Zach Edwards
Threat Analyst
zach@victorymedium.com

Members of the Committee, thank you for the time today.

My name is Zach Edwards and I'm a Senior Threat Analyst and a researcher with over 18 years of experience.

I'm providing feedback today because I'm an expert at tracking people and setting up systems to track behaviors on the internet.

For the first 10 years of my career I worked on dozens of digital advertising campaigns both for political and commercial clients. I've spent and managed millions of advertising dollars, and I've helped to make decisions about data to purchase and "data appending solutions" for clients.

Over the last 8 years I've been conducting research into a wide range of internet threats, supporting privacy complaints both in Europe and the U.S., and I've helped reporters, regulators and the public understand complex technical challenges.

Before I get too far into my testimony, I want to acknowledge that I'm not a Vermont resident, I'm from California. I did however recently have the pleasure of attending a family reunion in Vermont, and enjoyed the state thoroughly. But I certainly don't consider myself an expert on Vermont politics, so I appreciate your patience with me.

I am however an expert in online privacy and online threats, and I am someone who knows these issues backwards and forwards.

I'm here today to stand in support of H.342 and to explain why I think this bill makes good progress to protect vulnerable citizens in Vermont.

This bill aligns with a sensible effort in New Jersey called Daniel's Law.

It's important to appreciate that this bill isn't novel – it's using simple language like we've seen elsewhere, and it's attempting to plug a big privacy hole that creates risks for government employees, police officers, judges and other civil servants.

This bill puts guardrails around a few different types of data, which if exposed could put someone's physical safety at risk.

The bill covers home and secondary addresses, home telephone numbers, personal email addresses, Social Security or drivers licenses, and license plate numbers. That's it. These are narrowly-defined pieces of data which can be used to track someone.

And I think it's important to pause and explain that the data that is covered, is also the data that numerous data brokers are selling right now all over the internet. Anyone with a pulse and a credit card can buy data on Vermont residents, including on sensitive government workers. And many of these services make it incredibly easy to buy profiles of people that contain all the details that are known – dozens of fields of sensitive data.

I think it's also important to highlight that Local, State and Federal government agencies often release sensitive details about individuals, especially with regard to property ownership, voting, business registrations, and court orders. And many data brokers point to these disclosures as evidence that what they are doing is acceptable and even normal.

But don't buy into those lies. What data brokers are doing right now all across the internet makes every type of government transparency effort look like a solid steel wall. There has never been more data floating around – sensitive personal data – than we have right now. For less than $5 you can buy reports from dozens of websites that include everything you need to stalk someone. The problem is deeply out of hand and the scale is hard to imagine.

It should also be noted that the reason why data brokers are such experts on the personal data being shared from governments, is that they are the number one user of that data. Right now, the biggest user of government data at the local, state and federal levels are data brokers and AI companies. Period. They are scraping and saving every piece of consumer data not bolted to the floor, and they are making money off government transparency while pretending like they aren't creating significant risks for certain communities and individuals.

As a California resident who has exercised my rights under our privacy frameworks, I can tell you that our "Right to say No" and to opt-out of data broker sales has been extraordinarily useful – but it's not enough just to give people these rights and to expect global data brokers to comply with sensible requests.

Every single month more data brokers are added to the California data broker registry, and there is a massive sprawl of these businesses being formed with overseas investors, who are mining Americans data for profit. Many data brokers are also not even registered – they either don't know or don't care about the state by state privacy laws – essentially becoming invisible for anyone who isn't an expert in this field.

For the data brokers who don't register in a state or aren't complying with state laws, relying on the government to enforce these complicated frameworks is a nearly impossible task. How is a government agency supposed to hold hundreds of data brokers accountable for niche violations? They can't. It's impossible. And we can know this is true by just looking at the speed of privacy complaints being resolved globally. When you require a government agency to solve complex business disputes, you either need to dramatically scale up the size of government, or warn your constituents about the speed of justice.

This Vermont bill strikes a healthy balance with the allowance for a private right of action, while capping damages to ensure that this framework is used to prevent non-compliance, and not as a windfall for litigators.

I want to highlight again that this is a battle between regular folks who may not understand these systems, and global data brokers who don't care at all about personal privacy.

And I want to make a disclosure – I've personally bought data from these brokers, and that data included bulk location data for people in Vermont.

I want to pause and repeat myself to make sure everyone understands what I just said. It's possible right now to buy bulk location data for people in Vermont – data and signals acquired from the so-called "advertising bid stream" aka the "Real time bidding" advertising ecosystem are being actively sold by global data brokers.

And why does this matter? If a threat actor is able to buy bulk location data, and if a vulnerable target isn't properly protecting their phone from transmitting a "Mobile advertising ID" which is then used to associate location data to a singular device, then it's possible to connect up a known location like a home address, to other locations that person frequents.

It's possible to pivot from a home address into a church, or a school, or a local coffee shop, or somewhere more sensitive that someone goes to regularly.

If civil servants and government employees aren't able to request redaction of their personal details from global data brokers, then it becomes possible for someone to pivot from protected PII like a home address, into even more sensitive details using location data.

And this location data isn't just available for commercial interests, this data is widely purchased by governments all over the world who can then use the data to understand all types of geopolitical events.

To my knowledge, this bill is not attempting to reform the online advertising systems, or the location data brokers that facilitate bulk location sales derived from mobile devices. But it's solving the issue from the front-end — if someone is able to protect themselves by removing their details from global data broker systems, it becomes much harder for that person to be tracked with other methods.

If someone can remove their physical address from being sold by hundreds of data brokers, this protects someone in a way that most people don't understand. This means that when a random stalker searches "People finder" on a search network and stumbles into any of the results, they won't be able to easily find sensitive details on a judge or a police officer who has taken efforts to opt-out of those data sales. This won't solve all stalking risks or personal safety concerns, but it stops making sensitive personal data widely available for anyone and everyone who can use a search engine and has a credit card.

I think it's important to appreciate that this bill balances privacy and First Amendment rights. This bill wouldn't prevent a reporter from writing that an elected official lived outside their district, it would merely prevent the exact home address from being made public. Is this perfect? No, but we live in an imperfect world and can't ignore the real physical risks to civil service workers.

Right now, any state that doesn't have a comprehensive data privacy framework is putting their citizens at significant risk – and government employees and civil servants face unique physical threats from those lack of protections. And without a strong framework that allows people to independently enforce these complex laws, Vermont will just become another state with a privacy law and an overburdened privacy agency, along with unmet expectations from constituents.

I appreciate this opportunity to speak out in favor of H.342 and I urge passage of this important piece of legislation. Thank you for your time.