March 6, 2025

Representative Jon Burns
Speaker of the House
Georgia House of Representatives
332 State Capitol
Atlanta, GA 30334

Re: S.B 111, Georgia Consumer Privacy Protection Act - OPPOSE

Dear Speaker Burns,

Consumer Reports and the Electronic Privacy Information Center (EPIC) write in respectful opposition to S.B. 111, consumer privacy legislation that recently passed a Senate vote. The Georgia Consumer Privacy Protection Act seeks to provide to Georgia 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 Georgia 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, religious beliefs, and even their precise geolocation. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and enables opaque algorithmic scoring.

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.

S.B. 111 would require several strengthening amendments to provide the level of protection that Georgia consumers deserve, including:

- *Include meaningful data minimization provisions, or at least require companies to honor browser privacy signals as opt outs.* Privacy laws should set strong default limits on the data that companies can collect and use so that consumers can use online services or apps safely without having to take any action, such as opting in or opting out. For this reason, we recommend that privacy laws include a strong data minimization requirement that limits data collection and use to what is reasonably necessary to provide the service requested by the consumer, as outlined in Consumer Reports and EPIC's model bill.[1] A strong default prohibition on unwanted data sharing is preferable to an opt-out based regime which relies on users to hunt down and navigate divergent opt-out processes for potentially thousands of different companies.

  However, if the drafters are intent on using an opt-out standard, consumers at least need tools, like universal opt out mechanisms (UOOMs), to ensure that they can exercise their rights in a meaningful way. UOOMs allow consumers to broadcast to businesses they interact with online their preference to opt out from their personal information being sold or shared with third parties through a simple toggle. Covered businesses are then expected to comply with the signal as if the consumer individually contacted them. The majority of state comprehensive privacy laws now include such a provision, including recently passed laws in Montana, Nebraska, and Texas.[2]

  Privacy researchers, advocates, and publishers have already created a "do not sell" specification designed to work with such frameworks, the Global Privacy Control (GPC).[3] This could help make the opt-out model more workable for consumers,[4] but unless companies are required to comply, it is unlikely that consumers will benefit. We recommend using the following language:

---

[1] Consumer Reports and the Electronic Privacy Information Center unveil new model legislation to protect the privacy of American consumers, (September 24, 2024), https://advocacy.consumerreports.org/press_release/consumer-reports-and-the-electronic-privacy-information-center-unveil-new-model-legislation-to-protect-the-privacy-of-american-consumers/

[2] Julie Rubash, SourcePoint, The Always-Up-To-Date US State Privacy Law Comparison Chart, (July 1, 2024), https://sourcepoint.com/blog/us-state-privacy-laws-comparison-chart/

[3] Global Privacy Control, https://globalprivacycontrol.org .

[4] Press release, Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights, Global Privacy Control (Oct. 7, 2020), https://globalprivacycontrol.org/press-release/20201007.html.

> *Consumers or a consumer's authorized agent may exercise the rights set forth in this act by submitting a request, at any time, to a business specifying which rights the individual wishes to exercise. Consumers may exercise their rights under Section 10-1-963 via user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism that communicate or signal the consumer's choice to opt out.*

Notably, the "authorized agent" provision mentioned above would allow a consumer to designate a third party to perform requests on their behalf — allowing for another practical option for consumers to exercise their privacy rights in an opt-out framework. Consumer Reports has already submitted more than 4 million requests on consumers' behalf, with their permission, through authorized agent provisions under numerous state laws.[5] Authorized agent services are an important supplement to platform-level global opt outs. For example, an authorized agent could process offline opt-outs that are beyond the reach of a browser signal. An authorized agent could also perform access and deletion requests on behalf of consumers, for which there is not an analogous tool similar to the GPC.

- *Remove pseudonymous data exemption.* Section 10-1-967(c) of the bill currently provides that all consumer rights under the bill, including opt-outs, do not apply to so-called "pseudonymous" data. This represents a major loophole that could exempt the majority of the online advertising ecosystem from the most substantive aspects of this bill's coverage. Online platforms and advertisers use pseudonymous identifiers (often cookies) to track users across websites, collecting extremely granular data about a user's search history, usage, personal characteristics, and interests in order to serve them targeted advertisements or to create a profile they can sell to other interested third-parties. Though this is precisely the type of online tracking this bill ostensibly seeks to grant consumers more control over, this exemption would allow vast swaths of it to continue unabated. We presume that the intention of this provision is to minimize unnecessary data linkage as a result of a rights request. However, given the inclusion of the reasonable provision that does not require businesses to re-identify pseudonymous data (Section 10-1-967(b)) and the separate exclusions for truly de-identified data, we question why Section 10-1-967(c) is necessary at all.

- *Ensure targeted advertising is adequately covered.* 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**"

[5] Ginny Fahs, Putting the CCPA into Practice: Piloting a CR Authorized Agent, Digital Lab at Consumer Reports (Oct. 19, 2020), https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8.

(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.*

- *Strengthen non-discrimination provisions.* Consumers should not be retaliated against for exercising their privacy rights—otherwise, those rights are functionally meaningless. Unfortunately, Section 10-1-964(a)(5) of this bill could allow companies to deny service or charge consumers a different price if consumers exercise their opt-out rights under this bill. We urge you to adopt language from our model legislation that clarifies that consumers cannot be discriminated against for refusing that companies sell their information, and limits the disclosure of information to third parties pursuant to loyalty programs:

> *(C) 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.

- *Remove authentication requirements for opt-outs.* While authentication requirements may be appropriate when consumers are requesting to access, delete, or correct their information, controllers should not be allowed to authenticate requests to opt-out. Fraudulent access, deletion, or correction requests can pose real consumer harm, such as identity theft or stalking. 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. For example, in Consumer Reports's investigation into the usability of then-new privacy rights in California, it found examples of companies requiring consumers to fax in copies of their drivers' license in order to verify residency and applicability of CCPA rights.[6] The bill should be amended to clarify that controllers may only authenticate requests to confirm, access, obtain, delete, or correct personal data.

- *Strengthen enforcement.* We recommend removing the "right to cure" provision to ensure that companies are incentivized to follow the law, particularly given that other states have already passed similar provisions, giving companies plenty of time to acclimate to compliance. Already, the AG has limited ability to enforce the law effectively against tech giants with billions of dollars a year in revenue. Forcing them to waste resources building cases that could go nowhere would further weaken their efficacy. 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.

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

- *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.[7] At most, the bill should 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.

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

Sincerely,

Matt Schwartz
Policy Analyst
Consumer Reports

Caitriona Fitzgerald
Deputy Director
Electronic Privacy Information Center (EPIC)

[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, "Big Tech searches for a way back into healthcare," Financial Times, (May 17, 2020), https://www.ft.com/content/74be707e-6848-11ea-a6ac-9122541af204