Testimony from Jeff Jockisch on Vermont H342

Chairperson, Members of the Committee, and Representative Priestley.

Thank you for the opportunity to speak today. My name is Jeff Jockisch, CXO of ObscureIQ. My partner Colby Scullion and I specialize in data privacy, digital security, and the surveillance economy.

Through our work, we track over 8,000 organizations engaged in data collection and brokerage, mapping how personal data flows, who profits from it, and how individuals - especially those in sensitive roles - are put at risk.

The reality is stark: publicly available personal information has become a weapon. Judges, law enforcement officers, public officials, and others performing critical jobs face escalating threats - not just online harassment, but real-world dangers from doxxing, swatting, and targeted violence.

H.342 is a necessary response to this growing threat. It addresses a glaring gap in how Vermont protects those who serve the public from the unchecked exposure of their personal information. Today, I'd like to focus on the role of data brokers and how this industry fuels these risks - along with key considerations for implementation.

Slide 1: Pre-Internet

==

In the past, when we interacted with businesses, the value exchange was clear: we shared some personal data in return for a coupon, a discount, membership in a loyalty program, or inclusion on a mailing list.

But those days are long gone - though most people haven't fully realized it. And that's a problem.

Because the landscape has fundamentally changed.

This is the core issue: businesses' privacy policies and the data broker industry exploit consumers in ways that weren't possible before.

Let's take a brief walk through history to understand how we got here.

You shared your data with the government.
You shared your data with businesses.
But data brokers? They were barely a factor in our daily lives.
Back then, giving your data to one company didn't mean it would end up in the hands of another business, a data broker, or even the government.

We can't say the same today.

Slide 2: How Do Brokers Get Data?

==

So, what changed?

Digital data means copies are everywhere.

Consider this example:

A student takes an online survey sponsored by Edvisors.
Their data is sent to Experian, a credit bureau, for identity resolution and enhancement.
It also goes to ALC (American List Counsel), now rebranded as Adstra.
ALC plays a major role in the data economy - despite being largely unknown to the public.
ALC then partners with Ethnic Technologies, which predicts the student's ethnicity, religion, and language skills before repackaging and selling the enriched data to marketers.
This is just one small example of how personal data flows, gets copied, and is further monetized.

Slide 3: Early-Internet

==

Let’s go back to the early internet.

This is when data brokers entered our lives - primarily through adtech.
Adtech became the internet’s funding model. You probably know the story:

Originally, Google resisted using adtech to make money.
But after taking venture capital, they needed a revenue model.
The solution? Ads in search results.

Google then acquired DoubleClick, which changed everything:

- It placed cookies on users’ computers.
- It tracked browsing history.
- It enabled targeted and personalized ads.

This was the foundation for today’s online advertising and data collection practices.

Slide 4: Today

==

The chart may look similar, but today’s data landscape is an entirely different world.

The data broker industry now generates over $300 billion annually - not just for ads, but for surveillance.

While some data brokers operate within the law, many sell data indiscriminately with little oversight.

Data flows everywhere:

- Government agencies may acquire it, bypassing Fourth Amendment protections.
- Bad actors can buy it easily or steal it through frequent breaches.

The scale is staggering. I personally track over 8,000 organizations surveilling consumers.

The line between businesses and data brokers has blurred. Companies aren't just selling products - they're monetizing your data as a lucrative side business. From car manufacturers to phone companies, software providers to utility services - they're all in the data game.

This new reality demands new laws. We are living in a world that most people don't fully understand - and the laws haven't caught up.

Slide 5: A History of of Privacy & Tech

==

This chart tracks key trends from 1970 to today.

Red Line: The Growth of Information Technology
It started with mainframes, then PCs in 1980, the Web in 1990, and Google before 2000.
Then came Facebook, the iPhone, Big Data, IoT, and now Generative AI.
Data Growth Has Been Even More Exponential.

Gold Cloud: The Rise of Massive Data Breaches
2005: Breaches started escalating.
More data collected → More data stored → More data breached.
2013 onward: Leaks from Snowden and others revealed just how deep government surveillance runs in a big-data world.

At the top of the chart, you'll see privacy legislation trends - but I won't go into them here. The key takeaway is this: our current laws do not protect personal data.

Slide 5: Are Brokers Regulated? Not Much.

==

Data brokers remain largely unregulated.

- There are a handful of laws, but they can easily work around them.
- They sell personal data freely.
- And they rarely face consequences.

Extro

==

Data exposure is not just a privacy issue - , It’s a security issue.

If Vermont fails to act, bad actors will continue exploiting this loophole, accessing sensitive personal information in ways that can put public servants in harm’s way. This bill is a practical, necessary step to align the law with modern threats and set a standard for responsible data handling.

I appreciate the Committee’s attention to this critical issue and am happy to answer any questions.