June 25, 2024

Chair Tracy Pennycuick
Minority Chair Jimmy Dillon
Communications and Technology Committee
Pennsylvania Senate
462 Main Capitol Building
Harrisburg, PA 17120

Re: H.B. 1201, Pennsylvania Consumer Privacy Legislation - *OPPOSE*

Dear Chair Pennycuick, Minority Chair Dillon, and Members of the Communications and Technology Committee,

Consumer Reports writes in respectful opposition to H.B. 1201. The bill seeks to provide to Pennsylvania consumers the right to know the information companies have collected about them, the right to access, correct, and delete that information, as well as the right to stop the disclosure of certain information to third parties. However, in its current form it would do little to protect Pennsylvania consumers' personal information, or to rein in major tech companies like Google and Facebook. The bill needs to be substantially improved before it is enacted; otherwise, it would risk locking in industry-friendly provisions that avoid actual reform.

Consumers currently possess very limited power to protect their personal information in the digital economy, while online businesses operate with virtually no limitations as to how they collect and process that information (so long as they note their behavior somewhere in their privacy policy). As a result, consumers' every move is constantly tracked and often combined with offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual orientation. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and enables opaque algorithmic scoring—all of which can lead to disparate outcomes along racial and ethnic lines.

At the same time, spending time online has become integral to modern life, with many individuals required to sign up for accounts with tech companies because of school, work, or simply out of a desire to connect with distant family and friends. Consumers are offered the illusory "choice" to consent to company data processing activities, but in reality this is an all or nothing decision; if you do not approve of any one of a company's practices, your only choices are to either forgo the service altogether or acquiesce completely.

We therefore offer several suggestions to strengthen the bill to provide the level of protection that Pennsylvania consumers deserve:

- *Include strong data minimization rules to limit collection and use of personal data.* Privacy laws should set strong limits on the data that companies can collect and share so that consumers can use online services or apps safely without having to take any action, such as opting in or opting out. We recommend including a strong data minimization requirement, like that recently passed as part of comprehensive legislation in Maryland, that limits data collection to what is reasonably necessary to provide the service requested by the consumer, similar to the standard outlined in Consumer Reports' model bill.[1] In addition, a strong default prohibition on unnecessary data sharing is preferable to an opt-out based regime which relies on users to hunt down and navigate divergent opt-out processes for every business with which they interact.

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* In the absence of strong data minimization requirements, at the very least, H.B. 1201's opt-out should cover all data transfers to a third party for a commercial purpose (with narrowly tailored exceptions). In California, many companies have sought to avoid the CCPA's opt-out requirements by claiming that much online data sharing is not technically a "sale" (appropriately, CPRA expands the scope of California's opt-out to include all data sharing and clarifies that targeted ads are clearly covered by this opt out).[2] We recommend including "sharing" in H.B. 1201's opt-out right and using the following definition:

  > *"Share" [or sell] means renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.*

  We also recommend refining the definition of "targeted advertising" to better match consumer expectations of the term. The drafted definition 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**" (emphasis ours). This would open the argument that the text 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 had left a merchant's site — are the stereotypical example of targeted advertising;

---

[1] Model State Privacy Act, Consumer Reports, (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/

[2] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously, supra* note 3, Medium (January 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.

the law's opt-out provisions should certainly apply to it. We suggest a shift toward the following definition:

> *"Targeted advertising" means the targeting of advertisements to a consumer based on the consumer's activities with one or more businesses, distinctly-branded websites, applications or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts. It does not include advertising: (a) Based on activities within a controller's own commonly-branded websites or online applications; (b) based on the context of a consumer's current search query or visit to a website or online application; or (c) to a consumer in response to the consumer's request for information or feedback.*

- *Narrow the loyalty program exemption.* We are concerned that the exception to the anti-discrimination provision when a consumer voluntarily participates in a "bona fide reward, club card or loyalty program" (Section 5(b)) is too vague and could offer companies wide loopholes to deny consumer rights by simply labeling any data sale or targeted advertising practice as part of the "bona fide loyalty program." We urge the sponsors to adopt a more precise definition and to provide clearer examples of prohibited behavior that does not fall under this exception. For example, it's reasonable that consumers may be denied participation in a loyalty program if they have chosen to delete information or deny consent for processing 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-site targeted 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.

  Loyalty programs take advantage of the exact type of informational asymmetry that privacy law should strive to eliminate. While consumers typically view loyalty programs as a way to save money or get rewards based on their repeated patronage of a business, they rarely understand the amount of data tracking that can occur through such programs.[3] For example, many grocery store loyalty programs collect information that go far beyond mere purchasing habits, sometimes going as far as tracking consumer's precise movements within a physical store.[4] This information is used to create detailed user profiles and is regularly sold to other retailers, social media companies, and data brokers, among others. Data sales are extremely profitable for such entities — Kroger estimates that its "alternative profit" business streams, including data sales, could earn it $1 billion annually.[5] At a minimum, businesses should be

[3] Joe Keegan, *Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You,* The Markup, (February 16, 2023), https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you
[4] Ibid.
[5] Ibid.

required to give consumers control over how their information is collected and processed pursuant to loyalty programs, including the ability to participate in the program without allowing the business to sell their personal information to third-parties.

- *Remove the right to cure from the Attorney General enforcement section and add a private right of action*. The "right to cure" provisions from the administrative enforcement sections of the bill should be removed — as Proposition 24 removed similar provisions from the CCPA.[6] In practice, the "right to cure" is little more than a "get-out-of-jail-free" card that makes it difficult for the AG to enforce the law by signaling that a company won't be punished the first time it's caught breaking the law. In addition, consumers should be able to hold companies accountable in some way for violating their rights—there should be some form of a private right of action.

- *Apply authorized agent provisions to rights to access, correct, and delete.* H.B. 1201 currently only allows authorized agents to send requests to opt-out, meaning for all other rights requests consumers must go to each business they interact with one by one and navigate its bespoke system. This means requests to access, correct, and delete are impractical to use at scale, especially when the law allows businesses to ask for onerous documentation to complete the request. The purpose of authorized agents is to cut down on the amount of time that each consumer must spend haggling with individual businesses to accept their rights requests, ultimately making those rights much more usable for consumers. CPRA includes a provision that extends authorized agent rights to all consumer rights under the act that Pennsylvania could emulate.[7]

- *Eliminate entity level carveouts*. The draft bill currently exempts from coverage any financial institution or an affiliate of a financial institution covered by the privacy provisions of 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.[8] The bill already carves out from coverage information that is collected pursuant to those laws, so the need to exempt entire entities is unnecessary.

- *Remove ambiguities around requirements that the universal opt out mechanism not "unfairly disadvantage" other controllers*. The bill requires controllers to allow consumers

---

[6] At the very least, the right to cure should be reduced to 30 days before the sunset period elapses. See Public Act No. 22-15, Section 11(b), https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF

[7] See California Civil Code 1798.130 A(3)(a), https://cpra.gtlaw.com/cpra-full-text/

[8] See e.g., The Economist, "Big Tech Pushes Further into Finance," (Dec. 15, 2022), https://www.economist.com/business/2022/12/15/big-tech-pushes-further-into-finance; Richard Waters, "Big Tech searches for a way back into healthcare," Financial Times, (May 17, 2020), https://www.ft.com/content/74be707e-6848-11ea-a6ac-9122541af204

to opt out of sales and targeted advertising through an opt-out preference signal (OOPS). However, Section 5(e)(1)(ii)(A) proceeds to confusingly prohibit OOPSs from "unfairly disadvantag[ing]" other controllers in exercising consumers' opt-out rights. It is unclear what "unfairly disadvantage" might mean in this context, as by their definition mechanisms that facilitate global opt-outs "disadvantage" some segment of controllers by limiting their ability to monetize data. Consumers should be free to utilize OOPSs to opt out from whatever controllers they want. For example, a consumer may want to use a certain OOPS that specifically opts them out from data brokers (or may configure a general purpose mechanism to only target data brokers); in that case, a consumer (and the OOPS) should be empowered to only send opt-out requests to data brokers. The term "unfairly" introduces unnecessary ambiguity and the subsection should be eliminated.

- *Amend prohibitions on default opt-outs*. Currently, Section 5(e)(1)(ii)(B) states that OOPSs cannot send opt-out requests or signals by default. The bill should be amended to clarify that the selection of a privacy-focused user agent or control should be sufficient to overcome the prohibition on defaults; an OOPS should not be required to specifically invoke Pennsylvania law when exercising opt-out rights. OOPSs are generally not jurisdiction-specific — they are designed to operate (and exercise relevant legal rights) in hundreds of different jurisdictions. If a consumer selects a privacy-focused browser such as Duck Duck Go or Brave — or a tracker blocker such as Privacy Badger or Disconnect.me — it should be assumed that they do not want to be tracked across the web, and they should not have to take additional steps to enable the agent to send a Pennsylvania-specific opt-out signal. Such a clarification would make the Pennsylvania law consistent with other jurisdictions such as California and Colorado that allow privacy-focused agents to exercise opt-out rights without presenting to users a boilerplate list of all possible legal rights that could be implicated around the world.

- *Clarify that approximating geolocation by IP address is sufficient residency authentication*. Section 5(e)(1)(ii)(E) provides that an OOPS must "[e]nable the controller to accurately determine whether the consumer is a resident of this state" and has made a legitimate request. Today, companies generally comply with state and national privacy laws by approximating geolocation based on IP address. The drafters should revise the legislation to clearly state that estimating residency based on IP address is generally sufficient for determining residency and legitimacy, unless the company has a good faith basis to determine that a particular device is not associated with a Pennsylvania resident or is otherwise illegitimate.

- *Include strong civil rights protections.* A key harm observed in the digital marketplace today is the disparate impact that can occur through processing of personal data for the purpose of creating granularized profiles of individuals based off of data both collected and inferred about them. Therefore a crucial piece of strong privacy legislation is ensuring that a business' processing of personal data does not discriminate against or otherwise makes opportunity or public accommodation unavailable on the basis of

protected classes. Strong protections against discrimination and algorithmic bias have been a staple of federal privacy bills in recent years, in both bipartisan bills as well as partisan bills put forward by Republicans or Democrats alike.[9] Legislation passed into law in Maryland also includes similar language.[10]

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
Policy Analyst

[9] E.g. Rep. Pallone, Rep. Rodgers, Rep. Schakowsky, Rep. Bilirakis, H.R. 8152, American Data Privacy and Protection Act, (117th Congress), https://www.congress.gov/117/bills/hr8152/BILLS-117hr8152rh.pdf; E.g. Control Our Data Act, (117th Congress), https://web.archive.org/web/20220601033730/https://republicans-energycommerce.house.gov/wp-content/uploads/2021/11/2021.11.02-Republican-CODA-Draft-.pdf; E.g. Sen. Cantwell, S. 2968, Consumer Online Privacy Rights Act, (116th Congress) https://www.congress.gov/116/bills/s2968/BILLS-116s2968is.pdf

[10] Maryland S.B. 541, Section 14-4607(A)(7) https://mgaleg.maryland.gov/2024RS/bills/sb/sb0541E.pdf