March 8, 2022

The Honorable Dennis Powers, Chair
House Subcommittee on Banking and Consumer Affairs
674 Cordell Hull Building
Nashville, TN 37243

Re: HB 1467 (Tennessee Information Privacy Act) — OPPOSED

Dear Chair Powers,

The undersigned consumer, privacy, and civil rights groups write in respectful opposition to HB 1467. The Tennessee Information Protection Act (TIPA) seeks to provide to Tennessee consumers the right to know the information companies have collected about them, the right to delete that information, and 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.

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 that limits data collection and sharing to what is reasonably necessary to provide the service

requested by the consumer.[1] 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. Consumer Reports has documented that some California Consumer Privacy Act (CCPA) opt-out processes are so onerous that they have the effect of preventing consumers from stopping the sale of their information.[2]

However, within the parameters of an opt-out based bill, we make the following recommendations to improve the Tennessee Information Privacy Act:

- *Require companies to honor 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; Proposition 24 added the global opt-out requirement to the statute. The new Colorado law requires it as well.[3] Privacy researchers, advocates, and publishers have already created a "Do Not Sell" specification designed to work with the CCPA, the Global Privacy Control (GPC).[4] This could help make the opt-out model more workable for consumers,[5] but unless companies are required to comply, it is unlikely that consumers will benefit.

  Further, the bill should also be amended to include "authorized agent" provisions that 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.[6] Authorized agent services will be 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.

---

[1] *Model State Privacy Act*, Consumer Reports (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.
[2] *Consumer Reports Study Finds Significant Obstacles to Exercising California Privacy Right*s, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.
[3] Cal. Code Regs tit. 11 § 999.315(c); CPRA adds this existing regulatory requirement to the statute, going 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.
[4] Global Privacy Control, https://globalprivacycontrol.org.
[5] 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.
[6] 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.

- *Broaden opt-out rights.* While we appreciate that this draft 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.

  In addition, there are other loopholes in the bill for cross-context targeted advertising that should be addressed. We urge you to ensure that pseudonymous data—which is typically used for ad tracking—is covered by the opt out, as it is in California, Colorado, and Virginia. For the bill to be meaningful, consumers must have control over the transfer of this data.

- *Remove the safe harbor for reasonable compliance with the NIST privacy framework.* The safe harbor in enforcement for companies that reasonably comply with the NIST privacy framework should be removed. The NIST framework was designed as a voluntary risk-management tool; it was not designed as an alternative to privacy rules. While potentially useful as an internal protocol for assessing privacy issues within a company, the framework does not provide clear guidance as to what companies can or cannot do with personal data, and as such is inappropriate as a safe harbor from legislative protections.

- *Non-discrimination.* Consumers shouldn't be charged for exercising their privacy rights—otherwise, those rights are only extended to those who can afford to pay for them. Unfortunately, language in this bill could allow companies to charge consumers a different price if they opt out of the sale of their information. We urge you to adopt consensus language that clarifies that consumers can't be charged for declining to sell their information, and limits the disclosure of information to third parties pursuant to loyalty programs.

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

Thank you again for your consideration.

Sincerely,

Consumer Reports
Common Sense
Consumer Federation of America
Electronic Frontier Foundation
Fight for the Future
Privacy Rights Clearinghouse

cc: Members, House Subcommittee on Banking and Consumer Affairs
The Honorable Johnny Garrett