Testimony Regarding Comprehensive Privacy Protections

Eric Null, Director, Privacy & Data Program
Center for Democracy & Technology
Washington, DC

Before the Vermont House Committee on
Commerce and Economic Development

Tuesday, April 28, 2026,
Hearing on S. 71 – An act relating to consumer
data privacy and online surveillance

Thank you for the invitation to speak remotely today as you are thinking through how to protect Vermonters' privacy. I commend your efforts at trying to protect privacy over the past several years, I know it's not been easy.

My name is Eric Null, I am the director of the privacy & data program at the Center for Democracy & Technology, a thirty-year-old nonpartisan, nonprofit organization based in Washington, DC, focusing on protecting individual rights, civil rights, and civil liberties in the digital age.

While I may have spent most of my legal career in Washington DC, I am a born-and-raised Vermonter. I grew up in Williston, and I did most of my schooling in Vermont, including graduating from the University of Vermont.

One thing I learned during that time is that Vermonters value their privacy and it's probably not a huge surprise that I adopted that value and grew up to fight for consumers' right to privacy as well. My experience was that people in Vermont generally keep to themselves. Much of the state is rural, where neighbors are few and far between, and people prefer to live on mountains and dirt roads rather than cities like Boston or New York. There is an ethos of privacy in the Green Mountain State, built into the fabric of everyday life. I remember when I first got internet access back in the early aughts, I used a fake name because while the vast world of the internet was cool and exciting, my family knew there were risks and unknowns, so we took actions to protect ourselves.

Almost thirty years later, we have basically the same expectations for individuals to protect their privacy online, but the scale of the internet today makes that impossible. The internet is orders of magnitude larger than 30 years ago. The tsunami of privacy-related information coming at people is overwhelming.

It would be quite fitting, as a result, for Vermont to be a national leader on privacy protections, by passing strong comprehensive privacy legislation.

Our goal for the internet should be for people to be able to go online, purchase the goods they want, access the services they want, talk to their friends and family, engage in research, educate themselves, and generally use the internet *without* worrying about the vast overcollection and

use of data about them from every corner of the internet. People should be able to trust that those online services are collecting only the data needed to provide the service, which then would reduce the potential harms they might experience from, for example, the sale of that data in the vast data brokerage market, or from inevitable data breaches, or from sensitive data being misused. Basically, we need to stop making protecting privacy a purely individual problem.

Unfortunately, what we have right now is the opposite. Today, most state comprehensive privacy laws have largely followed the federal approach, the failed notice-and-consent model, by merely requiring companies to disclose their purposes for processing data and consumers either accept those privacy policies or not. Rather than place affirmative obligations on online companies, these states continue to bless the industry practices that got us into the privacy mess of today.

This regime is based on the fiction that an individual somehow consents to any data processing so long as it is buried somewhere in a dense, legalistic privacy policy. We know people don't view privacy policies as particularly effective or useful.[1] We know people don't read privacy policies.[2] And we know that if people did try to read privacy policies, it would take them hundreds of hours per year.[3] As a result, people have a sense of futility and feel a lack of control over privacy risks, and they often underestimate the risks of disclosing data.[4]

Because of the notice-and-consent approach, Vermonters and consumers everywhere are bombarded with all kinds of so-called "choice architecture" built into the internet – cookie consent pop-ups, opt-out pop-ups, lengthy privacy policies and terms of service agreements, and toggles for various complicated or unexplained privacy practices.

---

[1] Sixty-one percent of adults consider privacy policies to be an ineffective way for companies to explain data practices, and almost seventy percent consider privacy policies to be just something to "get past." Colleen McClain *et al*, *How Americans View Data Privacy*, Pew Research Center (2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy.

[2] Fifty-six percent of American adults say they agree to privacy policies without reading them, compared to only eighteen percent who say they rarely or never agree without reading. *Id.*

[3] A 2008 study estimated that people would spend 244 hours per year, or forty minutes a day, reading privacy policies if they read all policies that apply to them. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society 540, 560 (2008), https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2013/02/Cranor_Formatted_Final1.pdf. Privacy policies have only gotten longer since. Ryan Amos *et al*, *Privacy Policies Over Time: Curation and Analysis of a Million-Document Dataset*, In Proceedings of the Web Conference (2021), https://arxiv.org/pdf/2008.09159.

[4] Wenjun Wang *et al.*, *An Exploration of the Influencing Factors of Privacy Fatigue Among Mobile Social Media Users From the Configuration Perspective*, Scientific Reports (2025), https://www.nature.com/articles/s41598-024-84646-z.

Worse, notice-and-choice is even less effective at protecting Vermonters given the emergence of dark patterns, which nudge people into sharing more data about themselves than they otherwise might. Many companies employ these dark patterns, like highlighting the "Accept All" button on a cookie consent pop-up, or nagging a person over and over again to share their data. Thus, even well-meaning and well-informed Vermonters may be tricked or goaded into sharing more data than they'd otherwise want.

Vermont should not follow suit. Such a permissive law would be a rotten deal for Vermonters, whose lives have moved more and more online. In a state that values its privacy, companies have a permanent seat inside everyone's home and smartphone, collecting all information about those Vermonters to be used for a variety of purposes beyond simply providing the service – everything from fraud detection and product development to targeting intrusive behavioral ads and, now, training of AI systems.

Artificial Intelligence is the new frontier in privacy policy, presenting many privacy issues like the mass repurposing of data for AI training and the sensitivity and depth of data collected via AI prompts. It also presents civil rights issues, as we know that AI systems can discriminate based on protected classes.

AI is yet another example of why Vermont should refuse to let companies continue setting their own rules. If companies must only disclose their practices to Vermonters, then they can just add "we collect and process data to train AI" to their policy, creating essentially a blank check to collect and retain indefinitely any data they want as that data can always be fed into an AI training dataset. A law purporting to protect privacy should not have such an easy workaround. I encourage you all to continue considering these and other AI protections including antidiscrimination provisions.

It's time to right these wrongs, and you can do that for Vermonters by refusing to maintain the status quo.

We should place the privacy burden on the companies that benefit most from the collection and exploitation of that data — meaning, it should be the company's responsibility to justify their data processing. To accomplish that, legislation should require companies to collect, use, and

disclose data *only* to the extent needed to provide the services that are requested by the individual. This is the real data minimization standard, as adopted in Maryland,[5] and as proposed throughout the country and at the federal level, and in today's bill.[6]

Contrary to their claims, companies can still create effective advertising systems with less data. Companies don't need behavioral data from years ago to target useful ads. Companies don't need your precise geolocation, within feet, to serve you a relevant restaurant ad in your town or city. In fact, behavioral data in general is a pretty poor proxy for interest in products, as we all use the internet for a variety of reasons, not just to signal our interest in being sold something. A regime that allows for higher quality data, and less data processing overall, would be better for companies and Vermonters.

I'd be remiss if I didn't say that privacy laws are only as strong as their enforcement, and they should be enforced through multiple channels. Companies don't comply with laws they don't think will be enforced, much like drivers violate speed limits when they don't think police are ahead to pull them over. The Vermont Attorney General should have rulemaking authority and civil penalty authority, plus additional funding, and individuals should have a private right of action. Physical and economic harm have long been recognized as a cognizable privacy harm, so a private right of action that covers at least actual damages and injunctive relief should be table stakes, and should be palatable to industry.

With reasonable limits in place, Vermonters may finally be able to realize the dream of enjoying the fruits of the internet without worrying about their privacy, because they will know there are strong laws protecting their data.

If you were hoping the United States Congress would solve this problem for you, I wouldn't hold your breath. Last week, House Energy & Commerce Republicans ignored years of bipartisan negotiations and introduced a partisan bill that would be a major step back for privacy

---

[5] Maryland Online Data Privacy Act, https://mgaleg.maryland.gov/2024RS/chapters_noln/Ch_454_hb0567E.pdf.
[6] American Data Privacy and Protection Act, https://www.congress.gov/bill/117th-congress/house-bill/8152/text; American Privacy Rights Act, https://www.congress.gov/bill/118th-congress/house-bill/8818/text. *See also* New Mexico's Community Privacy and Safety Act, SB 420, https://www.nmlegis.gov/Sessions/25%20Regular/bills/senate/SB0420.HTML, and Massachusetts' Consumer Data Privacy Act, H. 78, https://malegislature.gov/Bills/194/H78.

protections, while simultaneously preempting state laws that are stronger, and some that are much stronger. That is a non-starter for those of us who advocate on behalf of consumers.

Thank you again for inviting me to testify, and I look forward to answering any questions you may have.