February 13, 2024

Chair Pamela Beidle
Vice Chair Katherine Klausmeier
Finance Committee
Maryland Senate
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Re: S.B. 541 Maryland Online Data Privacy Act - SUPPORT WITH AMENDMENTS

Dear Chair Beidle, Vice Chair Klausmeier, and Members of the Finance Committee,

Consumer Reports[1] sincerely thanks you for your work to advance consumer privacy in Maryland. S.B. 541 would extend to Maryland consumers important new protections, including meaningful data minimization restrictions, heightened standards for the processing of sensitive data, and strong civil rights protections. The bill also creates baseline consumer privacy rights, including the right to know the information companies have collected about them, the right to access, correct, and delete that information, as well as the ability to require businesses to honor universal opt-out signals and authorized agent requests to opt out of sales, targeted advertising, and profiling.

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 process that information (so long as they note their behavior somewhere in their privacy policy). As a result, consumers are constantly tracked online and their behaviors are often combined with offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual preferences. 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 erode individuals' basic expectation of privacy and can lead to disparate outcomes along racial and ethnic lines.

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

This bill's data minimization provision (Section 14-4607 (B)(1)(I)) surpasses many other states' and would go a long way toward mitigating many of these types of harms. 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)[2], simply reigning in systemic over-collection of consumers' personal information alone would help eliminate common practices that have contributed to, among other things, the persistent drip of massive data breaches.

Suitably, S.B. 541 also seeks to reduce unwanted secondary processing of data by creating a framework for universal opt-out through universal controls. Privacy legislation with universal opt-outs empowers consumers by making it easier to set their preferences relating to secondary processing, like sales or targeted advertising, eliminating the need for them to manage the otherwise untenably complicated ecosystem of privacy notices, opt-out requests, and verification.[3] The goal of universal opt-out is to create an environment where consumers can set their preference once and feel confident that businesses will honor their choices as if they contacted each business individually.

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

- *Special Protections for Sensitive Data.* The bill builds on the underlying data minimization standard by requiring that the collection, processing, or sharing of any *sensitive* information be "strictly necessary" to provide the service requested by the consumer and that the controller obtain consent prior to undertaking any of these activities. These restrictions would effectively ban third-party targeted advertising and data sales based on our most personal characteristics, including data about our race, religious beliefs, health data, and data about children (targeted advertising to teens is also separately banned), which would represent a major change to the digital ecosystem, appropriately shifting the burden of privacy protection away from consumers themselves to companies that otherwise have every incentive to exploit consumer data for their own benefit. While we have concerns that this section's opt-in consent provisions may introduce unnecessary consent fatigue (if data processing is truly limited to providing what the consumer asked for, why should they need to consent on top of that), we support the intent of this provision wholeheartedly.

---

[2] Section 14-4607(9) of the bill ostensibly includes data minimization language restricting processing activities; however, because data processing is limited to any purpose listed by a company in its privacy policy — instead of to what is reasonably necessary to fulfill a transaction — that language will in practice have little effect for secondary purposes after data is collected.

[3] Aleecia M. McDonanld and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," I/S: A Journal of Law and Policy for the Information Society, vol. 4, no. 3 (2008), 543-568. https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf?sequence=1&isAllowed=y

We also note that Section 14-4604 (4) should be eliminated, since consumer health data is included as a category of sensitive data, and sales of sensitive data would never be "strictly necessary" to provide or maintain a service.

- *Strong civil rights protections.* This bill appropriately addresses a key harm observed in the digital marketplace today: 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. The bill ensures that a business' processing of personal data cannot lead to discrimination against individuals or otherwise make opportunity or public accommodation unavailable on the basis of protected classes. A number of privacy bills introduced federally in recent years have included similar civil rights protections, including the American Data Privacy and Protection Act which overwhelmingly passed the House Energy and Commerce Committee on a 53-2 bipartisan vote.[4] Consumer Reports' Model State Privacy Legislation also contains similar language prohibiting the use of personal information to discriminate against consumers.[5]

At the same time, the legislation still contains several loopholes that would hinder its overall effectiveness. We offer several suggestions to strengthen the bill to provide the level of protection that Maryland consumers deserve:

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* S.B. 541'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).[6] We recommend including "sharing" in S.B. 541'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

[4] See Section 2076, Amendment in the Nature of a Substitute to the American Data Privacy and Protection Act, https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf
[5] See Sections 125 and 126, Consumer Reports, Model State Privacy Act, (Feb. 2021) https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf
[6] Id.

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 would 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 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.*

- *Add a private right of action.* Given the AG's limited resources, a private right of action is key to incentivizing companies to comply. Under an AG-only enforcement framework, businesses that recognize that the AG is only capable of bringing a handful of enforcement actions each year might simply ignore the law and take their chances in evading detection. Further, it's appropriate that consumers are able to hold companies accountable in some way for violating their rights. We strongly encourage legislators to include a private right of action in future drafts of the legislation.

- *Eliminate the GLBA carveout .* The bill currently exempts from coverage any financial institution or an affiliate of a financial institution, as defined in the Gramm-Leach-Bliley Act. This carveout makes 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 crosses the threshold into providing traditional financial services, a line many of them are already skirting, if not already well past.[7] The bill should instead simply provide an exemption for *information* that is collected pursuant to GLBA, as was done with HIPAA covered data.

- *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 loyalty, rewards, premium features, discounts, or club card program" (Section 14-4607(c)(2)) is too vague and could offer companies wide loopholes to deny or discourage 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 provide clearer examples of prohibited discrimination that

[7] 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,

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 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.

Loyalty programs take advantage of the exact type of informational asymmetry that privacy laws 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.[8] 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.[9] 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.[10] At a minimum, businesses should be 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.[11]

- *Remove ambiguities around requirements that the universal opt out mechanism not "unfairly disadvantage" other controllers*. The bill requires controllers to allow consumers to opt out of sales and targeted advertising through an opt-out preference signal (OOPS). However, the bill would also 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

[8] 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
[9] ibid.
[10] ibid.
[11] See Consumer Reports' model State Privacy Act, Section 125(a)(5) for an example of a concise, narrowly-scoped exemption for loyalty programs. https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/

term “unfairly” introduces unnecessary ambiguity and the subsection should be eliminated.

- *Amend prohibitions on default opt-outs*. Currently, the bill 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 Maryland 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 Maryland-specific opt-out signal. Such a clarification would make the Maryland 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.

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

Sincerely,
Matt Schwartz
Policy Analyst