February 3, 2026

Chair Patrick Stefano
Minority Chair Lisa Boscola
Senate Consumer Protection & Professional Licensure Committee
Room 8E-A, East Wing
501 N. 3rd Street
Harrisburg, PA 17120

Re: H.B. 78, Consumer Privacy Legislation - *OPPOSE UNLESS AMENDED*

Dear Chair Stefano and Minority Chair Boscola,

Passing a strong comprehensive privacy law is critical to protect the personal information of Pennsylvania residents, presenting the state with an opportunity to showcase its leadership on this important issue. However, the current draft of H.B. 78 is outdated, ignoring improvements made in other jurisdictions with otherwise similar privacy laws that close well-known enforcement loopholes and remedy unsatisfactory consumer experiences. In our view, approving this legislation without significant changes would be worse than doing nothing, since the bill, as written, would mostly provide an illusion of privacy without the substance to back it up.

Consumer Reports and the Electronic Privacy Information Center (EPIC) have therefore identified several key areas where amendments would enhance the effectiveness and clarity of H.B. 78. The proposed changes are intended to strengthen privacy protections and ensure that the legislation achieves its goals without unintended consequences. Below, we outline several of the key changes for your consideration. We recognize the challenges of balancing the equities between diversely positioned stakeholders in a divided legislature, but are hopeful that progress can be made. We've listed our suggested changes in order of priority.

1. **Limit data abuse – don't allow businesses to hide harmful practices in long privacy policies**

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 troves of personal information because such information is not necessary to provide the service requested, it's unexpected, and the collection of that data is unlikely to be in the consumer's interest. By contrast, H.B. 78 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.

This very dynamic was highlighted by the Connecticut Office of the Attorney General in its recent enforcement report, where it recommended legislative amendments to strengthen the CTDPA, stating that the: "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."[1]

Pennsylvania should join the other states, like Maryland and California, that have attempted to create a more workable standard for consumers. We suggest including the below language, adapted from Maryland:

Section 5(a)(1): Limit the collection of personal data to what is ~~adequate, relevant and~~ reasonably necessary to provide or maintain: ~~in relation to the purposes for which the data is processed, as disclosed to the consumer.~~

(A) a specific product or service requested by the consumer to whom the data pertains including any routine administrative, operational, or account-servicing activity, such as billing, shipping, delivery, storage, or accounting;
(B) a communication, that is not an advertisement, by the controller to the consumer reasonably anticipated within the context of the relationship between the controller and the consumer;
(C) a purpose permitted under Section 9 of this Act.

Except with respect to sensitive data, a controller may process or transfer personal data collected under this subsection to provide first-party advertising or targeted advertising; provided, however, that this paragraph does not permit the processing or transfer of personal data for targeted advertising to a consumer who has opted out of such advertising pursuant to section 3 or to a consumer under circumstances where the controller knew or should have known, based on knowledge fairly implied under objective circumstances, that the consumer is a minor.

[1] Connecticut Office of the Attorney General, Updated Enforcement Report Pursuant To Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-515, Et Seq, (April 17, 2025), https://portal.ct.gov/-/media/ag/press_releases/2025/updated-enforcement-report-pursuant-to-connecticut-data-privacy-act-conn-gen-stat--42515-et-seq.pdf

2. **Add meaningful enforcement, including a private right of action for large data holders**

Consumers should be able to hold companies accountable in some way for violating their rights. Unfortunately, most state Attorney General offices are under-resourced and do not have the capacity to bring enough actions to meaningfully deter illegal behavior, meaning consumers may have no recourse in the event of a violation that harms them. Despite ample evidence suggesting widespread non-compliance with existing privacy laws, there have not been commensurate enforcement efforts to-date. Consumer Reports has put out a number of reports demonstrating noncompliance with state privacy laws, including a recent report showing that many companies were showing targeted ads despite receiving legally binding universal opt-out signals.[2] Yet, there have been very few public enforcement actions to-date, so it is unsurprising that market behavior has yet to improve.

That said, we understand the desire to protect local small businesses from potentially costly litigation and are therefore proposing exempting all businesses from the private right of action except those making over $1 billion in annual revenues. In our view, this structure creates a fair, risk-based compromise. Smaller businesses are less likely to be engaging in the type of extensive and risky data processing performed by their larger competitors or Big Tech companies. This structure protects businesses with fewer resources from being exposed to the threat of private litigation while ensuring that the higher-risk companies (who also have more resources to weather lawsuits) are encouraged to comply in order to avoid such litigation.

3. **Include a ban on the sale of sensitive data**

Please consider including an outright ban on the sale of "sensitive data," which would match the standard set in Maryland and Oregon's comprehensive privacy laws and would prevent data about children, our precise geolocation, our health, and political or religious affiliations from being used against us. Other state privacy laws have "opt-in" frameworks for consumers' sensitive data, but these provisions aren't working. A prohibition on selling sensitive data should allow companies to transfer this data for legitimate business purposes—like a retailer sharing sensitive financial information with a payment processor—while eliminating data sales that serve only to increase profits rather than to benefit consumers. Under existing opt-in frameworks, companies aren't typically required to separate their request for consent for necessary processing (e.g. data collection) from unnecessary processing (e.g. data sales), so consumers are still often presented with take-it-or-leave-it choices that don't leave them any better off than before.

[2] Matt Schwartz et al., Consumer Reports, Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws, https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf, (April 1, 2025)

This weakness became apparent to many consumers last week when TikTok's transfer to a U.S. entity prompted a new pop-up notice for TikTok users. Upon opening the app, users were presented with a notice that TikTok was updating its Terms of Service and Privacy Policy to reflect changes including "new types of location information (including device geolocation) we may collect from you, with your permission" as well as changes to advertising practices. There was no "disagree" button—instead users had to agree or simply delete the app. That's not a real choice, particularly for other apps that may be required for work, school, or other life necessities.

And ultimately, more consent boxes aren't the solution to this issue. In addition to Maryland and Oregon's laws, other states, including Maine, Vermont, and Massachusetts, are also considering banning the sale of sensitive data.

Suggested language:

> *Section 5(a)(9):* *Notwithstanding Section 5(a)(4), a controller shall not sell a consumer's sensitive data.*

4. Improve Definition of Targeted Advertising

We recommend refining the definition of "targeted advertising" to better match consumer expectations of the term. The drafted 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). Some businesses may argue that this therefore exempts "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 have left a merchant's site—is the stereotypical example of targeted advertising; the law's opt-out provisions should certainly apply to it. Note, first-party data collection ("Advertisements based on activities within a controller's own Internet websites or online application") is already exempted under the definition).

We suggest the following changes:

"Targeted advertising." Displaying advertisements to a consumer or to a device identified by a unique persistent identifier if the advertisement is selected based on personal data obtained or inferred from the consumer or device identified by a unique persistent identifier's activities ~~over time and across nonaffiliated Internet websites or online applications~~ to predict the consumer's preferences or interests.

5. Close Loophole that Allows Business to Ignore Consumer Requests Related to Loyalty Programs

We encourage you to narrow the types of discrimination that are allowed under Section (5)(b). For example, it's reasonable that consumers may be denied participation in a loyalty program if they have chosen to use their privacy rights to delete information or deny consent for processing that is functionally necessary to operate that loyalty program. That is, if you erase a record of having purchased nine cups of coffee from a vendor, you cannot expect to get the tenth cup for free. However, generally controllers do not need to sell data to others or to engage in cross-context behavior advertising in order to operate a bona fide loyalty program—such behaviors have nothing to do with the tracking of purchases to offer discounts or first-party advertising.

We recommend the following definition:

Section(5)(b): Nothing in this section shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a financial incentive program such as a bona fide loyalty, rewards, premium features, discounts or club card program, provided that the controller may not transfer personal data to a third party as part of such program unless: (1) The transfer is functionally necessary to enable the third party to provide a benefit to which the consumer is entitled; (2) the transfer of personal data to the third party is clearly disclosed in the terms of the program; and (3) the third party uses the personal data only for purposes of facilitating a benefit to which the consumer is entitled and does not process or transfer the personal data for any other purpose. The sale of personal data shall not be considered functionally necessary to provide a financial incentive program. A controller shall not use financial incentive practices that are unjust, unreasonable, coercive or usurious in nature.

Alternatively, you could consider using the following formulation from Maryland's law:

A controller shall refrain from discriminating against a consumer for exercising any of the consumer rights under section 3(a), including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer, provided that the selling of personal information is not a condition of participation in the program.

6. **Remove Entity-Level Carveouts**

The bill 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 bill 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. At most, the bill should exempt information that is collected pursuant to those laws (as is done in Section 11(b)(1) for HIPAA-covered data), applying its protections to all other personal data collected by such entities that is not currently protected. Similarly, we would encourage you to remove the entity-level exemption for nonprofits. Many large organizations, including OpenAI and the College Board, that process massive amounts of personal data claim nonprofit status. All entities should be required to be responsible data-holders, regardless of whether they are for-profit or nonprofit. CA, CA, NJ, MD, MN, OR, and DE have all limited exemptions in at least one of these ways.

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

Sincerely,

Matt Schwartz
Senior Policy Analyst
Consumer Reports

Caitriona Fitzgerald
Deputy Director
Electronic Privacy Information Center (EPIC)