Protecting Privacy, Empowering Small Business: A Path Forward with S.71

Thank you for the opportunity to provide testimony regarding S.71, the Vermont Data Privacy and Online Surveillance Act. I am writing as a small business owner with expertise in privacy and cybersecurity. For the past twenty years, I have witnessed firsthand how data practices affect businesses of all sizes.

I started a small business called Discernible[1] five years ago, headquartered in Miami, Florida. My team and I specialize in helping privacy and cybersecurity professionals improve their communication skills (e.g. negotiation and persuasion) to gain influence and political capital inside their companies and steer business leaders toward safer decisions. And we've seen it all – data-hungry executives pressuring product, engineering, and data science teams to access previously collected data for newly imagined purposes without user consent, competitors hacking each other with spyware, and even well-meaning safety brands overlooking the relationship between private personal data and safe spaces.

Before starting my own business, I worked on the front lines of some of the worst data breaches and privacy screwups in tech, from the NSA revelations in 2013 to the lead up to the Cambridge Analytica scandal at Facebook and any number of data abuses that became the hallmark of Uber's early days. With my new company, I knew we needed to do things differently so that respecting the privacy and security of user data wouldn't require a passionate team member to risk their career or personal safety to make their voice heard. We built our brand on the fact that we know what's at stake and are willing to fight for it – and we can teach others how to fight for it too.

Our Approach to Effective Marketing Without Surveillance

At Discernible, we deliberately built our marketing strategy without relying on invasive surveillance technologies. Instead, we focus on:

- **Content Marketing**: We publish blog posts and other resources that address the real communication and credibility challenges privacy and cybersecurity professionals face. We've established expertise that attracts new customers to our services while respecting everyone's privacy.
- **Community Building**: We host webinars, participate in industry events, and cultivate professional communities based on shared interests and challenges rather than intrusive

[1] https://DiscernibleInc.com

data collection. When we sponsor a conference, we don't accept the usual trove of attendee data that organizers like to dangle in front of financial supporters like bait. We also run short weekly drills for the security community to practice communicating effectively during a breach or other emergency. These weekly touch points are also a great way for our supporters to meet each other and interact with people who are not yet familiar with our other services.

- **Contextual Advertising**: We place content in relevant industry publications and outlets where our target audience already engages, focusing on context rather than spying on people across the internet. Our industry loves newsletters and podcasts, so we go there.
- **First-Party Relationships**: We collect only essential information through transparent, opt-in methods, always with clear purpose and consent. We practice the data minimization principles we preach and delete personal data as quickly as possible. When people sign up for our newsletter, we're very clear that we will only use their email address to send that newsletter. We never use that mailing list for anything else. We hold fast to that promise four years after we sent our first newsletter.
- **Word-of-mouth**: Our business has grown significantly through referrals and testimonials from satisfied clients who value our expertise and ethical approach to data. We also offer discounts and referral fees for partners who help us meet new clients.

These methods have proven more respectful of privacy and more effective at building the trust essential in our industry. Our experience demonstrates that the surveillance economy poses a significant challenge for small businesses, and legislative action is needed to ensure their survival.

The Small Business Privacy Challenge

As a small business owner committed to privacy, one of my most significant challenges is finding vendors with privacy-respecting services. This is not just a personal challenge, but a collective responsibility that all businesses, large or small, should share. The fact that I can't obtain the privacy-respecting tools I need, despite my willingness to pay for them, represents a significant market failure that legislation like yours can help address.

This situation creates two problems. First, it undermines our privacy promises to customers. Second, it introduces unnecessary security vulnerabilities via dormant code that serves no legitimate purpose. The fact that I can't obtain the privacy-respecting tools I need, despite my willingness to pay for them, represents a significant market failure that legislation like yours can help address.

Until recently, with the introduction of platforms like Bluesky and Mastodon, we didn't have viable social media options that provided adequate privacy controls. This forced us to abandon social media engagement entirely or encourage our customers to engage with us on surveillance-based platforms. Our business has never had an account on a Meta platform and I don't regret it.

Every business, including small businesses, can use free tools to uncover hidden tracking technologies on their websites. These technologies often operate without the business's knowledge or explicit consent, especially if it is outsourcing the creation and maintenance of its website to a contractor or service provider. The two tools I use most often are BuiltWith[2] and Blacklight[3].

BuiltWith reveals the technology stack behind any website, allowing you to see which third-party services, trackers, and analytics tools are embedded in your site. From investigative journalism outlet The Markup, Blacklight goes even deeper, exposing surveillance techniques like session recording – which captures keystrokes, mouse movements, and scrolling behavior – fingerprinting, and hidden third-party cookies. Small business owners can use these tools to see what's actually happening on their websites, identify privacy vulnerabilities, and take steps to protect both their business and their customers.

The current draft of S.71 requires clear privacy policies, seemingly good for consumers. However, the lack of privacy-respecting options transformed privacy policies from a healthy dialogue with users into something that feels more like an "accept at your own risk" warning. Instead of confidently explaining how we protect customer data, small businesses are forced to disclose the limitations imposed by our vendors and the potential risks that remain despite our best efforts. This is not how building trust with customers works, and it puts small businesses that care about privacy at a disadvantage in establishing authentic relationships with our customers.

Big Tech's False Small Business Narrative

In my previous career, I spent a decade working for major tech platforms, including several that run advertising businesses. Big tech's narrative that privacy legislation harms small businesses is not just misleading, it's a gross injustice. Instead, it uses small businesses as human shields to protect its surveillance-based business models, putting the very businesses it claims to champion at a severe disadvantage.

Over the years, these companies have systematically manipulated small businesses into believing that participation in surveillance-level marketing and advertising is essential for success. This carefully crafted narrative suggests that without invasive tracking, detailed customer profiling, and targeted ads that follow people across the internet, small businesses cannot compete. This is not true, but many small business owners feel they have no choice but to participate. The advertising and platform giants continue pushing the message that their surveillance tools are indispensable, creating unnecessary fear among small business owners about privacy legislation. I know they've approached several members of this body over the past several years as you pursue the creation of your own state privacy laws. They're also bombarding us with marketing hype about the necessity of invasive tracking, but this narrative represents their interests, not ours.

---

[2] https://BuiltWith.com
[3] https://themarkup.org/blacklight

If these industry giants cared about small businesses, they would advocate for privacy bills that include financial and technical support to help us respect customer data while remaining competitive. Instead, they've created an ecosystem where privacy-invasive practices are the default, and small businesses have limited alternatives.

Small businesses can flourish without relying on invasive surveillance technology. They can build customer relationships through quality products, excellent service, and community engagement, not by tracking people or harvesting their sensitive data. That's gross.

Data Minimization Makes Business Sense

From a practical business perspective, collecting and storing excessive customer data is a liability, not an asset. As someone with expertise in privacy and cybersecurity, I've made the deliberate choice not to collect data I don't need because storing and protecting it properly is expensive.

It's important to understand that most small businesses simply cannot afford to implement robust data protection measures once they already possess sensitive data. We have a term for cybersecurity: "the security poverty line." This concept describes organizations lacking the resources, expertise, and budget to protect themselves and their customers' data from modern threats. Most small businesses fall below this security poverty line—not from negligence, but from economic reality. When tech platforms encourage small companies to collect vast amounts of customer data without explaining the true costs of securing it, they're setting these businesses up for failure and potentially catastrophic breaches.

Verizon publishes an annual Data Breach Investigations Report, widely regarded as one of the most authoritative and comprehensive annual analyses of global cybersecurity incidents. The report draws from thousands of confirmed breaches across industries investigated by security professionals worldwide.

In 2019, the report[4] addressed a crucial misconception about data breaches and small businesses:

> *"Small businesses are target #1 for criminals and represent 43% of all data breaches — often because their false sense of security leads them to not put proper defenses in place. It's like a homeowner leaving doors unlocked and open because he figures the criminals will go to the wealthier homes up the hill.*
>
> *What criminals do, though, is first go to the unguarded "homes" at the bottom of the hill to steal stuff. Small businesses have plenty of customer information — like credit card numbers, email addresses, and insurance details — that are enticing to cyber criminals.*

[4] https://www.verizon.com/business/resources/articles/small-business-cyber-security-and-data-breaches/

> *Criminals also see another benefit from attacking small businesses. They can be the entry point to invade the networks of larger companies they do business with. A study by the Ponemon Institute found that 59% of companies have experienced a data breach caused by a third party or one of their vendors with whom they have shared sensitive information.*
>
> *In this sense, the criminals break into the "homes" at the bottom of the hill, and then climb the fence to get to those "wealthier homes."*

This reality makes data minimization not only a privacy best practice but an economic necessity for most small businesses.

Big companies that profit from selling user data rarely inform small business owners about the downstream costs if that data is leaked or stolen from our systems. When a breach occurs, the small business faces reputational damage, potential liability, and loss of customer trust – not the tech vendors who encouraged the collection in the first place.

The solution isn't to pretend small businesses aren't vulnerable targets or to exempt them from privacy regulations. Rather, we need to level the playing field by restricting the data collection and processing practices of large tech companies that have created this surveillance economy in the first place. Small businesses will always be at a disadvantage in a system where we're forced to compete with the resources of tech giants. By establishing strong baseline privacy protections for everyone, legislation like S.71 helps create an environment where businesses can compete on product quality and customer service rather than surveillance capabilities.

Benefits of S.71 for Small Businesses

The Vermont Data Privacy and Online Surveillance Act provides a thoughtful, phased implementation approach that acknowledges small business challenges and gives small businesses the runway to adapt better data practices.

The bill's provisions requiring data minimization, purpose limitation, and reasonable security measures align with best practices already followed by privacy-conscious small businesses. S.71 also tries to level the playing field by ensuring that all businesses operate with similar respect for consumer privacy.

However, while I appreciate the bill's phased implementation approach, I suggest that future iterations consider regulating based primarily on data type rather than organizational size or volume. Just as we require businesses handling hazardous materials to follow the same safety protocols regardless of how many customers they serve, those handling particularly sensitive personal data should adhere to consistent standards no matter their size. Certain categories of data are inherently high-risk and deserve uniform protection standards across all businesses that collect them.

For the individuals whose data is lost, stolen, sold, or abused, the impact on their lives doesn't change with an organization's size or number of customers. When it's *your* data, that's the only thing that matters. Data about a single person can cause a lot of damage in the wrong hands.

Conclusion

I applaud this body's balanced approach to protecting consumer privacy while accounting for the practical realities facing small businesses. By establishing clear standards, providing implementation support, and creating enforcement mechanisms focused primarily on larger entities, this legislation can help make the market conditions where privacy-respecting services become more widely available to businesses of all sizes.

No business earns brand value or customer loyalty by meeting the legal minimum standards, but you won't hear big platforms touting that fact. On the other hand, S.71 has the potential to create the foundation that allows Vermont businesses to compete on privacy as a differentiating value—something increasingly important to consumers. I strongly urge you to treat S.71 as an opportunity to realize a digital ecosystem where privacy is the default rather than the exception.

Respectfully,

Melanie Ensign

Founder & CEO, Discernible Inc.