CHARITY R. CLARK
ATTORNEY GENERAL

TEL: (802) 828-3171

www.ago.vermont.gov

STATE OF VERMONT
OFFICE OF THE ATTORNEY GENERAL
109 STATE STREET
MONTPELIER, VT
05609-1001

To: Senator Ginny Lyons, Chair
Senate Committee on Health and Welfare

From: Charity R. Clark, Attorney General

Date: May 1, 2024

Re: H.121, Draft Version 4.1, dated 4-24-2024

In follow-up to my oral testimony this morning, I submit the following written testimony. I am in strong support of legislation that protects the data privacy rights of consumers and, in so doing, protects the integrity of the marketplace. To assist the Committee as it considers H.121, the following is a summary of my Office's recommendations and observations regarding the three main areas to which I testified this morning: the definition of "biometric data," a private right of action with statutory damages, and a potential entity-level exemption for HIPPA-covered entities.

Definition of 'biometric data'

I strongly recommend adopting the House version's definition of "biometric data." The Senate version contained in draft version 4.1 of H.121 excludes from the definition "digital or physical photographs," "audio or video recordings," and "any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual." As a preliminary matter, the bill seems to contradict itself in that "facial or hand mapping, geometry, or templates" is *included* as biometric data (§ 2415(4)(A)(iii)), but "any data generated" from photographs or audio or video recordings is *excluded* (§ 2415(4)(B)(iii)).

Moreover, this severe narrowing of the definition of "biometric data," in large part, guts the protections of biometric data from the bill. I believe Vermonters deserve to have these protections. Otherwise:

It will embolden companies like Clearview AI, whose entire business model is based on scraping the internet for "publicly available" photos and images to build a facial recognition database. This includes images of children and minors. To date, Clearview AI has collected over 40

billion[1] photos to help build its facial recognition database. That equals approximately five photos for every person on earth in the company's database.[2]

Second, it will also embolden anyone with a photo or audio/video recording of an individual to take that information and make deepfakes, including nonconsensual deep fake pornography. Like scraping the internet for photos, this is done without an individual's knowledge or consent. It can result in severe damage to a person's reputation. No one can make a deepfake with a person's Social Security number, but they can make it with that person's face or voice.

It is indisputable that the internet and other data storage locations contain more biometric data through photos, videos, and audio recordings than any other type. It seems incongruous to exclude this data from a bill designed to provide consumer protections of biometric data.

A private right of action

As I expressed during my testimony, privacy violations of biometric data are particularly insidious. Once the violation occurs, it is very difficult to remedy, because the data – our face, our fingerprint – cannot be changed in the same way other data – our credit card number, our Social Security number – can be. For this reason, I also strongly recommend adding back into the bill the private right of action with "statutory damages" for violations of the provisions regarding biometric data, as envisioned by the House. "Statutory damages" refers to a provision of damages that includes a specific amount of money – up to $1,000 in the House version. These kinds of damages are incredibly useful in a situation like this one where it can be difficult to quantify the harm.

We believe that preserving a consumer's right to bring a lawsuit when an entity or person misuses their biometric data provides them with the appropriate recourse. Notably, the cure period provided in the House version of the bill, which withholds this private right of action provision from taking effect until after an amount of time during which a violator of the law may "cure" the violation, is extremely business friendly.

Maintain data-level exemptions for consumer health data

Data-level exemptions for consumer health data, as envisioned by the House, should be maintained. This is important because consumer health data, like biometric data, genetic data, and reproductive or sexual health information that HIPPA covered entities may possess but that falls outside the ambit of HIPPA, should be covered. Washington's My Health My Data Act specifically targets this kind of data.[3]

Notably, early adopter states like Connecticut have encountered problems with their laws that provide several entity-level exemptions, including exemptions for entities that have to comply with HIPPA. In February 2024, the Connecticut Attorney General's Office issued a report recommending that entity-level exemptions for HIPPA compliant organizations be rolled back in

---

[1] Note that during my testimony I underestimated this figure by 20 billion photographs. The correct figure is 40 billion.

[2] Clearview AI was first brought to my attention by this article in the *New York Times:* "The Secret Company that Might End Privacy as We Know It," Jan. 18, 2020.

[3] https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/House%20Passed%20Legislature/1155-S.PL.pdf?q=20240501075403

future legislation because it precludes their ability to enforce the law. Vermont should take note from lessons learned in other states and avoid entity-level exemptions like these.

The bill's cure period is an important way to avoid confusion regarding the data-level exemptions around consumer health data. Should a HIPPA-covered entity find itself not in compliance with the bill, it will have a grace period to bring itself into compliance.

Finally, one theme of this bill is to anticipate the kinds of consumer harms that could arise from types of technology we have yet to foresee. As we move into the future of consumer data and health care data overlapping, it is important to ensure that consumer privacy is protected.

Conclusion

To summarize, I suggest the Committee:

- Adopt the House version's definition of biometric data;
- Allow for a private right of action with statutory damages for misuse of biometric data;
- Maintain data-level exemptions for consumer health data.

I support the Committee's efforts to protect the data privacy of Vermonters. If the Committee has any specific questions, I would be more than happy to provide additional testimony.