Connecticut residents, and as a penalty for failure to comply with Connecticut law. Our Office will continue to take this approach, as well as consider more formal action, to address notice delays going forward. Companies that have received a prior warning letter and subsequently report any new breaches outside the statutory timeframe may be subjected to even higher penalties as willful violations of the law.

Data Breach Investigations & Recent Settlements

In addition to breach notice 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.[4] For example, our team responded quickly to the massive data breach at Change Healthcare ("Change"), that impacted more than one-third of the U.S. population. This incident is the largest-ever healthcare-related security breach. It crippled the healthcare industry, jeopardized countless healthcare providers' solvency and ability to treat patients, and created serious risks of individual harm through scams and identity theft.

Further, within the past year, the Section has negotiated and entered into a number of important settlements setting robust data security and privacy expectations, including in cases like Enzo Biochem, Guardian Analytics, and Marriott. Marriott in particular has been lauded as a benchmark-setting resolution— in that case, a coalition of 50 attorneys general, co-led by Connecticut, reached a settlement with Marriott after an investigation into a large multi-year data breach of one of its guest reservation databases. Under the settlement, Marriott agreed to strengthen its data security practices using a dynamic risk-based approach, provide important consumer protections, and make a $52 million payment to the states.

Legislative Work & Outreach

Along with our enforcement work, the Privacy Section continues to monitor 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.

Most recently, we have updated our CTDPA FAQ page to highlight the Act's consumer health data, minors' privacy, and the universal opt-out provisions. We have also developed additional resources for consumers to learn how to send their opt-out preference signal ("OOPS"), and for businesses seeking to configure their online services to honor the Global Privacy Control ("GPC") signal.[5] On December 30, 2024 Attorney General Tong issued a press release regarding the universal opt-out provisions, emphasizing that this is a key step forward for consumer privacy rights and urging consumers to take advantage of this right to control their data.[6]

[3] 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).
[4] 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, and Morgan Stanley.
[5] 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.
[6] Press Release, Connecticut Office of the Attorney General, Attorney General Tong advises Connecticut con-sumers and businesses of opt out rights and requirements (Dec. 30, 2024), https://portal.ct.gov/ag/press-releases/2024-press-releases/tong-advises-connecticut-consumers-and-businesses-of-opt-out-rights-and-requirements.

Consumer Complaints

The Privacy Section continues to field privacy-related consumer complaints. Since our Initial Report, the OAG has received a steady volume of complaints under the CTDPA. Though it's been over a year since the CTDPA's passage, many complaints involve consumers' unsuccessful attempts to exercise data rights. It should not require our Office's intervention for Connecticut residents' data requests to be processed and honored. Further, we continue to receive complaints regarding websites that combine public records and post individual "profiles" online, which profiles are often extensive, unwanted and inaccurate. The profiles cross the line from public to private and underscore the need for legislative fixes to address the too-broad exemption related to "publicly available information."

In addition to complaints related to the CTDPA, our Office has received over one hundred 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 who the company is, why they have the impacted individual's data, and what specific personal information was compromised.

Early Enforcement Efforts— Updates & Takeaways

While many of the matters highlighted in our Initial Report remain ongoing, including investigations related to genetic information, geolocation data, and minors' data, we wanted to take this opportunity to highlight several key takeaways from our early enforcement efforts that we hope will provide insight regarding our Office's compliance expectations going forward.

Privacy Notices

As noted in our Initial Report, the CTDPA's transparency requirements are a crucial component of the law— 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. The OAG has continued to review companies' privacy notices and the functionality of consumer rights mechanisms under the CTDPA.

We have now issued three separate "privacy notice sweeps" consisting of over two dozen cure notices in total, all aimed at addressing privacy notice deficiencies. As noted in our Initial Report, we have seen many prompt and positive responses to these cure notices— with nearly all companies having taken steps to come into compliance. In particular, companies addressed flagged deficiencies by:

- incorporating the CTDPA and specific mention of all of its consumer data rights;
- incorporating, bolstering, or fixing consumer rights request mechanisms, including adding clear and conspicuous links to opt out of targeted advertising and the sale of personal data;
- incorporating and enhancing disclosures regarding the requisite consumer appeal process;
- strengthening disclosures concerning the processing and sharing of personal data, including sensitive data;
- reformatting privacy notices into a dedicated webpage with clear spacing, typeface, and type size;
- removing language limiting consumers' rights to access or to request a copy of their personal data only to data collected within the last twelve months, where no such limit exists in the CTDPA (or several other state data privacy acts for that matter);
- removing language implying a limit to the number of times a consumer may exercise certain data rights;
- removing language implying that the company will charge consumers for the exercise of data rights by default, as opposed to only for manifestly unfounded, excessive or repetitive requests; and
- removing conflicting language in privacy notices (i.e., where a company stated they did not process data for sale whereas other disclosures indicated that such sales were occurring).

Despite these efforts, we continue to find company privacy notices with glaring facial deficiencies. Indeed, although we are now well after the CTDPA's effective date, we continue to come across privacy notices that have not been updated for years. As more and more states' consumer data privacy laws come online, companies that have not engaged in any effort to update their privacy notices will not be in compliance with these laws. Companies should consider all privacy notices and public-facing representations to be under review.

We are also troubled by privacy notices that create a misimpression that consumer rights are exclusive to residents in only one state, or only in certain states, and that are not sufficiently inclusive of states that have enacted consumer data privacy laws. While companies do not necessarily need to include separate sections in privacy notices for every state that has passed or will pass a comprehensive consumer data privacy law, companies must avoid language that creates ambiguities over whether Connecticut residents have data rights, or conversely, that create the false impression that Connecticut residents lack those rights. There is no excuse for privacy notices that confuse or mislead Connecticut residents about their data rights or that ultimately deter them from exercising those rights.

Further, we underscore the need for companies to be proactive and responsive to our cure notices, notices of violation, and requests for additional information. By and large, companies have shown good faith efforts to bring their notices into compliance and have worked diligently to respond to the deficiencies we have flagged. However, where companies have not done so, we have taken and will continue to take more formal steps to ensure that those concerns are addressed and prioritized going forward.

Just as companies must promptly respond to our Office, they should prioritize consumer rights requests. By honoring valid requests, companies will avoid consumers submitting complaints to our Office. Companies must ensure that they have properly functioning data rights mechanisms and sufficient internal processes in place to timely review all consumer inquiries and requests.

Facial Recognition Technology

In our Initial Report, we noted that the OAG sent a cure notice after becoming aware of media reports and receiving consumer complaints regarding a Connecticut supermarket's use of biometric software for purposes of preventing and/or detecting shoplifting. This led the OAG to carefully consider more broadly Connecticut retailers' use of facial recognition technology ("FRT") as a loss-prevention tool under the CTDPA. While our Office is unable to provide legal advice, we are now providing informal guidance to ensure that Connecticut residents' privacy rights are respected and upheld by businesses choosing to deploy FRT despite its inherent and significant risks to consumers.[7]

By its nature, FRT involves the collection, use, and sometimes sharing of consumers' biometric information. The CTDPA defines sensitive data to expressly include biometric data[8] and appropriately sets forth heightened protections for such data. While the CTDPA contains a so-called crime/fraud exception, this is *not* a blanket exception.[9] Further, key requirements related to data minimization, purpose limitation, and data security apply even where an exception allegedly exists.[10] In other words, businesses that deploy FRT must comply with the CTDPA— there is no "out" on compliance.

[7] This informal guidance does not confer any rights on any person and does not operate to bind the OAG or the public. This guidance further does not preempt federal, state, or local laws, or impact the OAG's enforcement au-thority under the CTDPA or other applicable statutes.
[8] "'Sensitive data' means personal data that includes … (B) the processing of genetic or biometric data for the pur-pose of uniquely identifying an individual, …." (Conn. Gen. Stat. § 42-515(27)).
[9] See Conn. Gen. Stat. § 42-524(a)(9) ("Nothing… shall be construed to restrict a controller's, processor's or consum-er health data controller's ability to prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity… .").
[10] Conn. Gen. Stat. § 42-524(f).

In particular, the CTDPA requires that businesses provide consumers with a reasonably accessible, clear, and meaningful notice about the use of FRT.[11] Such disclosures should clearly point consumers to their rights related to such data. Transparency is critical, especially given that the CTDPA requires that businesses obtain consumers' affirmative consent for the processing of sensitive data[12] and that such consent must be, among other things, *informed* and *freely given*.[13] Additionally, businesses must provide an effective mechanism for consumers to revoke consent and honor consumers' requests to do so.[14]

Under the CTDPA, businesses that use FRT must conduct Data Protection Assessments ("DPAs") as processing sensitive data poses a heightened risk of harm to consumers.[15] While the CTDPA does not dictate a format for DPAs, the scope and detail in DPAs involving FRT should reflect its significant, and well documented, potential impact to consumers' civil liberties. DPAs must carefully assess and document whether and how any benefits from FRT outweigh the serious risks posed to individuals' privacy rights.[16]

Businesses that choose to deploy FRT should actively monitor its use through DPAs. For example, businesses should track the number of true and false positive identifications and understand whether these correlate with demographic differences that may result in discrimination. This is particularly important given that the CTDPA prohibits businesses from processing personal data in a manner that unlawfully discriminates against consumers.[17]

Prior to deploying FRT, businesses should adopt strong policies and procedures related to conducting and documenting DPAs, including an appropriate risk rating methodology, as well as implementing FRT-specific bias and discrimination training for all relevant stakeholders. When using FRT, businesses should capture outcomes of alerts and notifications for feedback and training purposes. Businesses should also continue to monitor the impacts of technological changes to FRT and repeat DPAs upon substantial changes to the system or trends in the observed data.

Businesses deploying FRT should pay special attention to the CTDPA's requirements around data minimization, purpose limitation, and data security— these provisions are at the heart of the CTDPA and become even more significant in the context of FRT. Businesses must limit the amount of personal data processed through FRT, as well as establish and uphold clear data retention and deletion policies and procedures for biometric data. Further, businesses must only process biometric data according to the specific purpose for which such data was collected. Finally, businesses must implement and maintain a comprehensive information security program to protect personal data processed through FRT, including but not limited to strict access controls, multi-factor authentication, and appropriate segmentation.

We have included this informal guidance to provide baseline expectations for businesses that choose to deploy FRT, but it is not exhaustive. Because of FRT's inherent risks and the heightened potential for harm, businesses must seriously consider all consumer rights and privacy obligations under the CTDPA prior to deployment.[18] This guidance is not a blessing or an endorsement of the use of FRT. Given that FRT and related legislation are quickly evolving, this guidance is subject to change.

Marketing and Advertising Practices

In our Initial Report, we noted that the OAG sent an inquiry letter to a national cremation services company based on a complaint from a Connecticut resident who received an advertisement in the mail from them after recently completing chemotherapy. Based on our review, we later issued a cure notice to the cremation services company, as well as inquiry letters to the data analytics firm that identified the individual for the marketing list and the data broker that supplied the data at issue.

[11] See Conn. Gen. Stat. §§ 42-520(c), et seq.
[12] Conn. Gen. Stat. §§ 42-515(7) and 42-520(a)(4).
[13] Conn. Gen. Stat. § 42-515(7).
[14] Conn. Gen. Stat. § 42-520(6).
[15] Conn. Gen. Stat. § 42-522(b).
[16] Conn. Gen. Stat. § 42-522(b).
[17] Conn. Gen. Stat. § 42-520(a)(5).
[18] While this informal guidance focuses on the application of the CTDPA to FRT, businesses deploying this technology must ensure that they also comply with other applicable privacy and consumer protection laws, including CUTPA.

While we were concerned that the companies involved had used sensitive data attributes to identify recipients for the mailer at issue, we determined that the attributes used were name, age, and zip code only. Nonetheless, as a result of our cure notice, the cremation services company updated its privacy notice to disclose the processing of personal data obtained from third-party data analytics and marketing firms, as well as to identify the specific categories of personal data obtained from those firms. Ultimately, this matter illustrates how even the processing of non-sensitive data for advertising can lead to unwanted effects akin to the misuse of sensitive data. This is especially true in industries that involve sensitive topics such as cremation services and companies should exercise heightened caution and oversight when engaging in advertising in these types of industries.

In our broader investigation, we also pushed the data analytics firm to closely consider the CTDPA's requirements and, as a result, the firm has committed to suppress all sensitive data attributes for Connecticut residents in all future marketing campaigns. Finally, we are continuing to review the sensitive data practices of data brokers at issue, as well as data brokers more broadly, including as informed by insights drawn from this matter. Our Office will continue to focus on the entire data flow and we have encouraged legislative changes that will make it easier for Connecticut residents to understand all of the entities that may have their data so that they can best exercise their data rights.

Palm Recognition

We highlighted in our Initial Report that the OAG sent an inquiry letter to a major web service provider and retailer after the company announced its plans to widely deploy its palm recognition service across the U.S., including in Connecticut stores. We sought to understand what steps the retailer had taken to ensure that its roll-out was done in compliance with the CTDPA. We paid close attention to the company's disclosures and consent process, with a particular focus on the CTDPA's requirement that such consent be informed. The company worked with us to provide answers to our inquiries and we were able to address our concerns upfront. This matter is an example of how a cooperative and forthcoming approach to OAG inquiries can yield a productive and positive result.

Connected Vehicles

As noted in our Initial Report, the OAG sent a cure notice, as well as broader inquiries, to a large car manufacturer after public reports raised concerns that connected vehicles were collecting and sharing a range of highly personal data about consumers. As a result of our cure notice, the company quickly updated its privacy notice to clarify what personal data is collected from consumers as opposed to employees. We have since expanded our review to include other car manufacturers, which matters remain ongoing.

Genetic Data

In our Initial Report, 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. Our investigation is ongoing— in addition to reviewing the data security incident itself, we are focused on the company's compliance with applicable privacy laws, including the CTDPA. Our Office would like to remind Connecticut residents to use extreme caution when a business asks them to turn over highly sensitive personal data like genetic data. Connecticut residents should also keep in mind their important data rights under the CTDPA, including the right to delete their personal data, opt out of the sale of their data, and revoke consent for the processing of such data.

Teens' Data

In our Initial Report, we highlighted that the OAG sent a cure notice to a company in connection with its anonymous peer messaging app directed at teens after a children's advocacy group raised concerns that the app is inherently harmful to minors. This prompted us to review the company's practices under the CTDPA, among other laws. This matter underscores why the CTDPA's thresholds should not apply to the processing of minors' data— the law should not require that a company collect data from tens of thousands of minors for the Act to apply.

Expanded Enforcement Efforts

Problematic Opt-out Mechanisms/ Dark Patterns

As part of the next wave of our enforcement efforts, we have expanded our focus to include not just privacy notices but also cookie banners. Through our review, we identified a number of cookie banners that undermine or even override consumers' ability to make important privacy choices, including the right to opt out of targeted advertising or the sale of their personal data through the use of tracking technologies. In the Fall of 2024, we issued a cure notice sweep aimed at addressing these problematic practices, and have identified additional companies for a second sweep.

Under the CTDPA, if a controller sells personal data to third parties or engages in targeted advertising, the controller "shall 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." Further, the CTDPA prohibits controllers from obtaining consumers' consent through the use of dark patterns. A "dark pattern" is defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice… ."[19]

The cookie banners that we flagged violate these provisions of the CTDPA, and likely CUTPA, by failing to provide consumers with a symmetrical choice– meaning that the path for a consumer to "opt out" of targeted advertising or sale (the more privacy-protective option) is more difficult or time-consuming than the path to "opt in" (the less privacy-protective option).

For example, one of our target companies utilizes a cookie banner that allows the consumer to "opt in" to the use of cookies by clicking on an "AGREE" button, which is prominently highlighted in color. By contrast, to "opt out," the consumer must click on "SHOW PURPOSES," and then navigate to an entirely separate window to make that choice. Further, once there, the consumer's preferences are automatically defaulted to "opt in" to "Performance, Functionality, Targeting, and Social Media Technologies" – the less-privacy protection option.

Similarly, another target company utilizes a cookie banner that states: "By continuing to browse our site you accept our cookie policy" and then provides the consumer with only one option – to "opt in" to the use of cookies by clicking on a button that reads, "ACCEPT ALL COOKIES." Although the company includes a link to "click here for more information," that link simply brings the consumer to the general privacy policy and offers no opportunity to "opt out" of cookies.

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. Both options should be displayed on the screen at the same time, and in the same color, font, and size. Whenever possible, the banner should either display each time the consumer accesses the site and/or the mechanism to update/change cookie preferences should be prominently displayed on the site such that the consumer has the means to update/change those preferences at any time.[20]

SB3 (2023) Enforcement Efforts

The CTDPA was amended before it even took effect through 2023's Senate Bill 3 ("SB3") which contains provisions focused on minors' data and consumer health data. These new provisions have been a focus of some of our recent enforcement efforts and are discussed below.

[19] See also Conn. Gen Stat. § 42-520(a)(6) ("A controller shall provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent . . .."); California Privacy Protection Agency ("CPPA") Consent Order in In the Matter of Honda American Motor Co., Inc., at 9-11 (March 7, 2025) (finding Honda cookie management tool failed to provide symmetrical choice because "[w]hile Consumers can 'Accept All' cookies with one click, opting out of the cookies requires at least two clicks."); CPPA Enforcement Advisory No. 2024-02, Avoiding Dark Patterns: Clear and Understandable Language, Symmetry in Choice; Avoiding Dark Patterns, Clear and Understandable Language, Symmetry in Choice, September 4, 2024; FTC Staff Report, Bringing Dark Patterns to Light, September 2022.

[20] We have included this informal guidance to provide baseline expectations for businesses that choose to utilize cookie banners, but it is not intended to be exhaustive. This informal guidance does not confer any rights on any person and does not operate to bind the OAG or the public. This guidance further does not preempt federal, state, or local laws, or impact the OAG's enforcement authority under the CTDPA or other applicable statutes. Further, while this in-formal guidance focuses on the application of the CTDPA to the use of cookie banners, businesses utilizing such banners must ensure that they also comply with other applicable privacy and consumer protection laws, including CUTPA.

Minors—Online Services, Products and Features

As of October 1, 2024, SB3 imposes new obligations on companies that offer any "online service, product or feature" to "minors" who are defined under the law to include consumers who are younger than eighteen years of age.[21] Generally, these provisions require that covered entities use reasonable care to avoid causing a heightened risk of harm to minors. Further, these provisions prohibit: (1) the processing of a minor's personal data without consent for purposes of targeted advertising, profiling, or sale; (2) using a system design feature to significantly increase, sustain, or extend a minor's time online; and (3) collecting a minor's precise geolocation data without consent. The provisions further require that covered entities put specific safeguards in place for direct messaging apparatuses and provide a signal to minors while collecting their precise geolocation data. Lastly, covered entities must conduct DPAs that include an assessment of whether the service, product, or feature causes a heightened risk of harm to minors.

We recently sent inquiry letters to three popular companies that are known to offer online services, products, or features to minors in which we seek additional information to better understand the steps that the companies have taken to comply with these new provisions. Our Office also sent an inquiry letter to a technology company that has been the subject of recent reporting regarding alleged harm to minors and the use of addictive design features, to determine, amongst other things, whether a violation of the minors' data protection provisions, has occurred. In general, companies that offer online services, products, or features to minors should ensure that they have measures in place to comply with the CTDPA's new provisions.

Consumer Health Data

SB3 also amended the CTDPA to add "consumer health data" to the definition of "sensitive data" requiring that a controller obtain a consumer's opt-in consent before processing such data.[22] Further, the amendments require, among other things, that companies (1) not sell, or offer to sell, consumer health data without first obtaining the consumer's consent[23]; and (2) not provide any processor with access to consumer health data without proper contracts in place, including requiring that the processor keep the data confidential.[24] 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.[25]

We sent inquiry letters to two telehealth companies raising concerns that they were transmitting sensitive health information to third-party platforms, such as Meta and Google, through their use of tracking technologies marketed by those platforms. We subsequently sent a cure notice to one of them, noting that the company's mechanism for obtaining consent to process "consumer health data" was insufficient under the CTDPA. As a result of the cure notice, the company implemented an updated user consent process, added consumer disclosures specific to Connecticut law, and conducted a data protection assessment for "consumer health data" as defined by the CTDPA. Covered companies processing consumer health data must comply with the CTDPA's protections.

Universal Opt-Out Preference Signals

As of January 1, 2025, businesses are now required to recognize universal opt-out preference signals ("OOPS") indicating a consumer's intent to opt out of targeted advertising and sales of personal data. The OOPS provisions provide a simpler, privacy-protective online experience for consumers. To send their "signal," a consumer need only configure a setting on their internet browser or browser extension one time, which then automatically sends their choice to opt out to all websites they visit online. To date, the Global Privacy Control[26] ("GPC") is the most widely adopted OOPS mechanism for consumers to send their signal. It has been previously supported by our sister agencies whose comprehensive privacy laws already require compliance with similar OOPS provisions, and we join in that support. The GPC can be effectuated through an increasing number of platforms and mechanisms, including internet browser extensions and privacy-protective browsers.

[21] Conn. Gen. Stat. §§ 42-529, et seq.
[22] Conn. Gen. Stat. §§ 42-515(9)(38), 42-520(a)(4).
[23] Conn. Gen. Stat. § 42-526(a)(1)(D).
[24] Conn. Gen. Stat. § 42-526(a)(1)(B), 42-521.
[25] Conn. Gen. Stat. § 42-526(a)(2) (citing Conn. Gen. Stat. § 42-516).
[26] Global Privacy Control — Take Control Of Your Privacy.

Throughout Connecticut's legislative process, our Office maintained that the OOPS provisions were critical to offset the heavy burden placed on consumers wishing to exercise their rights under the law. Going forward, we will be focused on examining whether businesses are complying with the OOPS provisions and expect to engage in efforts to ensure this key consumer right is upheld.

CTDPA Legislative Recommendations

As noted in our Initial Report, through our enforcement efforts, as well as our collaboration with other states who have passed consumer privacy laws, we continue to identify areas where legislative changes would strengthen or clarify privacy protections under the CTDPA. We have expanded on and added to our recommendations for future revisions to the law in detail below. The CTDPA has become a model for states considering and passing comprehensive consumer data privacy laws, so it is imperative that the CTDPA be updated to provide a strong foundation for future legislation.

Scale Back Exemptions

We strongly urge the legislature to scale back exemptions in the CTDPA. First, the legislature should omit entity-level exemptions for GLBA (Gramm-Leach-Bliley-Act)- and HIPAA-covered entities. Various states have now passed laws without these exemptions— the CTDPA's wholesale carveouts not only put Connecticut residents at a disadvantage, but 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. Moreover, with respect to the GLBA in particular, entities have raised the CTDPA exemption in contexts that we believe are far outside of the legislative intent. Further, we have seen telehealth companies use this HIPAA exemption to avoid having to comply with the CTDPA despite the fact that much of the data they process is not protected health information.

Second, we believe the legislature should narrow the FCRA (Fair Credit Reporting Act) data-level exemption. While the legislature's clear intent was to create a limited FCRA exemption, the current language is overly broad, and businesses have cited to this exemption in a manner resembling an entity-level carveout. The CFPB (Consumer Financial Protection Bureau) recently issued a report calling out these shortcomings in state consumer data privacy laws. The CFPB aptly noted that "while states have significant latitude to provide additional data privacy protections, many states exempt the data and financial institutions subject to GLBA or the FCRA. … This means that such data often is not covered by the new state-law protections, such as the right under state law for consumers to fix or delete incorrect or outdated information, or the requirement that people opt in—instead of having to opt out—of the collection of especially sensitive data."[27]

Third, we believe the legislature should also remove the entity-level exemption for nonprofit organizations. Other states, including California, Colorado, New Jersey, and Maryland, cover non-profits in recognition of the fact that many non-profits collect an extensive amount of sensitive data. Further, privacy laws in Delaware and Oregon exempt only nonprofits with specific missions. Connecticut should join in regulating nonprofit entities that process Connecticut residents' data.

[27] CFPB Report Details Carveouts for Financial Institutions in State Data Privacy Laws (November 12, 2024).

Lower Thresholds

The legislature should lower considerably the CTDPA's thresholds for applicability. While Connecticut is a small state, the CTDPA contains thresholds mirroring those in consumer data privacy laws passed by much larger states. The CTDPA's threshold should be updated to match Delaware and New Hampshire's language, to cover businesses that, during the preceding calendar year: (i) controlled or processed the personal data of not less than thirty-five thousand consumers; or (ii) controlled or processed the personal data of not less than ten thousand consumers and derived more than twenty per cent of their gross revenue from the sale of personal data. Importantly, we believe the legislature should fully remove applicability thresholds for the processing of sensitive data and minors' data as it did in 2023 for "consumer health data" in SB3. All sensitive data and minors' data processing should be covered by the CTDPA and fall within the ambit of regulation.

Strengthen Data Minimization Provisions

The legislature should enhance the CTDPA's data minimization standard. We cannot underscore enough the importance of these provisions— in many cases, serious privacy and data security concerns could have been offset— if not fully alleviated— if companies had properly minimized the data they collected and maintained. Unfortunately, the CTDPA's current notice-and-consent model sets an exploitable standard— businesses can seek to justify unnecessary data collection by deeming such collection "adequate, relevant and reasonably necessary" to the purposes disclosed to consumers. This standard contravenes data minimization principles outright— it allows businesses to collect data they simply do not need so long as it is disclosed in privacy notices that are often bulky, confusing, or worse, misleading. We believe the legislature should amend the CTDPA to mirror Maryland's law, which limits collection to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer. Further, the legislature should limit the collection and processing of sensitive data to only when strictly necessary to provide or maintain a specific product or service requested by the consumer.

Expand Sensitive Data Definition

The legislature should expand Connecticut's definition of "sensitive data" to incorporate a comprehensive list of elements added by other states since the CTDPA's passage, including data categories like Social Security numbers, government-issued identifiers, union membership, status as transgender or non-binary, income level or indebtedness, and neural data. The CTDPA's heightened protections for sensitive data are a cornerstone of the law, and Connecticut residents deserve to be on the same footing as residents of other states.

Hand in hand with these updates, we again recommend that the legislature amend the CTDPA's definition for biometric data, a sensitive data element under the law. As a growing number of states have recognized, biometric data is sensitive if it can be used to identify an individual, even in circumstances where it is not affirmatively used to do so. The collection, sale, and use of biometric data raises serious privacy concerns for consumers that should trigger elevated protections.

Additionally, to reflect the realities of the online marketplace more accurately, we recommend removing the "known child" sensitive data element and replacing it with the "knows or has reason to know" standard enacted in Maryland. We have observed the ease with which companies disavow processing minors' data in their privacy notices, despite widely distributed press and reports describing consumer practices that contradict such statements.

Clarify and Strengthen Protections for Minors' Data

In our Initial Report, we asked the legislature to clarify whether it intended to ban targeted advertising to minors wholesale, or whether it intended that the opt-in consent qualifier applied to both sale and targeted advertising.[28] Through our work under the CTDPA as well as our broader privacy work, it has become more and more clear that targeted advertising to children and teens, and the sale of their personal data, should be banned. Further, we believe the "actual knowledge or willful disregard" standard throughout the CTDPA isa weakness of the law. Connecticut's protections should match those in Maryland, which prohibits businesses from sending targeted ads so long as the company "knew or should have known" that the individual is a minor. This "knew or should have known" standard is more fitting and mirrors the framework in CUTPA.

Further, we believe the legislature should update or remove other language in the CTDPA that jeopardizes privacy protections for minors. The rebuttable presumption framework creates an unnecessary hurdle for enforcement and is not appropriate in the context of minors' privacy, especially given that children and teens are uniquely vulnerable to privacy harms. Even beyond this issue, we believe the current consent structure in the CTDPA is inadequate for privacy protections related to minors. Should minors be able to "consent" to a system designed to "significantly increase, sustain or extend" minors' use of such online service, product or feature? [29] The fact that minors are not legally able to enter into contracts underscores why the consent structure should be removed.

Narrow "Publicly Available Information" Definition

As highlighted above, our Office continues to receive consumer complaints that unfortunately fall under the CTDPA's too-broad exemption for "publicly available information." In particular, these complaints involve websites that post individual profiles, combining public records like contact information and addresses, property records, court documents, and public social media posts, among others. 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 and, therefore, are not covered by the CTDPA. Further, data brokers routinely compile vast amounts of "public" consumer data to create inferences that are then sold to third parties. Consumers have little to no insight into how these profiles are used, but it has become increasingly clear that these practices can cause significant privacy harms.

We encourage the legislature to carveout from the definition of publicly available information: (i) information that is collated and combined to create consumer profiles on publicly available or subscription-based websites; (ii) information that is made available for sale; (iii) inferences generated from such information; and (iv) personal data that is created by combining personal data with publicly available information.

[28] 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, or wilfully disregards, that the consumer is at least thirteen years of age but younger than sixteen years of age." Conn. Gen. Stat. § 42-520(a)(7).
[29] See Conn. Gen. Stat. § 42-529a(b)(1)(B).

Add Right to Know Specific Third Parties

We urge the legislature to follow Oregon's lead by incorporating into the CTDPA a "right-to-know" the specific third parties that receive personal data from covered businesses. In addition, like Delaware, the legislature should update the CTDPA to provide Connecticut residents the ability to obtain a list of the categories of third parties to which the controller has disclosed that particular consumer's personal data. Through our investigations, we have learned that some controllers do not understand the breadth of third-party data sharing that happens through their online services and these heightened disclosure requirements would require more responsible data practices. Further, 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.

Expand the Utility of the OOPS Provisions and Enact a One-Stop-Shop Deletion Mechanism

Since January 1, 2025, Connecticut residents have had the right to opt out of targeted advertising and the sale of their personal data by sending their "opt out preference signal" to covered businesses. However, in practice, this right may only be exercised through certain privacy-protective browsers and browser extensions– none of which come preinstalled on consumer devices. This universal opt-out requirement should be readily available to all interested consumers. We recommendation amending the CTDPA's OOPS provisions to require all browser vendors and mobile operating systems include a setting which allows users to affirmatively send opt out preference signals. Since 2024, the California Privacy Protection Agency has supported such an effort and we join in this important initiative.

Similar to the universal opt-out requirement, a mechanism that allows Connecticut residents to exercise deletion rights at scale is sorely needed. The legislature should consider enacting a "one-stop-shop" deletion mechanism such as that contained in California's Delete Act, in order to allow Connecticut residents to delete their personal information held by data brokers through a single, verified request.

Conclusion

Connecticut remains at the forefront of consumer data privacy. Since passage of the CTDPA, the Privacy Section has worked to educate companies and consumers alike as well as learn about the practical applications of the law as written. We are focused on ensuring compliance with the CTDPA, including in key areas like transparency, opt-out rights, and sensitive data processing. We have also expanded our enforcement efforts as new legislation related to minors' privacy and consumer health data took effect, and as our universal opt-out provisions came online. It is clear that there is much to be done, including amending the CTDPA to provide stronger protections for Connecticut residents. We will continue to be transparent about our efforts to uphold this important law.