

STATE PRIVACY & SECURITY COALITION

February 23, 2022

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

Re: HB962 Proposed Amendments

Dear Chairman Wilson and Vice Chairman Crosby,

The State Privacy and Security Coalition, a coalition of 32 companies in the telecom, tech, payment card, automotive, and retail sectors, as well as seven trade associations, writes with minor proposed amendments to HB 962.

At the outset, we wish to thank the sponsor, Delegate Carey, and his staff for their diligent work on this bill over the past several years. We have found him to be responsive to and considerate of our concerns, and believe that our amendments accord with the intent of this bill while providing increased clarity. We have shared our amendments with the sponsor and believe we are very close to agreement.

Our amendments are as follows:

1. We ask that the proposed deletion in Section 14-3501(F)(1)(i) – “the name or” – be removed, so that all elements of the “Personal information” definition are notifiable only if they are unencrypted or otherwise rendered unusable. This would accord with nearly all other state breach laws; nearly all other states apply the encryption standard both to a consumer’s name as well as the data elements within the definition. As an alternative, we propose the Minnesota formulation of this definition, which reads: “Personal information’ does not include information that has been secured by encryption or another method of technology that makes electronic data unreadable and unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired.”¹
2. We would ask that the definition of biometric information be amended so that the information “generated by automatic measurements of an individual’s biological characteristics...that **is** used to uniquely authenticate the individual’s identity when the individual accesses a system or account.” There are 18 states that include biometric information as a data element, but none include this formulation, because it includes information that is not definitively linked to an individual’s identity. We would request this change to align with all other states, so that notification processes can be efficient and consistent, giving clarity and greater certainty to consumers.

¹ [Minn. Stat. § 325E.61.](#)

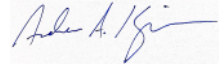
STATE PRIVACY & SECURITY COALITION

3. We would request that the element of genetic information also be subject to encryption and redaction standards, and have suggested to Delegate Carey the following language: “Genetic information with respect to an individual, when the genetic information is not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable.” Genetic information is certainly capable of identifying an individual, but we do not believe it should be a notifiable event if an individual’s *encrypted* (or otherwise unusable) information is accessed, unless that encryption key is also accessed. It would be very confusing and unnecessarily concerning to consumers if they received a notice that their genetic information was accessed, when in reality there was, in fact, no way of the hacker actually accessing the data.
4. We have also worked with Delegate Carey’s office on exempting test results for COVID-19 from the bill, and have proposed language in 14-3501(F)(1)(ii), to read: “‘Personal information’ does not include: **(iv) The results of a test for Covid-19.**” Covid-19 tests are a new wrinkle since this bill was last considered. The results of a test, which are extremely prevalent, could be considered “health information” as defined in this statute, do not present a real threat of identity theft or fraud, and therefore should be exempted from the bill.
5. We would propose that s. 14-3505(a)(2) be amended to acknowledge that contractual requirements between businesses and third parties regularly contain provisions that allocate responsibilities, including notification, among the parties. With the author’s proposed amendment, businesses will have to renegotiate these contracts to account for the truncated notice period time; we believe this is not necessary in most cases, and would propose the following language at the end of the paragraph: “...but not later than 10 days after the business discovers or is notified of the breach of the security system **or pursuant to the contractual requirements between the business and the owner or licensor of personal information.**”
6. Lastly but importantly, we have also worked with the author on adding language to s. 14-3504(d)(2) to eliminate an unintended consequence. As currently drafted, a business that delayed notification for a law enforcement investigation lasting less than 38 days would be required to notify consumers ***in a shorter timeframe than statutorily contemplated***. As an example, if a law enforcement investigation took only 10 days, a business would be required to notify consumers in 17 days, rather than the allowed period of 45. We are proposing the following language to fix this unintended consequence of the current draft:
 - (2) If notification is delayed under paragraph (1)(i) of this subsection, notification shall be given as soon as reasonably practicable, but not later than 7 days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security, **if the 45-day period following discovery has already elapsed. If the 45-day period following discovery has not yet elapsed, then notice shall be given within the original 45-day period.**

Again, we thank Delegate Carey for his work on this legislation and believe our amendments are in line with the intent of the bill. We look forward to continued work as need, and would support favorable passage out of committee with these changes.

STATE PRIVACY & SECURITY COALITION

Respectfully submitted,



Andrew Kingman
General Counsel
State Privacy and Security Coalition