Testimony on H.211 before House Committee on Commerce and Economic Development

Ryan Kriger, Montpelier resident, formerly of VT AGO and FTC

February 27, 2026

My name is Ryan Kriger. I have been a resident of Montpelier, Vermont for fifteen years. For most of that time I worked as an Assistant Attorney General in the Vermont Attorney General's Office Public Protection Division, focusing on privacy and data security as well as antitrust and other consumer protection issues. After that I worked at the Federal Trade Commission in the Division of Privacy and Identity Protection. I also teach about privacy law and policy, as well as consumer protection and First Amendment at the University of Vermont. Currently, I am Deputy Chief of the Massachusetts Attorney General's Privacy and Responsible Technology Division.

Today, I am speaking in my personal capacity as a Vermonter who cares about his own privacy and the privacy and safety of his wife, his friends, their children, and his fellow Vermonters.

My comments today are mine alone and do not reflect any positions of the Massachusetts Attorney General or those of her office.

When I was a Vermont AAG, I drafted the Data Broker report and had the honor of working with this committee, and Chairman Marcotte, on the original data broker law. In the course of advocating for that law and negotiating language with stakeholders, I observed incredible pushback from industry and their lobbyists. Years later I was told that one major data broker had made killing that bill their primary focus for the year.

At the time, I didn't understand why the pushback was so ferocious, given that the bill didn't actually require any businesses to change their practices other than documenting the fact of their existence. Over the course of that experience, I came to realize that data brokers really don't seem to want anyone to know they exist. They are the only industry I have encountered in two decades of legal practice that doesn't want anyone to know about them. Most companies spend a lot of money announcing their existence in the form of marketing and advertising, but not this one.

One lobbyist told me in a moment of candor that businesses didn't want to be in the registry because being called a "data broker" was like having a scarlet letter. I posit that if you are actually ashamed to acknowledge your line of business, that says a lot about the ethics of the work you do and its value to society.

Despite that resistance, the fact that this law was enacted, the first law in the nation, state or federal, to actually name data brokers, should be a point of pride for this committee and

the state of Vermont. Were it not for this law, I do not believe California would have passed its data broker registry, nor would it have passed the Delete Act, which creates a method for Californians to easily remove themselves from most data broker databases. The Delete Act isn't a perfect law, it has more exemptions than I'd prefer and like many recent privacy laws requires consumers to take affirmative steps to protect their privacy rather than putting the onus on data brokers to justify invading their privacy, but it is a major step toward.

This law has received criticism from some privacy advocates, mainly that it does not actually do much. The term "light touch" was used so often during negotiations that at one point it seemed that if it was any more "light touch" it would be practicing Reiki.

That light touch was, however, a feature and not a bug. We had two goals at the time: to put data brokers on the regulatory map, and to pass a law that would stand up to Constitutional scrutiny. That first goal is an important one. When it comes to passing legislation, it is far easier to stop something from happening than to build something, and one compelling argument is, "It's never been done before." This law eliminated that argument.

The second goal was equally important because at the time the Supreme Court case of *IMS v. Sorrell* was still fresh in the mind of many legislators. That case nullified a Vermont law that attempted to permit doctors to opt out of having pharmacies sell their prescribing information to data brokers. Many scholars have criticized that opinion, and it should be noted that in that case the Supreme Court did *not* rule that attempting to regulate data brokers was unconstitutional. It held that the law was not viewpoint neutral because it restricted the ability of pharmaceutical marketers to engage in commerce but permitted the same data to be used for academic purposes.

My hope at the time was that having laid the foundation, this body would return to the law and build upon it, and I am thankful to see that happening now. In particular, the I applaud the following improvements:

- In the original bill I hoped to see a strong credentialing requirement to address the problem of data brokers supplying information directly to fraudsters and other bad actors. This bill corrects that omission in section 2431(b).
- Once we started enforcing the new law, we quickly realized that while the law imposes fines for failing to register, it did not impose fines for filing incorrect or overly vague information. This bill mostly corrects that in section 2446(b). It imposes appropriate fines for filing materially incorrect information. I suggest expanding that to included, "omitting sufficiently detailed information" or words to that effect. If

that language is included, I would suggest a cure period applicable in that limited circumstance.

- The bill includes a number of additional reportable data elements in section 2446(a), which I believe will be extremely beneficial to enforcers, researchers, advocates and journalists, and through their efforts, consumers. I recommend the deletion of original law 2446(a)(4)(D) and (E). These two sections, which require the reporting of whether a data broker imposes a credentialling process, and how many data broker data breaches it experiences, were included as a compromise because the law did not require credentialling or the direct reporting of data broker data breaches. As the current bill (mostly, see below) corrects those omissions, sections (D) and (E) are no longer necessary.
- Finally, I have long argued that the exemption of public information from covered data definitions is a huge loophole and fatal flaw for many privacy laws. This bill fixes that problem in its definition of publicly available information, section 2430(16)(B). I hope that you fight like hell to keep that section intact, and that it will serve as a model for other states.

All that being said, I do have four suggestions as to how this bill could be improved:

1. Most critically, fix the data broker data breach language, which currently does not accomplish what you want it to;
2. The prohibition on "fraudulent acquisition of data" can be improved to address current enforcement gaps;
3. You might consider expanding the definition of data broker to include certain major first-party data brokers; and
4. Consider fixing a key jurisdiction issue.

First, I am heartened to see that a direct notification requirement for data brokers in the event of a data broker security breaches has been included. Although the necessary definitions were included in the original bill, the actual notice requirement never made it in. This is necessary because data brokers often collect copious amounts of information about consumers: thousands of data points including addresses, birthdays, purchase histories, and other information that can be valuable to fraudsters. Historically, con artists have had to research their targets before committing a fraud. Data brokers have in effect permitted con-artists and scammers to outsource this task.

However, the way this requirement has been implemented is flawed, for the following reason:

1. Security breaches are defined as breaches that involve "Personally Identifiable Information," or PII. PII are data elements that are so sensitive that if they are lost, those elements when connected with individuals have a high likelihood of harming consumers: social security numbers, financial account numbers, etc. All companies, including data brokers, are currently required to report data breaches involving PII. In other words, if a business accidentally discloses the T-shirt sizes of all its customers, it does not need to report that as a security breach, because T-shirt size is not PII. A criminal knowing my T-shirt size is not likely to cause me harm.
2. "Brokered Personal Information" is a much broader type data than PII. That is because if a data broker collects T-shirt sizes, in addition to 4,000 other data points, the aggregate of all that information permits such a detailed profile of the consumer that its breach is harmful to consumers, even though none of those data points, in isolation, might be harmful. Data brokers often collect these giant data sets which do not include PII, meaning that they do not have to report these breaches.
3. The law as currently written contains a definition of "data broker security breach" which is identical to the definition of security breach, except that the data affected is brokered personal information, not PII.
4. This bill deletes the definition of "data broker security breach" and adds the words "data broker" to the definition of security breach next to "data collector." But data brokers are already considered a data collectors for the purposes of PII security breaches. That is to say, if a data broker experiences unauthorized acquisition of social security numbers, it must already report that breach under current law.
5. You want data brokers to have to report that broader category of breaches that are dangerous due to the sheer volume of data points the data brokers collect. This bill contains a new section 2436 which outlines the procedure for reporting "data broker security breaches," but that term is no longer defined. The only definition is the narrower PII data breach definition, which means, as currently drafted, section 2436 adds no obligations that data brokers don't already have.
6. The solution is to put back the definition of data broker security breach. Adding data brokers to the definition of security breach does not address this problem.

Second, I suggest you expand the prohibition on fraudulent acquisition of brokered personal information in section 2431(a). I would change "fraudulent means" to "deception." It is much more difficult to prosecute fraud, which is why we have statutory deception in Section 2453. Also, prohibit the use of brokered personal information that violates the terms through which the person acquired it. For example, anyone can acquire the Vermont Statewide Voter Checklist upon certifying that they "will not use the information in the statewide checklist for commercial purposes" under penalty of perjury. A

short internet search will demonstrate that data brokers have done exactly that. The only penalty for doing so, however, appears to be a prosecution for perjury, which is unlikely to happen.

Third, when the law passed some critics didn't like that it only covered third-party data brokers. The current bill does expand the definition to include first-party data brokers who obtain data through third-party means, which is an improvement. However certain businesses that collect enormous amounts of data about consumers directly, such as Google, Meta, and Amazon, appear to be exempt under this law. I propose including first-party acquirers of data above a certain threshold, like "collected the data of more than 200 million consumers in the previous year."

Finally, recently the Superior Court of Washington County dismissed the Vermont Attorney General's lawsuit against Clearview AI, the company that screen-scraped billions of images, including Vermonters, for an invasive facial recognition tool. The court found a lack of personal jurisdiction, essentially finding that Clearview AI lacked sufficient contacts with the state of Vermont. I ask that this committee consider ways to address jurisdictional issues when it comes to data, and to include language that makes it clear that if a company is collecting the personal information of Vermonters, that gives Vermont courts jurisdiction to hold them accountable.