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: **Sen. Wendy Harrison, Chair**
Senate Committee on Institutions

FROM: **Charity Clark, Attorney General**

DATE: **March 13, 2025**

RE: **Written Testimony Regarding Data Privacy**
S.71, An act relating to consumer data privacy and online surveillance

For over five years, I have supported legislation that protects the data privacy of Vermont consumers. To assist the Committee as it considers S.71 and potentially S.93, the following is a summary of my recommendations and observations of both bills.

S.71:

S.71 builds on the work of the Legislature last year when it passed H.121, An act relating to enhancing consumer privacy and the age-appropriate design code. Notably, it provides key protections and remedies for Vermont consumers while also providing predictability for entities doing businesses in Vermont.

That said, I recommend the following changes to S.71:

§ 2424. ENFORCEMENT; ATTORNEY GENERAL'S POWERS.

I recommend striking subsections (c)(1) and (c)(2). Section 2458 of Title 9 already gives my Office discretion to determine whether to pursue an action against an actor that is violating Vermont consumer protection laws. It is rare for us to bring a lawsuit where it is possible to instead bring an actor into compliance outside of court. Because this authority already exists under Title 9, there is no need for a cure period to be part of S.71.

However, should the Legislature believe a cure period to be necessary for purposes of this bill, I recommend maintaining the language that preserves my Office's ability to determine the best course of action:

(c)(1) If the Attorney General determines that a violation of this chapter or rules adopted pursuant to this chapter may be cured, the Attorney General may, prior to initiating any action for the violation, issue a notice of violation extending a 60-day cure period to the controller, processor, or consumer health data controller alleged to have violated this chapter or rules adopted pursuant to this chapter.

(2) The Attorney General may, in determining whether to grant a controller, processor, or consumer health data controller the opportunity to cure an alleged violation described in subdivision (1) of this subsection, consider…"

I also recommend modifying subsection (d)(2) to continue the consumer remedies that have been available in the Consumer Protection Act for almost 60 years: actual damages for consumers instead of statutory damages. I strongly believe that consumers should have the right to seek recourse against bad actors when they are harmed. But I understand that statutory damages can at times be problematic, specifically in the data privacy space. Should S.71 provide for actual damages in lieu of statutory damages, it will maintain remedies for consumers and also protect businesses (and in turn the marketplace) from claims that may lack merit.

S.93:

Turning to S.93, I believe this bill, while well intentioned, considers the interests of businesses over those of consumers. I have three central concerns with this bill. First, as currently written, very few Vermont businesses will be captured under the bill because the applicability thresholds are too high and are not right-sized for Vermont. Second, what is considered "publicly available information" does not adequately incorporate protections for biometric information that may be misused by bad actors. The Legislature should seek clarity from stakeholders on the use and transfer of this extremely sensitive data. Finally, S.93 does not provide for consumer remedies at all and instead places all enforcement powers with my Office. Putting the onus solely on taxpayers to enforce a data privacy law is misguided and inefficient. Importantly, the Attorney General does not and cannot represent individuals.

I therefore recommend the following changes:

§ 2416. APPLICABILITY

The bill as currently written states:

(a) Except as provided in subsection (b) of this section, this chapter applies to a person that conducts business in this State or a person that produces products or services that are targeted to residents of this State and that during the preceding calendar year:

(1) controlled or processed the personal data of not fewer than 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

(2) controlled or processed the personal data of not fewer than 25,000 consumers and derived more than 25 percent of the person's gross revenue from the sale of personal data.

This language is lifted from Connecticut's data privacy law. Connecticut has a population of 3.7 million. When compared to Vermont's population of 650,000, it is not hard to see that very few businesses will be captured under this proposed "100,000 [Vermont] consumers" applicability threshold because such a high figure represents roughly 15% of Vermont's population (compared with roughly 3% of Connecticut).

Neighboring states with smaller populations that have passed similar data privacy laws have imposed lower applicability thresholds. For example, New Hampshire, with a population of 1.4 million, has an applicability threshold of 35,000 (2.5% of the population) or 25,000 and 25% gross revenue from the sale of personal data in its data privacy law. Rhode Island, population of 1.1 million, provides applicability thresholds of 35,000 (~3% of the population) or 10,000 and 20% of gross revenue from the sale of personal data in its law. These modified thresholds recognize that applicability should focus on the number of potential consumers in question.

I recommend following the lead of New Hampshire and Rhode Island and changing § 2416 to account for Vermont's small population, while striking a balance for regional consistency, as follows:

(1) controlled or processed the personal data of not fewer than 25,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

(2) controlled or processed the personal data of not fewer than 10,000 consumers and derived more than 20 percent of the person's gross revenue from the sale of personal data.

§ 2415. DEFINITIONS.

I recommend inserting a new subsection 33(C) that states:

"Publicly available information" does not include biometric data collected by a business about a consumer without the consumer's knowledge.

This definition will assure against publicly available information such as a photo of a consumers' face posted to a social-media or news site being manipulated for uses to which the consumer never consented. This provision is part of the Maryland Online Data Privacy Act and strikes a balance between public data and privacy by focusing on the consumer's intent and understanding.

§ 2425. ENFORCEMENT BY ATTORNEY GENERAL; NOTICE OF VIOLATION; CURE PERIOD; REPORT; PENALTY

I have several concerns with the enforcement section of S.93. The first is relatively minor. As noted above related to S.71, any "cure period" like the one proposed in §§ 2425(b),(c) should be at the discretion of the Attorney General, and not mandatory as the current draft makes it.

More importantly, doing away with consumer remedies completely in lieu of sole enforcement by my Office is a mistake. A private right of action is key to ensuring that consumers have their own avenue for redress when they are harmed. Vesting sole authority in my Office will create an "under enforcement" regime where taxpayers are forced to rely on my Office and my Office alone to bring data privacy actions. I would recommend striking §§ 2425(a), (d) – (f).

Instead of having no private right of action at all, I recommend a narrow consumer remedy that applies to biometric information – information that cannot be changed once it is compromised (your face, fingerprint, etc.), and is focused on larger businesses. I also recommend that the remedy provide for injunctive relief and actual damages in lieu of statutory damages. Here is some suggested language:

> (a) A person who violates this chapter or rules adopted pursuant to this chapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title, provided that a consumer private right of action under subsection 2461(b) of this title shall not apply to the violation, and the Attorney General shall have exclusive authority to enforce such violations, except as provided in subsection (c) of this section.
>
> (b) The Attorney General has the same authority to adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, bring civil actions, and take other enforcement actions as provided under chapter 63, subchapter 1 of this title.
>
> (c)(1) Notwithstanding subsection (a) of this section, the private right of action available to a consumer for violations of this chapter or rules adopted pursuant to this chapter shall be exclusively as provided under this subsection.
>
> (2) A consumer who is harmed by a data broker's or large data holder's violation of subdivision 2420(a) of this title, with regard to processing biometric data only, may bring an action under subsection 2461(b) of this title for the violation, but the right available under subsection 2461(b) of this title shall not be available for a violation of any other provision of this chapter or rules adopted pursuant to this chapter.
>
> (3) For the purpose of subsection (c)(2) of this section, "data broker" has the same meaning as subsection 2430(4) of this title, and "large

data holder" means a person that during the preceding calendar year processed the personal data of not fewer than 25,000 consumers.

Although I believe S.93 does not go far enough to provide adequate data privacy protections for consumers, I recognize that Vermont, once a leader in the data privacy space, has fallen behind. If passed, S.93 could be the foundation that we build upon as technology advances.