Testimony on H.211 before Senate Committee on
Economic Development, Housing & General Affairs

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

April 22, 2026

My name is Ryan Kriger. I am a resident of Montpelier, Vermont. I have over twenty years' experience as an attorney and specialize in consumer protection, privacy and data security. I have worked for the Vermont Attorney General and the Federal Trade Commission's Division of Privacy and Identity Protection, and I am currently the Deputy Chief of the Massachusetts Attorney General's Privacy and Responsible Technology Division. I also teach privacy, consumer protection, public policy, and administrative ethics at the University of Vermont.

I testify today in my personal capacity as a citizen of Vermont. My testimony does not reflect the positions of the Massachusetts Attorney General or that of her office.

I'd like to start with some big-picture observations, and then I will try to address some of the claims that have been made before this committee.

The data broker industry has been around for decades, but it didn't really experience public scrutiny until around 2014. They have had over a decade to address the many concerns that have been raised about them, but it appears that rather than try to reform their industry, they have instead decided to dig in their heels and oppose any efforts to reform them.

There are likely over a thousand data brokers out there, and potentially many more. Some data brokers are very large and sophisticated, like LexisNexis. Others appear to be very small, like National Public Data, the data broker that had a massive breach of almost 3 billion rows of data in 2024 (it is likely that 100 – 200 million consumers were affected). There doesn't need to be a correlation between the size of the business and the amount of data they are able to collect. Even a small, unsophisticated business can collect your data.

Some data brokers don't appear to have any scruples about who they'll sell your data to. Congress had to pass a federal law in 2024 to stop data brokers from selling our data to foreign adversaries.[1] LexisNexis will sells immigrants' data to ICE. They were sued in 2024 by immigrants' rights organizations to make them stop, but managed to get the case dismissed. In their filing they did not deny selling data to ICE, but instead emphasized that despite plaintiffs' claim to a right to privacy, "no such right exists." Back in 2006, the Federal Trade Commission levied the largest penalty it had ever implemented against ChoicePoint—$10 million—for selling people's Social Security numbers, birth dates, and credit histories to identity thieves, causing the actual compromise of over 163,000 consumers' financial data. ChoicePoint no longer exists as an independent entity; they were acquired shortly thereafter for $4.1 billion by LexisNexis.

But even if data brokers are not affirmatively trying to sell your data to bad guys, as so many do, the very fact that they have your data puts you at risk. That's because no one can fully protect your data. It is impossible to guarantee that a data breach won't happen. And data brokers have even less incentive to try to protect your data than other businesses, since no one even knows they have their data and they often have no duty to notify of the breach. We all remember the 2017 Equifax breach, which, by the way, turned out to have been conducted by China. But of course they're not alone. In December 2024, LexisNexis experienced a data breach exposing the names, dates of birth, phone numbers, email address, Social Security numbers, and

[1] The Protecting Americans' Data from Foreign Adversaries Act of 2024

driver's license numbers of 364,000 people. They did not report the breach for 6 months, until May 2025. It is reported they also had another breach last month, in March 2026, though it is unclear whether consumer data was involved.

I say all this by way of explaining that even if data brokers have our data and are acting with the best intentions, the very act of their collecting our data puts us at risk. As you know, many state privacy laws contain a data minimization provision. Data minimization is as close to a silver bullet as we have to protect our privacy and data security. The idea is that data breaches cannot be fully prevented, but companies can reduce our exposure by deleting data when it is no longer needed, and not collecting more data than they require. What's more, data minimization does not require any consumer to opt in or opt out to be protected – the duty lies solely with the data controller.

The problem is, even though many of these laws apply to data brokers, the data minimization provisions don't make much sense as applied to that industry. That's because the data broker's entire business model is data *maximization*, of collecting as much data as possible and holding on to it, thereby maximizing all of our exposure to risk. In light of this, our best defense is a right to ask data brokers to delete our data.

This bill goes a long way towards helping protect consumers, and it appears to have been very carefully drafted. I believe that on the House side, all sorts of people from industry, enforcement, academics, and data scientists were consulted to craft this language. For that reason, I hope the committee will be cautious in creating additional exemptions. I also ask that if the committee does include additional exemptions, they keep them to the relevant section, 2446(c)(3), and that they reject any suggestions that they change key definitions like "data broker" and "consumer."

I'd like to briefly note that I was confused by some of the objections to the bill that I have heard in prior testimony. For example, Mr. McLaughlin from the National Association of Mutual Insurance Companies essentially said that the insurance industry is already regulated at the federal and state level and that it would be inefficient to have to comply with this law as well. He also stated that insurers often need to retain personal information and that deletion requests would interfere with those needs. However, insurance companies will not have to comply with this law, because insurance companies are not data brokers. Nothing in this law prevents insurers from acquiring data about their customers, and they would not be required to delete data under this law.

We've heard testimony that allowing consumers to delete their data will interfere with attempts to review consumers' credit, but data brokers are allowed to reject requests to delete data that is used for Fair Credit Reporting Act purposes. Similarly, objections based on the need to prevent fraud or authenticate users fall flat, as those uses are also already exempted from the law.

One use of data that is *not* exempted, and which industry representatives have been silent on, is the use of data for marketing purposes. I suspect that is a concern for a lot of businesses, but I think it's fair to argue that the heightened risk consumers are put through by having data brokers collect their information outweighs the opportunity for businesses to send more spam and junk mail.

Finally, I would like to say a word about enforcement. There is no point to passing a law that will be ignored due to weak enforcement. I have full faith in the Attorney General to enforce this law to the extent of her ability, but her office has limited resources. I understand that private rights of action have been demonized for the past few decades, but if you consider what it actually is, they make sense. All they say is that if someone violates the law and harms you, you can seek a remedy and be made whole. Imagine a world where, if a car crashes into your own, you have no right to sue, but instead must file a complaint with the Attorney General.

That wouldn't make a lot of sense. If someone harms you, you should have the ability to seek an appropriate remedy. Note that someone suing under this law would be able to claim damages, or perhaps treble damages —which would only be provable in limited circumstances, such as where a data broker fails to delete data on requests, then suffers a security breach, and *then* a consumer experiences identity theft that is tied back to that breach. This law would be different than, for example, the Illinois Biometric Information Protection Act. That law includes statutory damages of $1,000 to $5,000. There is no such provision in this law.

I have also included a few reports with my testimony, including one from the U.S. Congressional Joint Economic Committee titled "Opt-Out Obstacles: Concerning Practices by Registered Data Brokers and the Multi-Billion-Dollar Cost of Breaches," and a report issued by the Consumer Financial Protection Bureau titled "State Consumer Privacy Laws and the Monetization of Consumer Financial Data," which warns against including broad exemptions from state privacy laws for entities covered by the Gramm-Leach-Bliley Act.

I would like to thank this committee for doing such great work, and for giving me the opportunity to contribute my knowledge, experience, and concerns, in order to craft a sensible solution to the problem caused by irresponsibility in the data broker industry.