



January 27, 2023

Virginia House Communications, Technology and Innovation Committee
Attn: Robert Asplund
House Room 3, Pocahontas Building
900 East Main Street
Richmond, VA 23219

**Re: HB 1688 - "Consumer Data Protection Act; protections for children"
(Oppose)**

Dear Chair Brewer and Members of the Committee on Communications, Technology and Innovation:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 1688.

CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For over 50 years, CCIA has promoted open markets, open systems, and open networks. The Association supports the enactment of comprehensive federal privacy legislation in order to promote a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights and responsibilities for organizations that collect data. A uniform federal approach to the protection of consumer privacy is necessary to ensure that businesses have regulatory certainty in meeting their compliance obligations and that consumers are able to understand and exercise their rights.

We appreciate, however, that in the absence of federal privacy protections, state lawmakers have a continued interest in enacting local legislation to guide businesses and protect consumers. As you know, Virginia is out in front of this effort as one of the five states with a comprehensive consumer data privacy law. CCIA commends lawmakers in their thoughtful approach in enacting legislation that supports meaningful privacy protections while avoiding interference with the ability of businesses to meet their compliance obligations and the opportunity for consumers to benefit from the innovation that supports the modern economy.

CCIA strongly believes younger users deserve an enhanced level of security and privacy online. Currently, there are a number of efforts among our members to incorporate protective design features into their websites and platforms. CCIA's members have been leading the effort in raising the standard for teen safety and privacy across our industry by creating new features, settings, parental tools, and protections that are age-appropriate and tailored to the differing developmental needs of young people.

We appreciated the opportunity to discuss the legislation in greater detail with Chair Brewer on January 26, and while CCIA understands that certain users may warrant specific treatments, we remain concerned with several provisions included in HB 1688.



1. The Virginia Consumer Data Privacy Act (VCDPA) established strong protections for all consumers, including rights for teenage users.

The VCDPA went into effect on January 1 of this year. The law includes strong protections for all users, including rights for teenage users. These include the right to know what personal information is being collected, and the right to correct, delete, or port their personal data. Users also have the ability to opt-out of targeted advertising, the sale of their personal data, and profiling in furtherance of decisions that produce legal or similarly significant effects concerning consumers. Since the law has only become effective this month, CCIA recommends pausing any further amendments to the law to allow time to examine its impacts and prevent creating an ever-moving compliance target. To comply with the current VCDPA requirements, businesses rolled out new mechanisms to enable such new consumer rights and introducing additional requirements immediately following the law's enactment would present additional compliance burdens.

2. The bill could result in online services being required to collect additional consumer data to achieve compliance – similar provisions in other proposals have raised constitutional concerns.

HB 1688 provides three examples of how to obtain verifiable parental consent: (i) providing a signed consent form; (ii) using a credit card, debit card, or other online payment system that provides notification of any transaction with the operator to the primary account holder; or (iii) providing a form of government issued identification. However, this raises questions about whether such verification mechanisms would conflict with data minimization principles and other consumer data privacy protection measures. CCIA is concerned that businesses may be forced to collect age verification data, which would paradoxically force companies to collect a higher volume of data on users.¹ Businesses may be forced to collect personal information they don't want to collect and consumers don't want to give, and that data collection creates extra privacy and security risks for everyone.

When the federal Communications Decency Act was passed, there was an effort to sort the online population into children and adults for different regulatory treatment. That requirement was struck down by the U.S. Supreme Court as unconstitutional because of the infeasibility.² Yet, after 25 years, age authentication still remains a vexing technical and social challenge.³ Though the intention to keep younger users safe online is commendable, this bill is counterproductive to that initiative by requiring more data collection about young people and their parents. California recently enacted legislation that would implement similar age verification measures which is currently being challenged for similar reasons.⁴ CCIA

¹ Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), <https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard>.

² *Reno v. ACLU*, 521 U.S. 844 (1997).

³ Jackie Snow, *Why age verification is so difficult for websites*, The Wall Street Journal (Feb. 27, 2022), <https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728>.

⁴ *NetChoice v. Bonta* (N.D. Cal. 22-cv-08861).



recommends that lawmakers permit this issue to be more fully examined by the judiciary before burdening businesses with legislation that risks being invalidated.

3. Requiring parental consent could adversely impact routine services and unnecessarily complicate user experience for teenage users.

HB 1688 would require parental consent for any collection of data from users between 14 and 17 years of age. In practice, this would require most internet websites to acquire parental consent. This would inevitably result in negative impacts to the user experience and create delays and impediments to using existing and new internet services by teens unless a parent is present to verify such collection each time. For example, compliance with HB 1688 could turn the simple act of a student researching online when completing school assignments into a completely unworkable experience. In practice, this could prevent students conducting work in a classroom setting or at a local library from accessing relevant online resources. And this could be an even bigger issue for students under 18 who are enrolled in higher education studies at a college or university at a physical location far from a parent.

* * * * *

We appreciate your consideration of these comments and stand ready to provide additional information as the legislature considers proposals related to technology policy.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association