Consumer Federation of America
1620 I Street, N.W., Suite 200 * Washington, DC 20006

August 13, 2021

The Honorable C. E. (Cliff) Hayes Jr., Commission Chair
Joint Commission on Technology and Science
Consumer Data Protection Work Group
Virginia General Assembly
Pocahontas Building, 8th Floor
900 E. Main Street
Richmond, VA 23219

Dear Chair Hayes:

I appreciate the opportunity to provide comments on how the Consumer Data Protection Act (CDPA) could be improved to better-protect Virginians from unwanted tracking and profiling, discriminatory practices, and disclosure of their personal information. These are the most important changes that should be made but this is by no means an exhaustive list. I urge the work group to convene a panel of experts from nonprofit consumer and privacy organizations that are independent of businesses in order to have a fulsome discussion of the issues and provide you with suggestions for ensuring that this law provides effective privacy protection.

Treat affiliates of companies as third parties.

Under the CDPA, consumers have no control over processors sharing their data with affiliated companies, even though those companies may be in completely different lines of business and have different data practices. Consumers have no idea who those affiliates are or what they do. For all practical purposes, affiliates are no different than third parties when it comes to protecting consumers' privacy and should be treated as such.

Require meaningful data minimization.

Virginians should be able to use online services and apps with confidence that their privacy will be respected and without having to wade through long and often obtuse privacy policies and take action to opt in or opt out. Currently, the CDPA only requires controllers to limit their data collection and processing to the purposes stated in their privacy policies – purposes that are very difficult to understand, as anyone who has attempted to read companies' privacy policies would acknowledge. Meaningful data minimization would limit data collection and processing to what is reasonably necessary to provide the products or services consumers have requested. If the sale of consumers' data continues to be allowed, it should only be done if the consumer has expressly consented – that is, opted in rather than opted out. Furthermore, the statute should provide that a consumer's agreement obtained through the use of "dark patterns," which are interfaces designed to manipulate consumers' choices, does not constitute express consent.

Broaden the definition of sale and change the definitions of personal data and publically available information.

Defining "sale" of consumers' data to "the exchange of personal data for monetary consideration" is far too limited to effectively protect consumers' privacy. In California, this type of narrow definition was construed by some to not apply to companies in the vast "ad tech" industry that track what consumers do across the internet and on apps to profile them. That is why the new California Privacy Rights Act provides definitions for both "sale" and "share," and both include renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating the data, orally, in writing, or electronically, to another business. Furthermore, since money may not be the only form of compensation involved, they apply when there is "monetary or other valuable consideration."

Another problem with the definition of "sale" is that it does not cover information that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience. This could be construed as not covering personal data gleaned from sources such as social media if consumers have failed to adequately restrict who can see that information. This is not a reasonable exception because consumers don't necessarily understand social media privacy settings or anticipate that their information could be harvested and "sold" for commercial purposes. The problem goes deeper than this, as the definition of personal data excludes publicly available data, and publicly available data includes information consumers intentionally made available to the general public via a channel of mass media and didn't restrict. The bottom line is that this data is not covered at all by the statute. Consumers have no rights, and processors have no obligations, in regard to this data. This must be changed. Public data is well-understood as data in government records that is publicly available. Personal information that isn't public data should be covered by the law.

Enable consumers to avoid all targeted advertising and profiling.

Under the CDPA, targeted advertising does not include advertising to consumers based on their activities on a company's own websites or apps. By definition then, the rights that consumers have regarding targeted advertising do not apply to companies such as Facebook and Google, which track what consumers do over the many different websites and apps they own, profile them, and serve them ads based on those profiles on behalf of other companies. Consumers can't opt-out of that.

Furthermore, consumers can only opt-out of being profiled if it would result in decisions that "produce legal or similarly significant effects" on them – a determination that would be made by the controllers. Consumers can't opt out if the controller decides there would be no such effects.

Many organizations, including mine, have called for a ban on targeted advertising, or what we call "surveillance advertising," because of its intrusiveness and the potential for discrimination and unfair treatment. Contextual advertising, in which ads are shown to consumers based on what they are looking at or doing at that moment, without collecting their personal data over time and space, is a much better alternative for consumers and studies have shown that it is effective for businesses that want to find customers for their products and services, at a lower cost than surveillance advertising. I will be happy to provide more information in this regard.

At the very least, consumers should not be subject to targeted advertising and profiling without their express consent.

Eliminate the "pay for privacy" provision.

Virginians should not be charged or penalized for asking companies to respect their privacy rights, nor should they be asked to pay more in order to protect their privacy. Yet the CDPA 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 opt out of targeted advertising or ask to delete their data. This provision must be removed to avoid unfairly separating Virginians into two classes; privacy "haves" and "have nots." We have no objection to a very narrowly tailored exception for voluntary participation in loyalty card or rewards programs.

Strengthen enforcement.

The "right to cure" provision in the CDPA should be removed. It offers companies a "get-out-of-jail-free" card, significantly undermining the Attorney General's ability to take enforcement action when it deems it necessary and incentivizing companies to be lax about providing necessary privacyprotections to their customers. It is not necessary, as the Attorney General has always used its discretion in deciding when it is appropriate to bring formal legal actions. There is nothing in the statute that changes this: the Attorney General is still free to send a warning letter to a company or otherwise resolve problems informally. Legislators must not tie the Attorney General's hands, however, when that agency determines that a different course of action is appropriate. As representatives of the Attorney General have noted, there are other concerns about the right to cure as well: it does not result in legal precedents to guide courts and businesses, and it does not provide recompense to consumers. The right to cure is being eliminated in California and it should be eliminated from the CDPA.

Finally, the law should be amended to give consumers the ability to enforce their rights. Private rights of action 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, 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.

Sincerely,

Susan Grant
Director of Consumer Protection and Privacy
Consumer Federation of America