Written Testimony in Support of S.71

Vermont Data Privacy and Online Surveillance Act

Submitted by Melanie Ensign, Founder & CEO, Discernible

April 29, 2026

Introduction

My name is Melanie Ensign. I'm the founder of Discernible, a cybersecurity and privacy communications advisory, and a small business owner. I hold a master's degree in corporate public relations and spent fifteen years working in PR for some of the largest technology companies in the world. I am submitting this written testimony in support of S.71, the Vermont Data Privacy and Online Surveillance Act.

I am not a lawyer or a political expert, but I know exactly how the companies lobbying against this bill communicate with legislators, because I have been in the rooms where those strategies are developed. The purpose of this testimony is to name those tactics plainly, so that policymakers can recognize them for what they are.

The five tactics described below are documented, studied, and named in the academic literature on public relations and crisis communication. They are also, in my direct professional experience, actively in use today.

Tactic 1: Harm Denial

When a company claims there is no evidence its products cause harm, that claim frequently reflects a deliberate choice not to measure harm, or to structure operations in a way that makes harm difficult to trace. The absence of evidence is not evidence of absence.

This industry has deliberately chosen complexity over accountability and uses that complexity as a shield. That choice is a business strategy and S.71 directly addresses this by requiring data protection assessments for high-risk processing activities, including targeted advertising, processing of sensitive data, and profiling that affects decisions about housing, credit, employment, and health care. These assessments create a record of decision-making that is essential for future accountability and enforcement.

The relevant bill section is §2415g (Data Protection Assessments).

Tactic 2: Consumer Blame

Legislators will hear some version of the argument that consumers choose to share their data, that they agreed to terms of service, and that they have sufficient tools to protect themselves. This framing is deliberate and well-documented in public relations scholarship and literature as a strategy for shifting responsibility away from powerful institutions and onto individuals.

S.71 explicitly names and rejects this argument. The bill's definition of consent (§2415a(7)) excludes agreement obtained through dark patterns and acceptance of broad terms of service that bundle privacy language with unrelated content. This reflects a substantive judgment that meaningful consent requires genuine choice rather than a manufactured illusion of it.

When a child's school requires a platform account, consent is not voluntary. When an employer uses behavioral tracking software, opting out is not a realistic option. The consumer blame argument describes a world that does not exist for most people.

Tactic 3: Manufactured Complexity

Privacy and data infrastructure can be technically complex, but that complexity is a choice. Companies knowingly take on technical debt and accumulate data in pursuit of growth and monetization. So, the complexity isn't incidental — it's what happens when you prioritize data collection over responsible design, and then use the resulting mess as a reason you can't be held accountable.

S.71 is specific. The definition of sensitive data (§2415a(53)) covers Social Security numbers, financial account credentials, immigration status, pregnancy status, gender identity, sexual orientation, biometric data, precise geolocation, neural data, and keystrokes. These are categories of information that, when collected and sold without meaningful consent, expose people to demonstrable harm. The bill's prohibition on selling sensitive data (§2415e(a)(8)) is a clear line. Complexity is not a compelling argument against that line — on the contrary, it’s an argument for the kind of clear, enforceable standards this bill provides.

On the small business argument, legislators are also told that this bill would hurt small businesses. Big Tech and data brokers use small businesses as a human shield while simultaneously misleading them about how indispensable their platforms are. Data brokers in particular have no direct relationship with consumers at all — they collect, package, and sell personal information about people who have never heard of them and never agreed to anything. Small businesses are not partners in this data economy. They are, in large part, data collection points that generate value for the platforms and brokers, not for themselves.

This argument also does not hold up against legal precedent. A small medical clinic is not exempt from HIPAA because compliance is burdensome. Nor is a community bank

exempt from anti-fraud regulations because it is not a large institution. The risk to consumers isn't based on the size of the business handling sensitive information; the risk travels with the data whereve it goes.

Tactic 4: Delay by Design

Calls for more studies, working groups, pilot programs, and stakeholder input are sometimes legitimate. In the context of data privacy legislation, they more often function as strategies for postponement. This industry has had decades to self-regulate and their record on voluntary compliance is not good.

Moreover, S.71 has already made significant concessions to industry. Enforcement runs through the Attorney General rather than through a private right of action (§2415j). This means individual Vermonters who are harmed by violations can't sue and the entire enforcement burden falls on a unit of two attorneys and one investigator appropriated only $650,000. The industry has received substantial accommodations in this bill's current form. Further delay or weakening is beyond a negotiation — it's capitulation.

Tactic 5: Science Manipulation

This tactic has a longer and better-documented history than most people realize, and understanding that history is useful context for evaluating the research industry lobbyists will present to legislators.

Edward Bernays, described in his 1995 New York Times obituary as the 'father of public relations' and a nephew of Sigmund Freud, used his uncle's insights on human psychology to advise corporate clients on how to move public opinion. One of his best-documented campaigns was a 1929 effort staging women smoking publicly at the New York City Easter parade, framing cigarettes as 'torches of freedom' on behalf of the American Tobacco Company.

The tobacco industry later retained the PR firm Hill & Knowlton to run a coordinated campaign manufacturing doubt about the scientific link between smoking and cancer. Beginning in 1953, the industry created the Tobacco Industry Research Committee to challenge mounting evidence of harm, funded alternative research designed to produce the appearance of scientific controversy, and distributed materials to doctors, media, and policymakers insisting there was no cause for alarm — all while internal industry documents showed executives privately acknowledged the evidence against them.

The same pattern has appeared in the technology sector and data brokers. In 2021, internal Facebook documents leaked by whistleblower Frances Haugen revealed that the company had conducted its own research into Instagram's negative effects on teen mental health, was aware of possible solutions, and had not acted on that research publicly. Six months before the leak, CEO Mark Zuckerberg testified before Congress that 'the research is not conclusive' on the connection between social media and teen mental health.

When industry presents legislators with research about the economic value of data sharing or the impracticality of data minimization, the appropriate questions are: Who funded this research? What research is not being presented (and why)? What do the companies' own internal studies actually show?

Conclusion

S.71 establishes that Vermonters have the right to know what data is being collected about them, to correct it, delete it, and opt out of having it sold or used to target them. It prohibits the sale of the most sensitive categories of personal information — the kind that can get someone fired, deported, denied housing, or physically harmed. Far from radical propositions, they are baseline conditions for any business, regardless of size or industry, to operate honestly, ethically, and with respect to human dignity.

I have spent my career helping security and privacy professionals communicate more clearly with the public. That work is necessary because the default in this industry is obfuscation and deflection. The protections consumers deserve do not happen voluntarily. They have to be required.

This bill is not perfect. No bill is. But the industry lobbying against it is not worried about compliance costs. They are worried about accountability. This bill should pass without further weakening.

Key Sources Referenced

S.71 Draft (April 24, 2026): Vermont Legislature

Edward Bernays, Wikipedia: en.wikipedia.org/wiki/Edward_Bernays

"A Frank Statement" and Hill & Knowlton tobacco campaign, Wikipedia: en.wikipedia.org/wiki/A_Frank_Statement

Inventing Conflicts of Interest: A History of Tobacco Industry Tactics, PMC/NCBI: pmc.ncbi.nlm.nih.gov/articles/PMC3490543

Facebook's Internal Documents on Teen Mental Health, The Conversation: theconversation.com

Whistleblower Frances Haugen Senate Testimony, NPR: npr.org

HIPAA Overview, HHS: hhs.gov/hipaa