March 17, 2023

Chair Jack Johnson
Senate Committee on Commerce and Labor
425 5th Avenue North
Suite 776 Cordell Hull Bldg.
Nashville, TN 37243

Chair Kevin Vaughan
House Committee on Commerce
425 5th Avenue North
Suite 622 Cordell Hull Bldg.
Nashville, TN 37243

Re: Tennessee Information Protection Act, S.B. 73/H.B. 1181 — OPPOSE

Dear Chair Johnson and Chair Vaughan,

Consumer Reports[1] writes in respectful opposition to S.B. 73/H.B. 1181. The bill seeks to provide to Tennessee 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 Tennessee 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 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 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.

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, you can either forgo the service altogether or acquiesce completely.

As such, 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.[2] We recommend including a strong data minimization requirement that limits data collection and sharing to what is reasonably necessary to provide the service requested by the consumer, as outlined in our model bill.[3] A strong default prohibition on 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.

Opt-out bills, like S.B. 73/H.B. 1181, simply shift far too much of the burden onto individual consumers to protect their privacy. Consumer Reports has found that consumers experienced significant difficulty exercising their rights under the CCPA's opt-out provision. In our study, hundreds of volunteers tested the opt-out provision of the CCPA, by submitting "do not sell" requests to companies listed on the data broker registry. About 14% of the time, burdensome or broken "do not sell" processes prevented consumers from exercising their rights under the CCPA.[4] Unfortunately, S.B. 73/H.B. 1181 lacks provisions, like a global opt-out and authorized agent rights, that helps make the California Privacy Rights Act (CPRA), which builds upon the CCPA, more workable for consumers.

However, within the parameters of an opt-out based bill, we make the following recommendations to improve S.B. 73/H.B. 1181:

- *Require companies to honor authorized agent requests and browser privacy signals as opt outs.* In the absence of strong data minimization requirements, at the very least, consumers need tools to ensure that they can better exercise their rights, such as a global opt out. CCPA regulations *require* companies to honor browser privacy signals as a "Do Not Sell" signal; CPRA added the global opt-out requirement to the statute. The Colorado

[2] Section 47-18-3204 (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.
[3] *Model State Privacy Act*, Consumer Reports (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.
[4] *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.

Privacy Act and Connecticut Data Privacy Act require it as well.[5] Proposals in a number of states this year, including Kentucky (S.B. 5), Oklahoma (H.B. 1030), Montana (S.B. 384), New Hampshire (S.B. 255), Rhode Island (H.B. 5745), Oregon (S.B. 619), New York (S.B. 365), and others include a similar provision. Moreover, privacy researchers, advocates, and publishers have already created a "do not sell" specification designed to work with such frameworks, the Global Privacy Control (GPC).[6] This could help make the opt-out model more workable for consumers,[7] but unless companies are required to comply, it is unlikely that consumers will benefit. We recommend using the following language:

> Consumers or a consumer's authorized agent may exercise the rights set forth in 47-18-3203(a)(2) of 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 47-18-3203(a)(2) 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 a practical option for consumers to exercise their privacy rights in an opt-out framework. Consumer Reports has already begun to experiment with submitting opt-out requests on consumers' behalf, with their permission, through the authorized agent provisions.[8] 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.

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* S.B. 73/H.B. 1181'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 by claiming that much online data

[5] Cal. Code Regs tit. 11 § 999.315(c); CPRA adds this existing regulatory requirement to the statute, which went into effect on January 1, 2023, at Cal. Civ. Code § 1798.135(e) https://thecpra.org/#1798.135. For the Colorado law, see SB 21-190, 6-1-1306(1)(a)(IV)(B), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf. For the Connecticut law, see Public Act No. 22-15, Section 6(a)(A)(ii)

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

[7] 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.

[8] 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.

sharing is not technically a "sale"[9] (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). We recommend 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 is ambiguous, and 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.

- *Non-discrimination.* Consumers should not be retaliated against for exercising their privacy rights—otherwise, those rights are functionally meaningless. Unfortunately, Section 47-18-3204 (a)(5) of this bill could allow companies to deny service or charge consumers a different price if they opt out of the sale of their information. We urge you to adopt consensus language from the Washington Privacy Act that clarifies that consumers cannot be discriminated against for declining to sell their information, and limits the disclosure of information to third parties pursuant to loyalty programs:

> A controller may not discriminate against a consumer for exercising any of the rights contained in this chapter, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. This subsection does not prohibit a controller from offering a different price, rate, level, quality, or

[9] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously, supra* note 3.

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 bona fide loyalty, rewards, premium features, discounts, or club card program. If a consumer exercises their rights pursuant to 47-18-3203(a)(2)(F) of this act, a controller may not sell personal data to a third-party controller as part of such a program unless: (a) The sale is reasonably necessary to enable the third party to provide a benefit to which the consumer is entitled; (b) the sale of personal data to third parties is clearly disclosed in the terms of the program; and (c) the third party uses the personal data only for purposes of facilitating such a benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose.

- *Remove the identity authentication requirement for opting out*. S.B. 73/H.B. 1181 gives consumers the right to opt out of certain uses of the consumer's information. But it sets an unacceptably high bar for these requests by subjecting them to identity authentication by the company. Consumers shouldn't have to authenticate their identity, for example by providing a driver's license, in order to opt-out of targeted advertising. Further, much of that data collected online (including for targeted advertising) is tied to a device and not an individual identity; in such cases, authentication may be impossible, rendering opt-out rights illusory. In contrast, the CCPA pointedly does not tether opt out rights to identity verification.[10]

- *Remove entity level carveouts*. 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, 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.[11] 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.

[10] Cal. Civ. Code § 1798.130(a)(2).
[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; 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

- *Strengthen enforcement*. We recommend removing the "right to cure" provision to ensure that companies are incentivized to follow the law.[12] 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.

We look forward to working with you to ensure that Tennessee consumers have the strongest possible privacy protections.

Sincerely,

Matt Schwartz
Policy Analyst

cc: The Honorable Johnny Garrett
The Honorable Bo Watson
Members of the House Commerce Committee
Members of the Senate Commerce and Labor Committee

[12] 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