Testimony of

Mike Yeagley
President of Cohort.ID

Before

VERMONT GENERAL ASSEMBLY
HOUSE COMMITTEE ON COMMERCE AND ECONOMIC DEVELOPMENT

On

“H.211”

Wednesday, January 14, 2026
Via VTC

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Introduction

Chair Marcotte, Vice Chair Graning, Ranking Member White, and Members of the Committee:

My name is Mike Yeagley. Nearly ten years ago, I delivered a wake-up call to U.S. Special Operations Command and Department of Defense leadership by exposing a clandestine forward operating base in a warzone—not through a hack or breach, but by purchasing commercially available data.

The message was simple: if a history major from St. Lawrence University could do this from a home office, hostile actors could do it too—if they weren't already.

Today, I advise the U.S. government on national security risks arising from commercial data systems and surveillance infrastructure, and I serve on the Board of Advisors for Unplugged, a privacy-focused smartphone company that designs hardware and operating systems to minimize data collection, tracking, and third-party telemetry.

I am here to offer my perspective on strengthening and future-proofing Vermont's privacy posture.

The Issue

The issue before this Committee is control of personal data—a central fault line of modern geopolitics. In this century, protecting the data heartland—from Bradford to Burlington, from the Vermont Brigade's 86th Infantry Brigade Combat Team to families in Morrisville—is as consequential as protecting shipping lanes once was for maritime empires.

Today's data ecosystem is dominated by an $8 trillion duopoly and a $740 billion advertising economy engineered to extract behavioral data at scale. A single mobile device is interrogated hundreds of times each day by opaque third-party networks that include foreign entities and adversarial actors.

When adversaries use the same data pipelines as advertisers, privacy becomes a national security issue. And when federal policy falls short—as demonstrated by years of

missteps surrounding TikTok—states become the front line of defense. That is why this Committee's work matters not just for Vermonters, but nationally.

When our movements can be tracked, our relationships mapped, and our intentions modeled, we cease to be citizens and become subjects.

Privacy is the surveillance circuit breaker that preserves individual freedom.

Future-Proofing Privacy Policy

I evaluate privacy from the perspective of adversaries who arbitrage commercially available data to obtain intelligence that would otherwise require high-risk operations. Why hack, intercept, or steal what can be bought?

The same data flows that enable commercial targeting, attribution, and analytics also lower the cost of intelligence collection, influence operations, and coercion when accessed by hostile actors.

The danger lies not in who uses the capability, but in the capability existing at all without consent.

That reality fundamentally changes the nature of risk.

When sensitive information can be purchased legally, the barrier to exploitation collapses. Capabilities once limited to intelligence services with significant resources are now accessible to anyone with a credit card and a plausible business justification. This is a structural vulnerability. Commercial data markets turn convenience into access, access into insight, and insight into power—often without the knowledge or consent of the people being observed.

This dynamic affects Vermonters. A teacher, healthcare worker, or high school student who disables tracking and never shares their name may still be recognized, linked, and profiled over time based solely on patterns of device use, movement, and network behavior. From the individual's perspective, privacy settings are enabled. From the system's perspective, identity has simply been reconstructed.

This is where state policy matters. Vermont cannot control how foreign intelligence services operate, but it can control whether commercial data markets make their work easier. By setting clear limits on identity reconstruction, cross-context linkage, and persistent tracking without consent, Vermont can raise the cost of exploitation and restore friction where it belongs.

Effective privacy legislation does not need to anticipate every new technique; it needs to regulate outcomes. When the outcome is persistent identification or cross-context linkage without consent, the harm is the same regardless of the technical method used. Done correctly, state law becomes a practical countermeasure—reducing exposure, limiting abuse, and protecting Vermonters from risks they never agreed to assume.

H.211 meaningfully strengthens transparency and accountability for traditional data brokers and includes a strong definition of brokered personal information, covering derived data, unique identifiers, and information that is linked or reasonably linkable to an individual or device. That language correctly recognizes a core reality of modern surveillance: identity is often inferred, not explicitly stated.

Modern tracking no longer depends on a single identifier like the advertising ID. That function is now replicated through the aggregation of metadata—device characteristics, network behavior, timing, location patterns, and usage signals—that, when combined, allow identity to be inferred with increasing precision.

This reflects a broader shift from regulating data as an object to regulating identity as a capability. The primary risk is no longer the sale of records, but the sale of the ability to continuously recognize, link, and predict individuals across time and context.

Legislation must therefore address the use of metadata for identity reconstruction, not just the presence or absence of explicit identifiers. By regulating outcomes such as persistent identification, cross-context linkage, and identity reconstruction without consent, Vermont can protect its residents from commercial exploitation while simultaneously denying adversarial actors an inexpensive path to intelligence, influence, and interference.

This approach does not restrict basic analytics, security functions, or first-party services. It targets covert identity reconstruction that occurs outside a direct consumer relationship and without meaningful consent.

In doing so, Vermont's privacy framework serves both consumer protection and national security—reducing harm at home while raising the cost of abuse abroad.

H.211 recognizes that modern privacy risk flows from identity reconstruction and linkability, not just explicit identifiers, and gives Vermont the authority to regulate that reality.

A clear statement of legislative intent clarifying that identity reconstruction and persistent linkability are regulated outcomes—regardless of technique—and that covered entities retain responsibility for preventing such data from being sold, transferred, or made accessible to foreign adversaries would future-proof Vermont's privacy framework and address emerging national security risk.

The remaining question is how Vermont implements these protections in a way that remains effective as technology and adversarial use of commercial data evolve.

Using the Authority Vermont Already Has

With the statutory foundation established by H.211, the remaining work is implementation aligned with how modern data systems actually operate.

Effective privacy regimes do not attempt to enumerate every dataset, data type, or business model. They succeed by clarifying how the law applies as technology evolves. Vermont can do this by emphasizing outcomes over labels and by using its enforcement authority to address identity reconstruction wherever it occurs.

First, Vermont should clarify that identity reconstruction and persistent linkability are regulated outcomes under H.211, regardless of technique. If a system enables an individual to be identified, linked across contexts, or persistently tracked without consent, that activity should fall within regulatory scope even when no traditional data "sale" occurs and even when data is described as derived, modeled, probabilistic, or anonymous.

Second, Vermont should treat third-party identity reconstruction as a high-risk processing activity. Where identity is reconstructed outside a direct consumer

relationship—through attribution, fingerprinting, or inference—affirmative and revocable consent should be the standard.

Third, Vermont should clarify compliance responsibility for downstream access. Entities that enable identity reconstruction or persistent linkability should remain accountable for how that capability is accessed and used, including when data or services are sold, transferred, or made accessible to foreign adversaries.

Finally, enforcement should remain focused on industrial-scale data intermediaries whose business models depend on large-scale data extraction, identity resolution, or third-party monetization—not small businesses using data to provide services to their own customers. This preserves proportionality while directing regulatory attention to the practices that create the greatest risk.

Taken together, these measures allow Vermont to future-proof its privacy framework without reopening statutory text, reduce regulatory arbitrage, and ensure protections remain effective as technology and adversarial use of commercial data continue to evolve.

What Success Looks Like

An effective privacy framework is measured by outcomes. Success is not the number of disclosures filed or notices posted. It is whether harmful practices become harder, rarer, and more expensive to sustain.

Privacy policy is working when identity reconstruction without consent is no longer a scalable business model. When systems designed to persistently identify, link, or track individuals across contexts face clear legal risk, market behavior changes. Services built around covert identity resolution either adapt to consent-based models or exit the market.

Success also means restoring friction where it belongs. When commercially available data no longer provides a low-cost shortcut to intelligence, influence, or surveillance, exploitation becomes harder and abuse less attractive.

A successful framework aligns public law with existing platform-level protections. When state enforcement and platform rules reinforce the same baseline—that persistent identification without consent is prohibited—regulatory arbitrage collapses and compliance becomes clearer for businesses operating in good faith.

Ultimately, the question before Vermont is whether its laws preserve agency as technology scales, or cede it by default.

Closing

Privacy determines whether people retain agency in systems that increasingly operate beyond human visibility. It sets the terms under which technology serves people, rather than people serving technology. It ensures that participation in modern life does not require surrendering control over one's identity, behavior, or future.

In a world where data shapes power, **privacy is the discipline of a free society.**

Mr. Chair, that concludes my statement. Thank you for the opportunity to appear before the Committee. I welcome your questions.