Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

25 Massachusetts Avenue NW
Suite 300C
Washington, DC 20001

January 30, 2023

House Health, Welfare and Institutions
Subcommittee #1
Attn: Susan Slough
Pocahontas Building
900 East Main Street
Richmond, VA 23219

Re: HB 2219 - "Health records privacy; consumer-generated health information" (Oppose)

Dear Chair Edmunds and Members of the House Health, Welfare and Institutions Subcommittee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 2219.

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 supports the protection of consumer health data, however, we caution against several provisions included in HB 2219.

1. The Virginia Consumer Data Privacy Act (VCDPA) established strong protections for consumers, including rights for health-related data.

The VCDPA went into effect on January 1 of this year. The law includes strong protections for consumers including the right to know what personal information is being collected, and the

right to correct, delete, or port their personal data. Further, under the VCDPA, consumers must provide opt-in consent to the use of their sensitive data, which includes mental and physical health conditions.

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. Introducing additional requirements immediately following the law's enactment would present additional compliance burdens.

2. The bill proposes duplicating many rights established under the VCDPA, but with slightly different approaches.

Several of the bill's provisions require actions taken for de-identified and aggregate data. However, under the VCDPA, the data is not considered de-identified *unless* those actions have been taken. This bill does not provide added privacy protections in such cases. Companies already must publish a Privacy Policy to consumers with information on the categories of third parties that may receive personal data – this would include personal data that is health-related. The bill would require those entities to create new systems to inform consumers of a "detailed list" of all entities to whom such information may be disclosed. This would require significant reengineering of systems. It is important to note that no other state has required disclosure of specific entities. Further, as noted below, other states specifically exempt disclosures to service providers.

3. The bill prohibits certain activity outright which could limit consumer ability to access features and services deemed as personally beneficial.

Many of the "health care" apps and services this bill regulates have utility because they can show the consumer progress over time. For example, consumers can track their sleep habits, weight loss or physical activity as compared with the previous month or year. However, the bill would require that providers delete information within 24 hours. Many devices do not process such information on the device itself and must be synced with another device such as a cell phone or computer. This would render useless many apps that consumers have specifically chosen to use.

Further, many companies use data to combat fraud and illegal activity. Requiring companies to delete data – including data that protects consumers from bad actors and identity theft – is counterintuitive to the goal of protecting consumers. Companies also use data for authentication purposes to help verify that the user of a device is in fact the intended user, as these devices are often interlinked.

4. Proposed consent requirements would adversely impact the user's experience.

The bill would require consumer opt-in consent for several actions that would provide little benefit to the user, but would likely create a frustrating, interruptive experience. For example, Consumers must agree to having their data stored in the cloud. Cloud service providers and companies providing services for devices are often able to provide superior protection for data separate from the device. This bill could impact an organization's ability to use new and innovative services and products to help keep their organization running and properly protect consumers.

Furthermore, under the VCDPA, consumers must opt-in to share data with service providers who are under contract with the provider to process the data. Service providers already have obligations to protect the processed data, along with other privacy obligations. Other states and the FTC expressly exempt sharing data with service providers to provide the service to consumers.

The bill treats identified, aggregate and de-identified data the same way, as if there were no privacy benefits to using privacy protective practices that tell us much about trends and concerns from larger groups. Opt-in consent is required for all three forms of data sharing.

5. The private right of action would result in the proliferation of frivolous lawsuits.

HB 2219 permits users to bring legal action against companies that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of Virginia's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. For example, the Illinois Biometric Information Privacy Act has resulted in numerous lawsuits and convictions for items such as photo organizing tools. As such, certain businesses have chosen to stop providing innovative services that are still available in other states. CCIA cautions Virginia against discouraging innovation that provides many benefits to consumers.

Lawsuits also prove extremely costly and time-intensive – it is foreseeable that these costs would be passed on to individual users in Virginia, disproportionately impacting smaller businesses and startups across the state.

* * * * *

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