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

April 17, 2024

To: Sen. Kesha Ram Hinsdale, Chair, Senate Committee on Economic Development, Housing and General Affairs
Sen. Alison Clarkson, Vice-Chair, Senate Committee on Economic Development, Housing and General Affairs
Sen. Randy Brock
Sen. Ann Cummings
Sen. Wendy Harrison

From: Charity R. Clark, Attorney General

Cc: Christopher J. Curtis, Assistant Attorney General, Director Consumer Assistance Program
Sarah Aceves, Assistant Attorney General

Date: April 17, 2024

Re: H.121, Draft Version 1.1., dated April 10, 2024

As draft version 1.1. of H.121, an act related to enhancing data privacy, dated April 10, 2024, was not made public until after my recent testimony and in light of a potential committee vote today, I wish to provide important context on two key areas: the private right of action and new § 2429.

A private of action

Vermonters deserve to be able to take action if their own data privacy has been violated. This is a value statement that I believe in, and one I wrote about earlier this winter in an op-ed published around Vermont. I testified last week in strong support of a private right of action – and, indeed, have been unwavering in this support for years – but I wanted to highlight in writing some of the protections in place.

First, H.121 itself has protections for businesses built in. Critically, the cure period allows for a defined amount of time during which a controller of data can "cure" any violation. A private right of action does not vest until *after* the cure period has lapsed and no cure has been affected. This means a company who has violated this version of the act will have had to fail to cure during, in this version of the bill, a 120-day period (roughly 4 months) before an individual can bring a civil suit against the controller. I should note that I prefer the House's 60-day cure period, which I believe is enough time for a data controller to effect a cure without unnecessarily jeopardizing a Vermonter's data privacy.

Also, I have heard concerns of "frivolous lawsuits." The Committee should know that bringing a frivolous lawsuit is a violation of the Vermont Rules of Professional Responsibility (the "Rules") for attorneys. See Rule 3.1, Meritorious Claims and Contentions, forbidding frivolous lawsuits. Note that under the Vermont Rules of Civil Procedure, a defendant in a frivolous lawsuit may request their attorney's fees be paid by the plaintiff. In addition, when a lawsuit has no merit, the Vermont Rules of Civil Procedure provide the ability for a defendant to move the court to dismiss claims.

It is my understanding that the Committee has recently heard from Vermont businesses who hold enough consumer data to be subject to the provisions around a private right of action due to being retail mail order catalogues. Voices from all Vermont businesses are critical in passing legislation that affects them, and I am glad these businesses stepped forward. What wasn't clear from the feedback I have seen is what factual scenario is imagined that would result in a retail mail order catalogue being sued by an individual using the private right of action provision of this bill. It seems unlikely that such businesses qualify as data brokers or collect biometric or health information. That leaves the provisions about data handling, disclosures, and data minimization. It is very important to emphasize that most, if not all, of these provisions are based on laws that already exist in other states, and that companies doing business in those states must already comply with these provisions. Also, if these provisions pass in Vermont, businesses will still have to comply with them, whether a private right of action exists or not. Importantly, the cure period adds a critical layer of protection for businesses, because prior to the private right of action being utilized, the business will have an opportunity to cure. Put another way, only when a business fails to cure will an individual be permitted to bring a lawsuit.

Regarding some of the specific changes in this draft, §2427(a)(2) has new language; the meaning of which is not entirely clear to me, i.e., allowing a private right of action be brought "individually, but not in a representative capacity." If the intention of this phrase is to forbid an individual from hiring counsel, I strongly advocate for its deletion. If you feel that it should be included, I recommend hearing testimony from the Judiciary. I myself would also request the ability to testify on this topic.

In addition, I find §2427(a)(3) problematic in its dramatic narrowing of the private right of action to, essentially, the sellers of data rather than holders of data, as well as its practical challenges. This section provides that Vermonters would have the ability to bring a lawsuit only against someone whose gross revenue was derived from over 50% from the sale of personal data. The Committee should consider how a Vermonter would establish, prior to bringing a lawsuit, what percentage of a business's gross revenue is derived from the sale of personal data (and, for that matter, the ease with which a data controller could determine this). Moreover, this provision would no doubt *dramatically* narrow the scope of data controllers who could be sued to, largely, data brokers. Good data hygiene practices should be practiced by all controllers of data, but the hundreds of data breaches impacting thousands of Vermonters reported to my office each year by a wide variety of companies suggests they are not. Gutting the private right of action in this way would deprive Vermonters of a right to bring an action if their data privacy was violated.

Finally, I see that this version of the draft includes in §2427(b)(2) a limiting of the considerations the Attorney General may consider in applying her prosecutorial discretion vis a vis an opportunity to cure. As I testified, my hunch is that you did not intend to limit the prosecutorial discretion the Attorney General already possesses, but this is the effect of this section. I would delete it.

§ 2429

This new section transforms the enforcement authority of the Attorney General in conflict with current law and should be deleted. In essence, § 2429 creates an "enforcement oversight board" to "provide advice and counsel to the Attorney General in carrying out the Attorney General's responsibilities" with regards to cure periods. This section was met with bewilderment by myself and my office. It is unknown to me why this section was added, but, suffice it to say, the Attorney General relies on the outstanding counsel, expertise, and wisdom provided by the 150 attorneys, investigators, paralegals, and other professionals working at the Attorney General's Office. The Attorney General is accountable to the public

who elected her, and creating an “enforcement oversight board” would be inappropriate and in conflict with current statute.

Attachment: “The legislative moment for data privacy,” VTDigger, February 5, 2024

OPINION

Attorney General Charity Clark: The legislative moment for data privacy

We must align our data privacy laws with Vermont's values of privacy and personal freedom.

February 5, 2024, 6:49 am

This commentary is by Attorney General Charity R. Clark.

The Vermont Legislature is taking up **a comprehensive data privacy law** — one that gives you the power to sue if your data has been mishandled in violation of that law — right in the nick of time.

Commentaries
Opinion pieces by community members

Facial recognition can let strangers identify us on the street. Geolocation tracking apps and spyware can map our physical location. Artificial intelligence tools create "deepfake" videos of political leaders and celebrities that are indistinguishable from reality — and have already been used to create nonconsensual pornography. Social media algorithms collect data they sell and use to addict children to their screens. Data brokers sell our information, including predictions about our interests, our personalities and our vulnerabilities, to anyone willing to pay for it. And even companies that do prioritize data privacy are vulnerable to data security breaches and the criminal enterprises that steal what they cannot buy.

I am pleased by strong legislative leadership prioritizing passage of a comprehensive data privacy law. For years, I have advocated for a law that includes data minimization provisions, requiring data brokers to offer consumers an "opt out" from having their data bought and sold,

and establishing a Biometric Data Privacy Act that would require notice and consent for collecting and using things like facial recognition.

Of these provisions, the industry collecting our data has been universally critical of one key component: your right to sue when your own biometric information has been mishandled in violation of a BIPA. Curiously thin on reasons for their dislike, industry has tried to use their dislike of this so-called “private right of action” as a boogeyman, spooking legislators by saying that a bill will struggle to pass if it is included. So far, the only reason I have heard why they don’t like this provision is simple: it will cost industry more money. But without a private right of action, only the Attorney General’s Office will have the authority to sue for violations of a BIPA. In other words, industry wishes to transfer their costs of violating BIPA to you, the Taxpayer.

Beyond data minimization, a BIPA, and requiring a data broker opt-out, there are other additional protections the Legislature could consider now or in the future. Artificial intelligence, for example, is a frontier with tremendous opportunity — and danger. Without appropriate regulation, use of AI by criminal actors — for example, scammers — could have a destabilizing impact on the online economy. Just as scam robocalls destabilized the buying and selling of goods and services over the phone, a lack of trust by consumers could have a chilling effect on online purchases. And while AI presents a potential harm to commerce, one particular type of AI — the use of deepfakes to make nonconsensual pornography — is currently much more prevalent. I urge the Legislature to also prioritize addressing this problem.

As Attorney General, I have made data privacy a priority, especially for children. We must align our data privacy laws with Vermont’s values of privacy and personal freedom. Legislators, stakeholders in the business community and data privacy advocates must work cooperatively to craft law and policy that is effective while leaving business free to develop and grow.