February 23, 2021

Governor Ralph Northam
P.O. Box 1475
Richmond, VA 23218

Re: Request to Veto or Add Reenactment Clause to the Consumer Data Protection Act

Dear Governor Northam,

The undersigned groups are organizations dedicated to consumer advocacy and protecting consumer privacy. We thank Virginia legislators for their concern about privacy but we respectfully ask you to veto the Consumer Data Protection Act (CDPA)—or consider adding a reenactment clause to this bill—because it falls far short of adequately protecting and empowering Virginians, and it allows unfair discrimination against those who exercise the few rights it provides.

As the legislature has recognized with this bill, average people have little insight into the ways that companies collect and use their information, and even fewer mechanisms for control over their personal data. We have worked with legislators across the country to encourage crafting legislation that gives consumers meaningful tools to better protect their privacy. To help address these issues, we suggest the bill be returned in the legislature to add the following protections:

Strengthen data minimization. It should be easy for consumers to understand what information is collected about them, and who has that information about them. Companies should have to ask consumers before they collect information at all – an opt-in framework rather than an opt-out framework. Making "opt-out" the default disempowers consumers and poses equity concerns; consumers with less time and resources to figure out how their data is being used and how to opt-out will inevitably be subject to more privacy violations. Where the default lies matters, as marketers well-know. It's time to change the default to "opt-in."

Even within a consent framework, however, consumer privacy laws should limit 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 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.

Strengthen consumer's control of their personal information. Currently, the definition of personal data does not include information gleaned about consumers from sources such as social media if consumers have failed to adequately restrict who can see that information. This is not a reasonable exception in light of the fact that many consumers do not understand social media privacy settings or anticipate that their information could be harvested for commercial purposes. Furthermore, the definition of personal data does not include information that is linked or can be linked to a particular household or device, a major gap considering today's complex data ecosystem in which information from the use of smart devices is used to target users and households and treat them in different ways on the basis of that data, without knowing their exact identities.

Consumers have no right to stop their personal data from being sold to companies' affiliates – businesses they do not know and whose products and services may be very different from that of their parent companies. In addition, some of the rights that consumers do have are unduly limited; for instance, they can avoid seeing targeted ads based on tracking their activities, but not being tracked. Furthermore, since targeted advertising does not include a business advertising to consumers based on their activities on its own website or app, it does not cover the business models of Facebook and Google, who profit from targeting ads to consumers based on that data on behalf of other companies.

Consumers have the right not to be profiled only when the profiling would result in decisions that "produce legal or similarly significant effects" on them – a determination that would be made by the controller. In other words, they cannot simply decide that they do not wish to have inferences made about them based on the personal data that are collected about them and the proprietary algorithms that are used to produce those profiles. In addition, consumers cannot designate someone else to exercise their rights; for instance, an elderly woman could not ask her grown child to act on her behalf to request that her data be deleted. There are also problems with references to "known child," which would appear to limit parents' and guardians' abilities to act on behalf of their children if the controller did not know that consumer was a child.

Remove the verification requirement for opting out. Consumers should not have to pass a high bar to stop companies from using their information. CDPA gives consumers the right to opt out of certain uses of their personal information but requires that they verify their identities to do so. We ask that you remove this unnecessary hurdle to prevent people from exercising their privacy rights.

No pay for privacy. No one should be charged or penalized for asking companies to respect their privacyrights. And no one should be asked to pay more in order to protect their privacy. Yet this bill allows companies to charge consumers more or provide them with a lower quality of goods or services if they have exercised their rights – for instance, to avoid targeted advertising. This provision must be removed to avoid unfairly separating Virginians into two classes; those who can pay to protect their privacy, and those who cannot.

Strengthen enforcement. The "right to cure" provision in the administrative enforcement section of the CDPA must be removed. It offers companies a "get-out-of-jail-free" card, significantly undermining the ability of the attorney general to take enforcement action when it deems it necessary and incentivizing companies to be lax about providing necessary privacyprotections to their customers.

Finally, it is essential to ensure that consumer privacy laws have teeth. Private rights of action, which are prohibited in this legislation, provide a valuable enforcement tool for everyday people and make clear that companies will face real consequences for privacy harms. People rightly can sue over product

defects, car accidents, breach of contract, do-not-call violations, or injuries to reputation— they do not have to wait for the state attorney general to bring actions on their behalf in any of these instances. Privacy harms should be no exception.

Consumers have made clear that they want stronger data privacy laws—largely in reaction to the ways that companies use and abuse their information. Unfortunately, consumer and privacy organizations were not consulted as this legislation was being crafted and only recently became aware of it. Furthermore, our letters and comments have been completed ignored. Virginia has the opportunity to take a leadership position in the national conversation around data privacy. We urge you to veto this bill or to add a reenactment clause, to allow all stakeholders to take the time necessary to enact meaningful privacy legislation that put the needs of people first. We would be happy to work on it with the legislature. It is better to get this right than to enact a law that does not provide privacy protection that Virginians want and deserve.

Sincerely,

Irene E. Leech, Virginia Citizens Consumer Council

Susan Grant, Consumer Federation of America

Lee Tien, Electronic Frontier Foundation

Emory Roane, Privacy Rights Clearinghouse

Ed Mierzwinski, U.S. PIRG