FPF Written/Verbal Testimony for 2/8/23 Hearing

Good Afternoon,

My name is Tatiana Rice, and I serve as Senior Counsel at the Future of Privacy Forum, a non-profit dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies.

In the absence of comprehensive privacy legislation, I appreciate this legislatures' efforts to establish new rights and protections for consumers biometric information. Today, I'm here to recommend to this Committee the three following points should it consider advancing this legislation:

1. **The carve-out for physical and digital photographs, and video or audio recording should be limited to identification**

As currently drafted, the definition of "biometric data" which "does not include a physical or digital photograph, or a video or audio recording" may unintentionally create loopholes for technologies that pose the highest privacy risks. For example, when developing a facial recognition system, photos of individuals are used to train the system by extracting certain unique features and vectors from the photograph and associating them with a known identity in a database. If the raw sources of data used to create biometric systems such as photos are excluded, it is possible an entity could escape liability due to this carve-out. Instead, the legislature should consider adopting the language used in the Connecticut Data Privacy Act, which excludes these sources, and any data generated therefrom, **unless it is used to identify a specific individual.**

2. **Consumer rights of access and deletion should be verifiable and required of all processing entities.**

SB 169 Section 14-4505 and Section 14-4502(A)(1)(III) provides consumers with important rights of access and deletion. If passed, this would be the first time a specific biometric data privacy bill in the US provides these rights to consumers, it also highlights the need to ensure these provisions are carefully drafted. While these rights are important, it is equally important to ensure that businesses are not required to process fraudulent requests from bad actors that could also risk consumers' information. As written, the "right to deletion" provision does not specify what a "verified" request means, it also does not instruct any service providers or third-parties to which a business may be using for its software to also delete the data, and it does not require notice to the individual if there is reason to believe someone is fraudulently attempting to access or delete their biometric data. Comprehensive data privacy laws that provide consumer privacy rights such as the California Privacy Protection Act (CCPA) can provide a useful framework, where the California AG specified in their implementing regulations that a "verifiable consumer request" could be determined by matching identifying information provided by the consumer to the personal information already maintained by the business.

3. **Lastly, the Bill should make the Fraud and Security exemptions consistent**

Decades of research has demonstrated that biometric authentication is one of the most important security measures for many companies to prevent against fraud. It is used, for example, to secure access to buildings or databases, or confirm the identity of a known consumer before providing access to financial information. Fingerprinting, is also a common requirement for employee background checks pursuant to state or federal laws.

Unlike other biometric data privacy laws in the US, this bill provides compliance exemptions for biometric data used for fraud prevention or security purposes as it relates to consent and deletion requirements. Section 14-4504 exempts entities from getting individual consent to process biometric information if it is required by federal, state, or local law, or if it used for fraud prevention or security purposes (so long as there is still conspicuous notice). However, Section 14-4502 only exempts entities from complying with deletion requests if the individual is "part of the state voluntary exclusion program" which appears to be a program for individuals who wish to ban themselves from Maryland casinos. As a result, if any non-casino entity received a verifiable deletion request, they must delete the data which would terminate the entity's ability to continue using the biometric authentication system for that individual. The entity, therefore, must choose between recommended security practices or compliance by federal or state law, or compliance with this Act, even if they were initially able to collect the individual information without consent. Given that the bill's consent fraud exemptions are broader than the fraud exemptions for deletion, the legislature may consider better aligning these provisions for consistency of compliance.

Should the legislature have any additional questions or seek additional information, I would be more than happy to assist in whatever way I can.

Tatiana Rice
Senior Counsel for U.S. Legislation and Biometrics
trice@fpf.org| www.fpf.org
1350 Eye Street NW, Suite 350
Washington, DC 20005