February 26, 2025

Co-Chair James Maroney
Co-Chair Roland Lemar
General Law Committee
Connecticut General Assembly
300 Capitol Avenue
Hartford, CT 06106

Re: *S.B. 1356 (An Act Concerning Data Privacy, Online Monitoring, Social Media And Data Brokers) - SUPPORT*

Dear Co-Chairs Maroney and Lemar,

Consumer Reports and the Electronic Privacy Information Center (EPIC) write in support of S.B. 1356 and sincerely thank you for your consideration of advancing consumer privacy in Connecticut. S.B. 1356 would build on the Connecticut Data Privacy Act (CTDPA) by extending to Connecticut consumers important new protections, including meaningful data minimization restrictions, improvements to key terms like "sensitive data" and "biometric data", removal of certain entity level exemptions, and more. These important amendments largely reflect the last several years of work on privacy legislation around the states, adopting targeted improvements made in other state privacy laws that incorporate feedback from regulators tasked with enforcing these laws, as well as other key stakeholders. They would raise the baseline of protection for consumers and should be adopted.

Consumer Reports and EPIC recently released a state model privacy bill that uses Connecticut's law as the baseline.[1] In part inspired by the Connecticut Attorney General's report to the General Law Committee in February of last year,[2] the model bill sought to identify areas in the CTDPA (often used as a model for other states to adopt) that could be improved to ensure that it meets its goal of providing strong consumer privacy protections. Several of the issues identified in our redline are addressed in S.B. 1356.

---

[1] Consumer Reports and EPIC, *The State Data Privacy Act*, https://epic.org/documents/the-state-data-privacy-act/.
[2] Conn. Att'y Gen., *Report to the General Assembly's General Law Committee Pursuant to Public Act 22-15, "An Act Concerning Personal Data Privacy and Online Monitoring" Referred to as the Connecticut Data Privacy Act ("CTDPA")*, https://portal.ct.gov/-/media/ag/press_releases/2024/ctdpa-final-report.pdf?rev=8fbba0ba237a42748d3ad6544fd8228c&hash=41BCE2F7485413487EE5F534E6AC6C60.

First and foremost, this bill's data minimization provision (Section 5(a)), which is aligned with Maryland's recently passed privacy law, would go a long way toward mitigating the rampant over-collection of consumer data that has led to a panoply of consumer harms.[3] A strong privacy law should limit the data companies can collect to match what consumers expect based on the context of their interaction with the business. For example, a mobile flashlight application should not be permitted to collect a consumer's precise geolocation information because such information is not necessary to provide the service requested and the collection of that data is unlikely to be in the consumer's interest.

In contrast, the core of the framework currently found in the CTDPA is "notice-and-choice," which focuses on disclosures in privacy policies. The law allows businesses to continue collecting whatever personal data they want and using it for any reason they want as long as they disclose those practices in their privacy policies and allow consumers to opt out. However, very few consumers have the time to read privacy policies in practice, and would likely struggle to decipher their lengthy legalese even if they did. Moreover, the opt-out framework offloads all of the burden of consumer protection onto consumers themselves, while absolving companies of the responsibility to engage in responsible data collection. Rather than continue with this approach that harms consumers, S.B. 1356 appropriately sets out a rule that businesses can only collect and use data when it is "reasonably necessary" to provide the services the consumer asks for.

While we prefer privacy legislation that limits companies' collection, use, *and* disclosure of data to what is reasonably necessary to provide the service requested by the consumer (the bill only currently applies this standard to data collection, while allowing a much looser standard for processing activities), simply reining in systemic overcollection of consumers' personal information alone would help eliminate common practices that have contributed to, among other things, the persistent drip of massive data breaches.[4]

Aside from this bill's thoughtful approach to minimization, we also appreciate that it includes the following elements:

- ***Expanded Definition of Sensitive Data.*** We support the expansion of the definition of sensitive data to include categories such as social security numbers, financial information, and status as nonbinary or transgender. These updates pull categories that other states have included in their definition of sensitive data and are common-sense additions of personal data that necessitate heightened protections.

---

[3] See, e.g., Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf; Consumer Financial Protection Bureau, Protecting Americans from Harmful Data Broker Practices (Regulation V), Proposed Rule; request for public comment, (December 3, 2024), https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf

[4] Joseph Cox, 404Media, Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data, (January 7, 2025), https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/;

- ***Improved Definition of Biometric Data.*** We applaud the updated definition of biometric data to include any data that *can be used* to identify an individual (not only if it is affirmatively used to do so). If biometric data such as a fingerprint is breached, it is no less sensitive simply because it was not previously used to identify an individual. This change is consistent with the Attorney General's recommendation, and with the Maryland Online Data Privacy Act.

- ***Lower Threshold.*** S.B. 1356 would lower the threshold for coverage so that the bill would apply to any businesses conducting business in the state that controls or processes the personal information of 35,000 consumers or that controls or processes the personal information of 10,000 consumers and that derives more than 20 percent of its revenue from the sale of sensitive data.[5] CTDPA's current baseline threshold of 100,000 consumer records means that Connecticut has one of the highest per-capita thresholds in the country, meaning that companies collecting a significant proportion of all Connecticut residents' data may still not be covered by the law. This change will expand protections for consumers, ensuring that large national companies with a moderately sized footprint on Connecticut will be required to abide by the law. This change will align Connecticut with several other states that have recently passed privacy laws with similar thresholds, including Maryland, Rhode Island, and New Hampshire.

- ***Removal of Entity Level Exemptions.*** CTDPA currently exempts from coverage any financial institution or an affiliate of a financial institution, as defined in the Gramm-Leach-Bliley Act, as well as covered entities and business associates under the Health Insurance Portability and Accountability Act. These carveouts arguably make it so that large tech companies (Apple, Amazon, Google, Facebook, and Microsoft) would be exempted from the entire law if one arm of their business receives enough financial information from banks or crosses the threshold into providing traditional healthcare services, a line many of them are already currently skirting. S.B. 1356 would amend the law to only exempt *information* that is collected pursuant to those laws, applying its protections to all other personal data collected by such entities that is not currently protected by other laws.

At the same time, we urge the drafters to strengthen the bill by adding the following protections, which are necessary to provide Connecticut consumers with the level of protection they deserve:

- ***Create Stronger Protections for Sensitive Data.*** The bill should build on the underlying data minimization standard by requiring that the collection and processing of any *sensitive* information be "strictly necessary" to provide the service requested by the consumer and by banning the sale of sensitive data outright, as was done in the Maryland Online Data Privacy Act. These will reduce the outward flow of data about our most personal characteristics, including our health, precise geolocation, race, religious beliefs, and data from children, and shift the burden of privacy protection away from consumers and toward companies that otherwise have every incentive to exploit consumer data for their own

[5] Note, Section 2(3) of the bill appears to extend coverage to any business that sells personal data, which conflicts with this provision.

benefit. The less sensitive information companies collect and sell about us in the first place, the less that can be used against us and the less that can be exposed in a data breach.

- ***Improve the Definition of Targeted Advertising.*** We recommend refining the definition of "targeted advertising" to better match consumer expectations of the term. The current definition potentially opens a loophole for data collected on a single site; it only includes ads based on a "consumer's activities over time and across nonaffiliated **websites**" (plural, emphasis ours). This may exempt "retargeted" ads from the scope of the bill's protections — ads based on one particular product you may have considered purchasing on another site. Such advertising — such as a pair of shoes that follows you all over the internet after you had left a merchant's site — are the stereotypical example of targeted advertising; the law's opt-out provisions should certainly apply to it. We suggest a shift toward the following definition:

> *"Targeted advertising" means displaying or presenting an online advertisement to a consumer or to a device identified by a unique persistent identifier (or to a group of consumers or devices identified by unique persistent identifiers), if the advertisement is selected based, in whole or in part, on known or predicted preferences, characteristics, behavior, or interests associated with the consumer or a device identified by a unique persistent identifier.*
>
> *"Targeted advertising" includes displaying or presenting an online advertisement for a product or service based on the previous interaction of a consumer or a device identified by a unique persistent identifier with such product or service on a website or online service that does not share common branding with the website or online service displaying or presenting the advertisement, and marketing measurement related to such advertisements.*
>
> *"Targeted advertising" does not include:*
> *(A) first-party advertising; or*
> *(B) contextual advertising.*

Thank you again for your consideration, and for your work on this legislation. We look forward to working with you to ensure that Connecticut residents have the strongest possible privacy protections.

Sincerely,

Matt Schwartz
Policy Analyst, Consumer Reports

Caitriona Fitzgerald
Deputy Director, EPIC