January 31, 2024

Senate General Laws and Technology Committee
Attn: Eric Bingham and Andrew Horton, Committee Clerks
Room 306, General Assembly Building
201 North Ninth Street
Richmond, VA 23219

RE: SB 252 - "Consumer Data Protection Act; controller privacy notice, consumer consent" (Oppose)

Dear Chair Ebbin and Members of the Senate General Laws and Technology Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to raise several concerns regarding SB 252.

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 growing number of states with a comprehensive consumer data privacy law. CCIA commends lawmakers for their thoughtful approach to 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.

SB 252 would establish additional requirements for privacy notices to include a method for consumers to "opt out of the automatic placement of a data file" or "cookie". Controllers would also be required to have express consent of a consumer to use such cookies, except for those that are "strictly necessary".

We appreciate the opportunity to highlight several of our concerns with SB 252's provisions, as included below.

1. CCIA has concerns regarding how the creation of a new opt-out right would work within the existing Virginia Consumer Data Protection Act, in addition to the associated compliance challenges that may create.

As you know, the VCDPA went into effect on January 1 of last year. The law includes strong protections for all users, including 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 only became effective last year, CCIA recommends pausing any further amendments to the law to allow time to examine its impacts and prevent creating an ever-moving compliance target.

2. SB 252 may prevent businesses from using tools to improve services.

SB 252 would also encompass a wide range of tools and technologies that businesses of all sizes depend on. For instance, small businesses heavily rely on such tools for analytics purposes like the number of unique site visitors. These businesses also use such tools to improve their sites and services, such as being able to remember a specific user and personalized experience settings such as the number of items they want displayed on a page. Further, such tools and technologies help small businesses remain competitive by providing them with new sources of revenue that enable them to improve upon, or expand, their existing offerings. If users were able to opt-out of first and third party cookies, then small businesses could not improve their products and may be forced to revert to a subscription or another costly model.

3. SB 252 could result in a degraded user experience.

Privacy protections should be directed toward managing data collection and processing practices that pose a high risk of harming consumers or are unexpected in the context of a service. Consent mechanisms can be a powerful tool for promoting transparency and consumer control. However, it is important to recognize that the provision of many services, both online and offline, requires the collection and processing of certain user information. Requiring specific opt-in user consent to use cookies, except for those that are "strictly necessary" would be inconsistent with consumer expectations, introduce unnecessary friction resulting in the degradation of user experience, and likely overwhelm consumers, resulting in "consent fatigue" that would lessen the impact of the most important user controls.[1]

* * * * *

We appreciate the Committee's consideration of these comments and stand ready to provide additional information as the General Assembly considers proposals related to technology policy.

[1] See Article 29 Data Protection Working Party, WP 259, *Guidelines on Consent Under Regulation 2016/679*, 17 (Apr. 10, 2018), ("In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing."), https://ec.europa.eu/newsroom/article29/items/623051.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association