July 9, 2021

The Honorable C.E. "Cliff" Hayes, Jr., Co-Chair
The Honorable David W. Marsden, Co-Chair
Joint Commission on Technology and Science, Consumer Data Protection Work Group
900 East Main Street
Richmond, VA 23129

Dear Chairs Hayes and Marsden,

Consumer Reports[1] sincerely thanks you for your work to advance consumer privacy in Virginia through the Consumer Data Protection Act (CDPA). The CDPA extends 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. We appreciate that the Joint Commission on Technology and Science, Consumer Data Protection Work Group is considering making recommendations to the legislature to further implementation of the new law.

We offer several suggestions to strengthen the 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 (currently 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.

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

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections.

limits data collection and sharing to what is reasonably necessary to provide the service requested by the consumer, as outlined in our model bill.[2] 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.[3]

However, within the parameters of an opt-out based bill, we make the following recommendations to improve the CDPA:

- *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 adds the global opt-out requirement to the statute. The new Colorado law requires this as well.[4] Privacy researchers, advocates, and publishers have already created a "Do Not Sell" specification designed to work with the CCPA, the Global Privacy Control (GPC).[5] This could help make the opt-out model more workable for consumers,[6] 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. 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

[2] *Model State Privacy Act*, CONSUMER REPORTS (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.
[3] *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/.
[4] 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.
[5] Global Privacy Control, https://globalprivacycontrol.org.
[6] 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.
[7] 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.

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. We recommend the following language to add both the browser privacy signal requirement and to extend rights to authorized agents:

> Consumers or a consumer's authorized agent may exercise the rights set forth in § 59.1-573 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 § 59.1-573(5)(i)-(ii) 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.

- *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 (similarly, the Colorado law sunsets the right to cure). 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 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, by establishing a right to opt out of sharing of data for cross-context behavioral advertising—which is one of the main reasons why CR supported the measure.[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

[8] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs To Act*, DIGITAL LAB AT CONSUMER REPORTS (Jan. 9, 2020), https://medium.com/crdigital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb; *Consumer Reports Study Finds Authorized Agents Can Empower People to Exercise their Digital Privacy Rights in California*, CONSUMER REPORTS at 16 (Feb. 4 2021), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-authorized-agents-can-empower-people-to-exercise-their-digital-privacy-rights-in-california/.
[9] Maureen Mahoney, *Consumer Reports Urges Californians to Vote Yes on Proposition 24*, DIGITAL LAB AT CONSUMER REPORTS (Oct. 23, 2020), https://medium.com/cr-digital-lab/consumer-reports-urges-californians-tovote-yes-on-proposition-24-693c26c8b4bd.

personal information is used in this way. We recommend replacing the definition of sale with the following:

> "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.

And using the following definition of targeted advertising:

> "Targeted advertising" means the targeting of advertisements to a consumer based on the consumer's activities over time and across 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 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

[10] Cal. Civ. Code § 1798.130(a)(2).

provision with consensus language from the Washington Privacy Act that 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 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 right pursuant to § 59.1-573(5) 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.

- *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 into line with 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]

> "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer signifies agreement to the processing of personal data relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through dark patterns does not constitute consent. "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

[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.

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,

Maureen Mahoney
Senior Policy Analyst

Justin Brookman
Director, Technology Policy

cc: Joint Commission on Technology and Science, Consumer Data Protection Work Group