May 6, 2026

Representative Michael Marcotte, Chair Representative Edye Graning, Vice Chair Vermont House Committee on Commerce and Economic Development

Testimony of Gaurav Laroia

Before the Vermont House Committee on Commerce and Economic Development

Regarding S.71 – An act relating to consumer data privacy and online surveillance

Chair Marcotte, Vice Chair Graning, and Members of the Committee:

Thank you for the opportunity to submit this testimony in strong support of S.71, particularly its substantive data minimization provisions.

My name is Gaurav Laroia and I've been a technology lawyer and advocate for over 10 years, and until about a year ago, I served as a consumer protection advisor to FTC Commissioner Becca Slaughter and was her point person on data and technology accountability issues.

Today, I want to share why her team at the FTC fought to turn the page on the outdated notice-and-consent framework that put untenable burdens on people and set the stage for the kinds of privacy violations your committee is working to address today.

During my time at the Commission we viewed these issues through the lens of unfairness, the abuse of data, and market power, rather than as just privacy abstractions. The data minimization provisions in S.71 - limiting "the collection and processing of personal data to what is reasonably necessary and proportionate" to providing the product or service they requested is the foundation of a fair exchange - the data companies actually need for the service people want. If enacted, Vermonters would have among the best digital protections in the nation - and more concretely, it means that the people of Vermont can use digital services knowing that they're not giving up more than what's fairly owed to the companies that mediate modern life.

Flawed Assumptions and Notice and Choice

Weakening this bill and abandoning these protections threatens to repeat the same mistake that has plagued federal data protection efforts for decades. Allowing companies to take the information they please for the purposes they please so long as they disclose it places an impossible burden on busy everyday people. It forces busy Vermonters to navigate endless privacy policies or complex opt-out mechanisms, rather than placing that obligation on the well-resourced company you've trusted with your data.

It's worth briefly understanding how we got here, and just how poorly the assumptions that held up notice based enforcement have fared in reality.[1] In the deregulatory fervor of the 1980s the

[1] For a comprehensive history of the Federal Trade Commission's privacy enforcement efforts, *see* Lina

agency took a hands-off approach to protecting people's information in the face of rapidly changing technology. Regulators made the assumption that consumers could take control of their personal data by educating themselves about privacy policies and making informed decisions in the free market.

Decades later we know this framework is broken. Privacy scholars have called these endless disclosures the "transparency paradox" As companies write longer policies to comply with the law the documents become incomprehensible to the average person. Recent studies show that the average privacy policy is almost 7,000 words long and it would take an average person a week to read the privacy policies of the websites they visit in a typical month.[2]

Digital services are the essential infrastructure for modern life. Faced with take-it-or-leave-it privacy policies any normal person will choose to participate in the economy. This failed idea led directly to the data ecosystem we know today: massive data breaches,[3] endless robocalls,[4] blockbuster fines for repeated FTC order violations,[5] and the creation of a massive, shadowy data broker industry.[6]

Towards Substantive Protections

During my tenure at the FTC advising Commissioner Slaughter we spent years sounding the

---

M. Khan, Samuel A.A. Levine & Stephanie T. Nguyen, *After Notice and Choice: Reinvigorating "Unfairness" to Rein In Data Abuses*, 77 Stan. L. Rev. 1375 (2025). The article details the paradigm shift in consumer protection at the Commission over the past half-decade, outlining the move away from failed disclosure-based regimes toward substantive limits on data abuses.

[2] *See generally* Josh Fuqua, *The Illusion of Consent: Rethinking Privacy Online*, GSU L. Rev. Blog (Apr. 10, 2025), https://www.gsulawreview.org/blog/the-illusion-of-consent-rethinking-privacy-online/ (arguing that the traditional notice-and-choice framework fails to protect consumers and that the burden of protection must shift to the data controllers). *see also* Irma Šlekytė, *NordVPN Study Shows: Nine Hours to Read the Privacy Policies of the 20 Most Visited Websites in the US*, NordVPN (Oct. 23, 2023), https://nordvpn.com/blog/privacy-policy-study-us/ [https://perma.cc/F432-TV7S] (finding that the average U.S. privacy policy is nearly 7,000 words, and calculating that reading the policies of the 96 websites an average person visits monthly would take 46.6 hours).

[3] *See* Lorenzo Franceschi-Bicchierai & Carly Page, *2024 in Data Breaches: 1 Billion Stolen Records and Rising*, TechCrunch (Oct. 14, 2024), https://techcrunch.com/2024/10/14/2024-in-data-breaches-1-billion-stolen-records-and-rising/.

[4] *See* Teresa Murray, *Ringing in Our Fears: 2025 Robocalls Hit 6-Year High*, U.S. PIRG Educ. Fund (2025), https://pirg.org/edfund/resources/ringing-in-our-fears-2025-robocalls-hit-6-year-high/.

[5] *See, e.g.*, Press Release, Fed. Trade Comm'n, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook (penalizing Facebook for violating a 2012 FTC privacy order); Press Release, Fed. Trade Comm'n, *FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads* (May 25, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads (imposing a $150 million penalty for violating a 2011 FTC order).

[6] *See generally Data Brokers*, Elec. Privacy Info. Ctr., https://epic.org/issues/consumer-privacy/data-brokers/ (last visited May 5, 2026).

alarm that this system was fundamentally broken. The FTC had relied on its Section 5 "deception" authority to make sure companies stayed true to their privacy policies, and little else. [7] It created a system where companies had the legal protection to gather, use, and sell as much of our information as possible so long as they admitted it in the fine print.

Using its limited authorities the FTC looked to the legal standard for "unfairness" to create data minimization orders with teeth. Under the FTC Act, a business practice is unfair if it meets three criteria: First, it causes substantial injury. Second, the injury cannot be reasonably avoided by consumers. And third, the harm is not outweighed by benefits to consumers or competition.[8]

When you look at the digital economy, the unfairness of rampant data collection outside the bounds of a reasonable commercial interaction is plain on its face. When there's little real competition among platforms, especially on privacy, and when digital services are required to function in modern society, consumers cannot reasonably avoid having their data extracted - leading to all the downstream harms we're here to address.

Using this authority the FTC found certain data practices harmful and unlawful, regardless of what a privacy policy may say. The agency took action against CafePress for holding onto consumer data indefinitely without a business need[9] and brought cases against companies like BetterHelp for taking sensitive mental health data to third party ad networks for targeted advertising.[10]

The agency also took aim at the data broker industry. In a series of cases against data brokers like Kochava, X-Mode, and InMarket, the agency found companies indiscriminately selling precise geolocation data that could track Americans to sensitive locations like reproductive health clinics and places of worship. By going after these data brokers the agency secured substantive bans on

---

[7] While the Commission historically relied almost exclusively on its "deception" authority to regulate data privacy and data collection, it is worth noting that the agency successfully pioneered the use of its "unfairness" authority earlier to combat lax data *security* procedures. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015) (affirming the FTC's authority to regulate corporate data security under the unfairness prong of Section 5 of the FTC Act); *see also* Press Release, Fed. Trade Comm'n, *Auto Dealer Software Provider Settles FTC Data Security Allegations* (June 12, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/06/auto-dealer-software-provider-settles-ftc-data-security-allegations (deploying unfairness authority against a service provider for failing to implement reasonable data security measures).

[8] 15 U.S.C. § 45(n)

[9] *See* Press Release, Fed. Trade Comm'n, *FTC Takes Action Against CafePress for Data Breach Cover Up and Lax Security* (Mar. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover-lax-security.

[10] *See* Press Release, Fed. Trade Comm'n, *FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising* (Mar. 2, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook.

the selling of sensitive location data.[11]

As Commissioner Slaughter frequently noted during my tenure, the only true way to protect consumers is to turn off the data pump. Data that is never collected cannot be breached by hackers, and it cannot be abused by data brokers.

But the FTC's Section 5 authority is a limited tool. The agency is forced to fight these battles case by case and company by company.

The fight for substantive privacy protections is in the hands of the states. Vermont has a historic opportunity to build on the foundation the FTC laid. You have the power to codify these substantive limits into statutory law and to heed the hard lessons of the FTC.

Two Paths

This isn't just a history lesson. Today, Vermont stands at a fork in the road. You can either mandate substantive limits on data collection, or you can fall back on the failed disclosure-based regime of the past.

To see the stark difference between these two paths, we only have to look at two FTC actions from the past few weeks.

First, the old paradigm: Last month, the FTC settled with Match Group, which runs the dating app OkCupid. The FTC found that the app took the profile pictures and exact locations of millions of users and handed them over to a completely unrelated AI startup. Why? Because OKCupid's founders were financial investors using their users' photos as a free data pipeline to boost their outside investments.[12]

---

[11] *See, e.g.*, Press Release, Fed. Trade Comm'n, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations* (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other; Press Release, Fed. Trade Comm'n, *FTC Order Will Ban Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data* (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-data-broker-x-mode-social-outlogic-selling-sensitive-location-data; Press Release, Fed. Trade Comm'n, *FTC Order Will Ban Data Broker InMarket from Selling Precise Consumer Location Data* (Jan. 18, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-data-broker-inmarket-selling-precise-consumer-location-data.

[12] *See* Press Release, Fed. Trade Comm'n, *FTC Takes Action Against Match and OkCupid for Deceiving Users by Sharing Personal Data with Third Party* (Mar. 30, 2026), https://www.ftc.gov/news-events/news/press-releases/2026/03/ftc-takes-action-against-match-okcupid-deceiving-users-sharing-personal-data-third-party; *see also* Abby Jackson, *OkCupid, Affiliate Match Gave Millions of Users' Photos to AI Facial Recognition Company, FTC Says*, Yahoo News (Apr. 6, 2026), https://www.yahoo.com/news/articles/okcupid-affiliate-match-gave-millions-053000984.html (detailing that the unauthorized data transfer was used to train facial recognition software for Clarifai, an AI startup

And what was the legal solution under the old, deceptive framework? Match was simply ordered not to misrepresent its privacy policies in the future. That means as long as they update the fine print, the extraction may continue. I cannot imagine that the average person thinks that when they use a dating site, the company is secretly feeding images of their face into a third-party facial recognition AI.

Now, look at the second path. Just two days ago, the FTC finalized a resolution against the data broker Kochava for selling the precise location data of millions of people. But instead of just demanding a better privacy policy, the FTC secured an order that places substantive limits on data collection and use. Kochava is now legally barred from selling that sensitive data unless it is used to provide a service directly requested by the consumer.[13]

I bring these up by way of example. Cases prosecuted under Vermont's privacy law will look different. But the core choice before this committee is the same.

Which regime would Vermonters like to live in? When a company abuses your data will it help to know that an explanation was hidden in a user agreement? Or do you want the law to ensure that companies simply do not collect or share what they do not need?"

Conclusion

As we enter the era of artificial intelligence, strict limits on data collection are essential. AI-powered inference means companies can now deduce highly intimate details about Vermonters from mundane, non-sensitive data. If AI systems can turn everyday data into a window into our private lives, procedural disclosures offer even less protection.[14]

Opponents of these provisions will likely say that substantive data minimization is untested or that it may break the internet. But, in truth, it may fix a broken market.

The digital economy incentivizes companies to extract the most personal information from people, instead of squarely providing value to them.

---

backed by OkCupid's founders).

[13] *See* Press Release, Fed. Trade Comm'n, *FTC to Ban Kochava and Subsidiary from Selling Sensitive Location Data to Settle Charges They Sold Location Data Linked to Millions of Mobile Devices* (May 4, 2026), https://www.ftc.gov/news-events/news/press-releases/2026/05/ftc-ban-kochava-subsidiary-selling-sensitive-location-data-settle-charges-they-sold-location-data.

[14] *See generally* Jennifer King & Caroline Meinhardt, *Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World*, Stanford Univ. Human-Centered Artificial Intelligence (Feb. 2024) (discussing how artificial intelligence's capacity to infer highly sensitive traits from non-sensitive, mundane data streams renders traditional, disclosure-based privacy frameworks obsolete and necessitates robust data-centric limits).

The FTC has already broken ground on substantive data protections, and in fits and starts is continuing the work. The federal government has shown the efficacy of this framework. Why would Vermont choose to go backwards?

I urge you to preserve the strong, substantive data minimization provisions in S.71. By doing so you'll ensure that Vermonters can participate in the modern economy safely and fairly. Thank you for your time and your leadership on this issue. I look forward to your questions.