February 5, 2021

The Honorable David W. Marsden
Pocahontas Building, Room No. E618
Senate of Virginia
P. O. Box 396
Richmond, VA 23218

Re: SB 1392, Consumer Data Protection Act

Dear Senator Marsden,

The undersigned consumer and privacy groups sincerely thank you for your work to advance consumer privacy in Virginia through the Consumer Data Protection Act (CDPA). Though consumers in Europe and California enjoy baseline privacy protections, Virginians currently do not have similar basic privacy rights. The CDPA would address this by extending to Virginia 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, with additional rights for sensitive data. These protections are long overdue: consumers are constantly tracked, and information about their online and offline activities are combined to provide detailed insights into a consumers' 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.

We offer several suggestions to strengthen the proposed CDPA to provide the level of protections that Virginians deserve. ***At the very least, the CDPA should be modified to bring it up to the standard of the California Consumer Privacy Act (CCPA)***, which was recently strengthened by the passage of Proposition 24, the California Privacy Rights Act (CPRA). In particular, the CCPA as refined by CPRA takes important steps such as adding to the statute a requirement to honor browser privacy signals as an opt out (previously it was required by regulation) and removing the "right to cure" provision in administrative enforcement. The CCPA also includes authorized agent provisions so that consumers can delegate third parties to exercise rights on their behalf, which should be replicated in this bill.

Because the CDPA is based on an opt-out model, like the CCPA, the deck is already stacked against consumers. Consumers have to contact hundreds, if not thousands, of different companies in order to fully protect their privacy. Making matters worse, Consumer Reports has documented that consumers often find it difficult to locate Do Not Sell links on data brokers' homepages. In our recent study, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?,* over 500 consumers submitted Do Not Sell requests to approximately 200 companies on the California Data Broker Registry.[1] Each company was tested by at least three study participants. We found that for 42.5% of sites tested, at least one of three testers was unable to find a DNS link. All three testers failed to find a "Do Not Sell" link on 12.6% of sites, and in several other cases one or two of three testers were unable to locate a link.

In some cases, the opt-out links simply weren't there; in others, the links were difficult to find. Follow-up research revealed that at least 24 companies on the data broker registry did not have the required DNS link on their homepage. All three testers were unable to find the DNS links for five additional companies, though follow-up research revealed that the companies did have DNS links on their homepages. If consumer testers who are actively searching for DNS links have difficulty finding them on the homepage, it's hard to imagine that the everyday consumer will find them.

To help address these issues, we offer the following recommendations:

- *Strengthen data minimization:* Privacy laws should set strong limits on the data that companies can collect and share. Consumers should be able to use an online service or app safely without having to take any action, such as opting in or opting out—by 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. A

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

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 hundreds of different companies.

- *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;[2] Proposition 24 added the global opt-out requirement to the statute.[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 Virginians will benefit.

- *Add an authorized agent provision:* CDPA should also be amended to include the CCPA's "authorized agent" provision that allows 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.[6] Consumer Reports has already begun to experiment with submitting opt-out requests on consumers' behalf, with their permission, through the authorized agent provisions.[7] 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.

- *Strengthen enforcement*: The "right to cure" provision in the administrative enforcement section of the CDPA should be removed, as Proposition 24 removed it from the CCPA. This "get-out-of-jail-free" card ties the AG's hands and signals that a company won't be punished for 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.

- *Strengthen control over targeted advertising*: Ensuring that consumers can control use of their data for targeted advertising was one of the primary goals of the CCPA, and it

[2] Cal. Code Regs. tit. 11 § 999.315(c) (2020).
[3] Cal. Civ. Code § 1798.135(e).
[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] Cal. Civ. Code § 1798.135(e); §1798.140(ak).
[7] Ginny Fahs, *Putting the CCPA into Practice: Piloting a CR Authorized Agent*, (Oct. 19, 2020), https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8.

should be a key element of any privacy law, including the CDPA. The CDPA's opt out should cover all data transfers to a third party for a commercial purpose. The CDPA's current language 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 California, many companies have sought to avoid the CCPA's opt-out with respect to targeted advertising, claiming that the CCPA does not apply to these data transfers.[8] Prop. 24 (CPRA) clarifies that targeted ads are clearly covered by the opt out.[9] For many consumers, targeted advertising is a serious violation of their privacy, and consumers should at least have the opportunity to decide whether their personal information is used in this way.

- *Remove the verification requirement for opting out*: CDPA 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 verification by the company. Thus, companies could require that consumers set up accounts in order to exercise their rights under the law—and hand over even more personal information. Consumers shouldn't have to verify 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, verification may be impossible, rendering opt-out rights illusory. In contrast, the CCPA explicitly states that companies "shall not require the consumer to create an account with the business in order to make a verifiable consumer request," and pointedly does not tether opt out rights to identity verification.[10]

- *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 replace this provision with consensus language from the Washington Privacy Act that limits the disclosure of information to third parties pursuant to loyalty programs.

- *Strengthen the definition of consent.* We appreciate that the bill adds opt-in protections for sensitive data, but the definition of consent needs to be strengthened—at least brought

[8] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs to Act* (Jan. 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california- consumer-privacy-act-seriously-dcb1d06128bb.
[9] Maureen Mahoney, *Consumer Reports Urges Californians to Vote Yes on Proposition 24* (Oct. 23, 2020), https://medium.com/cr-digital-lab/consumer-reports-urges-californians-to-vote-yes-on-proposition-24-693c26c8b4bd.
[10] Cal. Civ. Code § 1798.130(a)(2).

into line with the latest version of the Washington Privacy Act—to ensure that consumers have a meaningful choice. Like the WPA, there should be a prohibition on dark patterns—deceptive user interfaces that can lead consumers to take actions they didn't intend to, including to share more personal information. Too often, companies often use dubious dark patterns to nudge users to click "OK," providing the veneer, but not the reality of, knowing consent.[11]

While we offer these suggestions to improve the bill, we also readily acknowledge that there is a lot to like about the bill. The CDPA would grant important new rights to Virginia citizens that the residents of most states do not current enjoy. And many of the bills' definitions—such as "deidentified" information—are quite strong.

We ask that the House of Delegates pause voting on the bill to consider these improvements. Thank you again for your consideration, and for your work on this legislation. We look forward to working with you to ensure that Virginians have the strongest possible privacy protections.

Sincerely,

Common Sense
Consumer Federation of America
Consumer Reports
Electronic Frontier Foundation
EPIC
Privacy Rights Clearinghouse
U.S. PIRG

cc: Members of the Virginia House of Delegates

[11] *Most Cookie Banners are Annoying and Deceptive. This Is Not Consent,* PRIVACY INTERNATIONAL (May 21, 2019), https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent.