

STATE PRIVACY & SECURITY COALITION

February 27, 2023

Chairman C.T. Wilson
Vice Chair Brian M. Crosby
House Economic Matters Committee
Room 231
House Office Building
Annapolis, MD 21401

Re: Health Data Privacy (HB 995) - Unfavorable

Dear Chair Wilson, Vice Chair Crosby, and Members of the Committee,

The State Privacy & Security Coalition (SPSC), a coalition of over 30 companies and six trade associations in the retail, telecom, technology, automobile, health care, and payment card sectors, writes in opposition to HB 995. We do not oppose the intent of this legislation, but as drafted it suffers from similar overbreadth that the bill it is based on in Washington state suffers from, which will lead to a deluge of opt-in notification for routine types of data. Put another way, the actual scope of the bill as drafted could effectively be read to cover *virtually all data* that an individual generates – including purchases of deodorant, food, and toilet paper.

This type of overbreadth *is not helpful for consumer privacy*. A statute which results in consumers receiving numerous opt-in notifications each day for the collection of ordinary data will lead to consent fatigue, instead of receiving opt-in notifications for truly sensitive data like reproductive health care information.

Additionally, the bill also attempts to combine significant portions of HB 33 into a bill regarding reproductive health care, which increases the difficulty in understanding what the intent of the bill is.

SPSC would again note, as we have in prior hearings, that we believe pursuing a comprehensive approach to consumer privacy, such as the Connecticut framework – a framework which covers health data, children’s data, biometric data, and all other data that is “linked or reasonably linkable” to an individual – is a more effective approach to privacy than attempting to regulate biometrics via HB 33, health data and biometrics via HB 995 (which, incidentally, uses a different definition for “biometric data” than HB 33), and children’s privacy via HB 901. Regulating privacy in a topic-by-topic approach will inevitably lead to different standards, definitions, and operational requirements, rather than a uniform approach that consumers and businesses alike can understand and implement.

Lastly, we remain extremely concerned about the broad private right of action that will create a cottage industry for plaintiffs’ attorneys at the expense of both consumer control over their data and business compliance with the law.

STATE PRIVACY & SECURITY COALITION

Below, we outline our concerns with this bill.

1. Overbroad Definitions Will Dilute Consumer Awareness of the Collection of Sensitive Information; Missing Definitions Will Cause Confusion for Compliance

“Health Data”

Unfortunately, the bill as drafted suffers from overbroad definitions – namely that of “Health Data” – that cover far more than reproductive health data. The outer boundary of the definition would require opt-in consent to collect or process *any* personal data “that relates to...bodily functions” or any “symptoms” or “conditions” of a consumer.

This expansive scope, when combined with opt-in requirements, will not just be disruptive to the consumer experience, resulting in unintended consequences (such as collecting more data than necessary to demonstrate that it is not Health Data) – but it also threatens to obscure the use of opt-in consent for the truly sensitive uses of data regarding reproductive care. If consumers get used to clicking through opt-in mechanisms routinely, the mechanisms will cease to be a signal that there is truly sensitive information being collected or shared. This is known as “consent fatigue,” and occurs around, for example, the GDPR cookie banners that consumers regularly click through just to access the services and information they seek.

While this outcome creates difficulties for businesses, it is, more importantly, confusing for consumers. Consumers benefit from clear privacy standards in order to navigate the complex digital landscape. If a bill requires, or highly incentivizes, business to treat all data as potentially health data, it will be difficult for consumers to make informed choices about when to consent to data uses and when to exercise their rights over such sensitive data.

SPSC wants to ensure that when a consumer receives an opt-in notification, they notice and understand its implications. The scope of the bill will prevent this from happening.

“Geolocation Data”

As drafted, the bill references “geolocation information” in several key sections and definitions, but does not define the term. Other states with enacted comprehensive privacy standards recognize that the sensitivity of location data depends upon how precisely it can determine location.

“Personal Information”

In addition to using the California Consumer Privacy Act definition of “personal information” which creates a significant number of overbreadth issues, the definition includes “records of personal property” and “telephone number.” This raises issues of the First Amendment,

STATE PRIVACY & SECURITY COALITION

because these records are often publicly available information. Requiring consent to collect these records is unconstitutional.

“Consent,” “Sale,” “Private Entity” Are Key Terms That Are Not Defined

At the crux of most privacy laws are provisions that establish: a) who is being regulated; b) what activities are regulated; and c) how a consumer may provide or withdraw consent for particular activities.

HB 995 does not define any of these key terms, and leaves critical questions unanswered: Are nonprofit entities included in the scope of private entity? What about individuals acting in a commercial context? What constitutes a “sale” of health data? Is the exchange of monetary consideration, monetary or other valuable consideration, or any communication, orally or in writing? What constitutes consent? Can electronic consent be provided? Can voice consent be provided?

2. Operational Provisions Are Overbroad and Not Workable

a. Geofencing

SPSC does not object to a prohibition on geofencing *for reproductive health data*. Like several other provisions in the legislation, however, HB 995 is overbroad; there is a current ban on *all geofencing – even if it does not pertain to this type of health data*. This means that a gas station which happens to be near a health clinic cannot let nearby loyalty members know that it is offering discount gasoline to them. It will mean a business will violate the law by sending a text message to a nearby consumer letting them know a prescription is ready to pick up.

Again, because this legislation has a private right of action, this also means that the consumer who happens to receive such notifications will be able to sue the gas station or pharmacy for violating a consumer health data law. Moreover, there is no defined boundary to the geofencing (for example, one quarter mile) so that it is impossible to determine where the geofencing boundaries stop.

Not only is this bad public policy, but it is also an unconscionable restraint on commerce and trade, because many of the outcomes have no relation – as drafted – to the intent of the law. Surely, such an unintended consequence points toward reforming this definition and provision. The overbreadth of this will likely be challenged in court immediately upon enactment if it is not corrected, putting the whole legislation in jeopardy.

b. Biometric Data Provisions

Similar to HB 807, we are confused by the distinct provisions relating to biometric data that appear in this legislation. These additions appear as an attempt to shoehorn many of the provisions of HB 33 into a somewhat related topic, but in doing so lacks much of the

STATE PRIVACY & SECURITY COALITION

fundamental balance that exists in a comprehensive privacy approach (such as that of Connecticut).

Again, SPSC does not object to categorizing biometric data, health information, and children's data as types of sensitive data that deserve heightened protections. But if that is the goal of the legislature, it should be done in a comprehensive framework, not in a piecemeal fashion.

c. Personal Information Restrictions

HB 995 also attempts to regulate information that goes beyond either biometric or health data. Section 14-4505 states that after a consumer withdraws consent (undefined) to the collection (undefined) and use of the consumer's health data, "a private entity [undefined] may not, with respect to the consumer's health data **and personal information**, engage in: (1) Data Processing...or **any other use of the personal information...**" [emphasis added].

This is an extremely broad expansion of the bill, from a bill that tries to regulate health data (albeit broadly defined), to a bill that conditions use of **all** personal data on the consent regarding health data.

3. Private Right of Action

We strongly believe that a private right of action **will not help consumers or businesses**. It will not help businesses because the compliance lens will not be focused on the consumer, but rather on avoiding litigation; this is likely to lead to an amplification of opt-in mechanisms and notifications in order to "play it safe;" it is likely to further desensitize consumers to these notifications; and trial lawyers will be enriched while consumers, as usual, recover minimal compensation for technical, immaterial, errors by businesses.

We have seen what happens when a private right of action is deployed. In Illinois, **consumers are less safe than in any other state**, because companies that use biometrics to prevent fraud and identity theft turn down their services in order to avoid certain litigation; startups do not offer services to residents because they know they will be sued.

SPSC wants consumers to have increased control over the data and increased transparency as to how their data can be used. We want consumers to know that when they receive an opt-in consent mechanism flagging that a company is about to collect or share consumer health data, it is something to seriously consider.

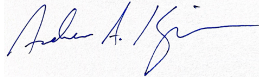
A private right of action jeopardizes all of this; it will result in an overload of opt-in consent requests, and consumers will lose the context of why carefully considering the use of their data is important' instead, requests will blur together in consumers' minds with no particular importance attached to providing consent in order to simply to access everyday services and products that have nothing to do with their consumer health data.

STATE PRIVACY & SECURITY COALITION

As stated throughout this legislation, SPSC believes that a comprehensive approach which covers health data, biometric data, children's data, and all other categories of personal data, and which has been vetted by hundreds of stakeholders in states throughout the country, is the best approach to resolve these issues.

We would be happy to answer any questions, and look forward to continued conversations.

Respectfully submitted,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition