May 17, 2023

Chair Kirsta Griffith
Vice Chair Cyndie Romer
Technology and Telecommunications Committee
Delaware House of Representatives
411 Legislative Avenue
Dover, DE 19901

Re: H.B. 154, the Delaware Personal Data Privacy Act - SUPPORT IF AMENDED

Dear Chair Griffith, Vice Chair Romer, and Members of the House Technology and Telecommunications Committee,

Consumer Reports and Consumer Federation of America sincerely thank you for your work to advance consumer privacy in Delaware. H.B. 154 would extend to Delaware consumers important new protections, 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 authorized agents' browser privacy signals as an opt out of sale and targeted advertising.

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.

While we prefer privacy legislation that limits companies' collection, use, and disclosure of data

to what is reasonably necessary to operate the service (i.e. data minimization)[1] or that at least restricts certain types of processing (sales, targeted advertising, and profiling), we appreciate that H.B. 154 creates a framework for universal opt-out through universal controls and authorized agents. Privacy legislation with universal opt-outs empowers consumers by making it easier to manage the otherwise untenably complicated ecosystem of privacy notices, opt-out requests, and verification.[2] 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.

Measures largely based on an opt-out model with no universal opt-out, like the original interpretation of the California Consumer Privacy Act (CCPA), would require consumers to contact hundreds, if not thousands, of different companies in order to fully protect their privacy. Making matters worse, Consumer Reports has documented that some companies' opt-out processes are so onerous that they have the effect of preventing consumers from stopping the sale of their information.[3]

Despite H.B. 154's thoughtful approach to opt-outs, the legislation contains significant loopholes that would hinder its overall effectiveness. We offer several suggestions to strengthen the bill to provide the level of protection that Delaware consumers deserve.

- *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 12D-106(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.

---

[1] Section 12D-106 (a)(1) of the bill ostensibly includes data minimization language; 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.

[2] 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

[3] Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Rights Protected, CONSUMER REPORTS (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf .

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.[4] 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.[5] 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.[6] 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.

- *Limit authentication requirements to requests to access, correct, and delete*. Section 12D-104(c)(4) allows (though does not require for opt outs) controllers to authenticate consumer requests to exercise their rights under the act. This may be appropriate when consumers are requesting to access, delete, or correct their information, since fraudulent requests for these rights can pose real consumer harm. However, opt-out rights do not carry similar risks to consumers and therefore should not be subjected to this heightened standard. In the past, businesses have used authentication clauses to stymie rights requests by insisting on receiving onerous documentation.[7] For example, in Consumer Reports's investigation into the usability of new privacy rights in California, we found examples of companies requiring consumers to fax in copies of their drivers' license in order to verify residency and applicability of CCPA rights. Controllers should be required to honor opt-out requests without any authentication.

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* H.B. 154'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

---

[4] 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

[5] Ibid.

[6] Ibid.

[7] 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.

this opt out).[8] We recommend including "sharing" in H.B. 154'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.*

While we appreciate that this measure has an opt-out for targeted advertising, the current definition of targeted advertising could allow internet giants like Google, Facebook, and Amazon to serve targeted ads based on their own vast data stores on other websites. This loophole would undermine privacy interests and further entrench dominant players in the online advertising ecosystem. We recommend using 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.*

- *Remove the right to cure from the Attorney General enforcement section*. 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.[9] 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. 154 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

---

[8] 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.

[9] At the very least, the right to cure should be reduced to 30 days and sunset like it does under the Connecticut Data Privacy Act. See Public Act No. 22-15, Section 11(b), https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF

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 Delaware could emulate.[10]

- *Eliminate the financial institution carveout*. The draft bill currently exempts from coverage any financial institution or an affiliate of a financial institution, as defined in the Gramm-Leach-Bliley Act (GLBA). This carveout arguably 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 receives enough financial information from banks to become an "affiliate" under GLBA, a line many of them are already currently skirting.[11] We appreciate that the bill limits its HIPAA-related carveouts to the information already protected by HIPAA and we urge drafters to apply the same logic to financial institutions.

- *Remove ambiguities around requirements that the universal opt out mechanism not "unfairly disadvantage" other controllers*. Section 12D-106(e)(1)(a)(2) requires controllers to allow consumers to opt out of sales and targeted advertising through an opt-out preference signal (OOPS). However, Section 12D-106(e)(1)(a)(2)(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 are "disadvantaging" 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 12D-106(e)(1)(a)(2)(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 Delaware 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

[10] See California Civil Code 1798.130 A(3)(a), https://cpra.gtlaw.com/cpra-full-text/
[11] 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

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 Delaware-specific opt-out signal. Such a clarification would make the Delaware 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 12D-106(e)(1)(a)(2)(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 an Delaware 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. A number of privacy bills introduced federally in recent years have included such 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.[12] Consumer Reports' Model State Privacy Legislation also contains specific language prohibiting the use of personal information to discriminate against consumers.[13]

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

Sincerely,
Consumer Reports
Consumer Federation of America

---

[12] 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

[13] 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