Office of Racial Equity
Agency of Administration
Pavilion Office Building
109 State Street, 5th Floor
Montpelier, VT 05609-0201
racialequity.vermont.gov/

Xusana R. Davis, Executive Director

TO: Members of the House Committee on Commerce and Economic Development

FROM: Jeffrey Mbarushimana, Policy and Research Analyst

DATE: May 5, 2026

RE: Written Advocacy on S. 71 – An Act Relating to Consumer Data Privacy and Online Surveillance

The Vermont Office of Racial Equity (ORE) submits this written advocacy in support of S.71 and to offer equity analysis on four provisions that are central to the committee's upcoming markup: (1) the data minimization standard; (2) the private right of action; (3) the GLBA automotive finance exemption; and (4) the scope of sensitive data protections for immigration status, reproductive health, and gender-affirming health data. ORE does not take a position on every provision of S.71, but on those where the equity implications are direct and documented, ORE's mandate requires it to speak clearly.

S.71 and ORE's Equity Mandate

Consumer data is not collected, shared, and sold neutrally across race, immigration status, income, and identity. The Federal Trade Commission, peer-reviewed academic research, and two weeks of committee testimony have established that the commercial data ecosystem - data brokers, behavioral advertising networks, connected device manufacturers, and automotive telematics systems is actively being used to: identify and locate undocumented immigrants for federal enforcement; sell location data linked to abortion clinic visits to anti-abortion enforcement actors; enable insurance discrimination through covert behavioral profiling; facilitate intimate partner surveillance through connected vehicle systems; and build AI systems trained on sensitive personal data without consumer knowledge or consent. These are not theoretical risks. They are documented, ongoing, and disproportionately harming the communities ORE is mandated to serve.

ORE offers the following analysis on the four provisions most directly relevant to that mandate.

1. The Data Minimization Standard Should Be Retained

Draft 2.3's requirement that data collection be limited to what is "reasonably necessary and proportionate to provide the service requested" is the provision with the most direct and consequential equity relevance in S.71. It is also the provision under the most pressure from

industry witnesses. ORE urges the committee to retain it.

Vermont's immigrant communities - including the Somali, Nepali, Bosnian, Karen, and Spanish-speaking families in Chittenden County and across the state are directly threatened by the commercial surveillance infrastructure that data minimization constrains. An Immigration and Customs Enforcement Request for Information, read into the committee record during testimony, explicitly explored using commercial behavioral advertising data, data collected through the cross-site tracking infrastructure S.71's minimization standard is designed to limit - for immigration enforcement without consumer consent or judicial oversight.[1] Data minimization does not eliminate this threat entirely, but it materially limits the volume and granularity of commercial data available for warrantless government acquisition.

The notice-and-consent model that 21 other state privacy laws use has been documented as a complete failure by the Federal Trade Commission, by Consumer Reports, by EPIC, and by peer-reviewed academic research. A Carnegie Mellon study found that it would take 76 eight-hour workdays for a consumer to read every privacy policy they encounter in a single year[2] making informed consent structurally impossible for any consumer, let alone for consumers who face language barriers, digital literacy gaps, or limited time due to economic precarity. The notice-and-consent model fails disproportionately for the communities who can least afford its failure.

ORE recommends: Retain the data minimization standard in Draft 2.3. If the committee determines that the three sensitive data categories unique to Draft 2.3 - keystrokes and input monitoring, driving behavior, and cross-device online activity profiles require additional refinement, ORE supports addressing those categories specifically rather than removing the minimization standard as a whole.

2. The Private Right of Action Should Be Restored for Sensitive Data Violations

S.71's current draft removes the private right of action, the provision that allows an individual Vermonter harmed by a violation of this law to bring a direct claim in court. ORE urges the committee to restore it, at minimum for violations involving sensitive data categories.

The Attorney General of Vermont represents the state of Vermont, not individual Vermonters. A privacy violation that harms one person: a denial of insurance based on covertly collected driving behavior, a sharing of location data with a stalker, a disclosure of health information to an employer, a profile of immigration status sold to federal authorities without consent may not be large enough, or cost-efficient enough to recover, for the AG to pursue. Vermont has maintained a private right of action under the Consumer Protection Act since the 1960s. Every data-related bill this session - the genetic privacy bill (H.639), the kids code, the data broker bill (H.211) includes a private right of action. S.71 is the anomaly.

The concern about litigation incentives, frequently cited by industry witnesses, does not apply to Vermont's Consumer Protection Act model, which requires proof of actual harm. A

consumer who cannot demonstrate that they were actually harmed by a violation cannot recover. This is not a liquidated damages regime like Illinois's BIPA, which has \$1,000-\$5,000 per violation penalties that created the wave of class action litigation that industry appropriately fears. Vermont's CPA model requires harm, not just violation. The AG's own office confirmed in testimony that actual-harm PRA claims are not a litigation incentive, they are an access-to-justice provision for Vermonters the AG cannot represent.

ORE recommends: Restore a private right of action for violations involving sensitive data categories, consistent with the Consumer Protection Act framework Vermont has used for decades and with every other data bill this session. If a full PRA is not achievable in markup, ORE supports a targeted PRA limited to sensitive data violations, which addresses the highest-stakes harms while limiting the scope of litigation exposure the committee is concerned about.

3. The GLBA Entity-Level Exemption Should Not Apply to Automotive Finance and Insurance Data

S.71's current GLBA entity-level exemption creates a specific and documented loophole in the automotive sector that disproportionately harms low-income Vermonters and communities of color. ORE urges the committee to close it.

Vermont has approximately one vehicle per resident and Vermonters drive 20% more than the national average. Modern connected vehicles collect precise geolocation data, driving behavior, health inferences from location (medical center visits), religious affiliation inferences from location (church parking), and financial behavior and transfer that data to manufacturers, telematics companies, data brokers, and insurers, largely without consumer knowledge or consent. The nonprofit Mozilla Foundation rated connected vehicles as the worst product category for privacy they have ever reviewed, worse than dating apps and fertility trackers.

The GLBA entity-level exemption enables the following documented practice: an auto manufacturer collects a consumer's driving behavior daily through its connected vehicle platform. That data flows to the manufacturer's captive finance company - a bank - as an affiliate transfer, not classified as a "sale" under S.71. Once inside the finance company, the bill does not apply at all. The finance company now combines loan data, income, credit score, and daily driving behavior into a composite risk profile that affects loan approval, interest rates, and insurance premiums. The consumer never knew this was happening. The bill's sensitive data protections never applied.

This is not hypothetical. Insurance premiums have increased by as much as 80% after automakers shared driving behavior data with data brokers.[3] Driving data has been used to deny coverage entirely. Low-income consumers who are disproportionately communities of color have the least ability to absorb these premium increases and the least access to alternative transportation options. The fix is one sentence: automotive retailers, lenders, and insurers shall not qualify for the GLBA entity-level exemption for data collected from or about vehicles.

ORE recommends: Add a one-sentence carve-out specifying that automotive retailers, lenders, and insurers do not qualify for the GLBA entity-level exemption for data collected from or about vehicles. This targeted fix does not disrupt the bill's broader GLBA framework, it closes a specific and documented equity gap.

4. Immigration Status, Reproductive Health, and Gender-Affirming Health Data Protections Must Be Preserved

Draft 2.3 classifies immigration status, reproductive and sexual health data, and gender-affirming health data as sensitive data categories requiring opt-in consent and prohibiting sale. ORE urges the committee to preserve these categories in whatever version of S.71 advances from markup.

These are not hypothetical data risks. The FTC brought enforcement actions in 2024 against data brokers marketing location data revealing visits to abortion clinics and other medical centers, characterizing these sales as "a revealing business."[4] Data brokers have sold location data linked to reproductive healthcare visits to anti-abortion enforcement actors in states where abortion is criminalized. Vermont residents who travel to Vermont from states where abortion is illegal are exposed by this ecosystem today, without any state-law remedy. The immigration status data category directly protects Vermont's immigrant communities from the same commercial surveillance pipeline that federal immigration enforcement is actively seeking to access through data broker contracts.

ORE also endorses the ACLU of Vermont's recommendation that the committee align S.71's subpoena language with Vermont's 2025 reproductive healthcare shield law. Without this alignment, data collected under S.71's framework could potentially be accessed through the bill's subpoena provision in ways that the shield law was specifically designed to prevent. This is a targeted technical fix that does not require renegotiating any other provision of the bill.

ORE recommends: Preserve immigration status, reproductive and sexual health data, and gender-affirming health data as sensitive data categories in S.71's final version, regardless of which draft framework the committee adopts. Align the bill's subpoena language with Vermont's 2025 reproductive healthcare shield law as recommended by the ACLU of Vermont.

5. On the HIPAA Exemption: A Note

ORE is not opposed to addressing the legitimate compliance complexity concerns raised by Vermont's healthcare organizations. HIPAA is a comprehensive federal framework, and the committee has heard extensive, credible testimony about the operational challenges that the data-element approach in Draft 2.3 creates for healthcare entities whose data is inherently mixed - some PHI, some not across the same systems.

ORE's position is that the solution should be a data-element approach with clear operational guidance, rather than a full entity-level exemption. An entity-level exemption leaves ungoverned the websites, donor databases, appointment reminder systems, and chatbots of every healthcare

organization in Vermont - data that is not PHI, is not covered by HIPAA, and is directly relevant to the bill's protective purpose. Rep. Priestley's live website audit of a Vermont health organization demonstrated this gap precisely. ORE supports targeted language that addresses the irresolvable compliance conflicts created by the current data-element approach while preserving the bill's coverage of non-PHI data held by healthcare organizations.

Conclusion

S.71 represents Vermont's most significant opportunity this session to create state-law protections against a commercial surveillance infrastructure that is actively harming the communities ORE serves. ORE respectfully urges the committee to: retain the data minimization standard; restore a private right of action for sensitive data violations; close the GLBA automotive finance loophole; and preserve the sensitive data protections for immigration status, reproductive health, and gender-affirming health data. Each of these positions reflects not a preference but a documented pattern of harm that ORE's mandate requires it to name and address.

We thank the committee for the opportunity to submit this advocacy.

Citations

1. ICE Request for Information on Commercially Available Information (CAI) for Immigration Enforcement (2025). Cited in testimony of Katrina Fitzgerald, EPIC, before the House Committee on Commerce and Economic Development, April 28, 2026. Also documented in: Electronic Privacy Information Center (EPIC), Commercial Data Brokers and Immigration Enforcement (2024). Available at: https://epic.org.

2. McDonald, A.M. & Cranor, L.F. (2008). The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society, 4(3), 540–565. Carnegie Mellon University. The study found it would require 76 eight-hour workdays annually for a consumer to read every privacy policy encountered. Cited in testimony of Ryan Krueger, Deputy Chief, Massachusetts AG Privacy Division, before the House Committee on Commerce and Economic Development, April 29, 2026.

3. Testimony of Mary Marwig, Vice President, Privacy for Cars, before the House Committee on Commerce and Economic Development, May 1, 2026. Marwig cited documented cases in which auto insurers used telematics driving behavior data shared by manufacturers to increase premiums by up to 80% and deny coverage. Supporting documentation: Mozilla Foundation, *Privacy Not Included: Cars* (2023). Available at: https://foundation.mozilla.org/en/privacynotincluded/categories/cars/.

4. Federal Trade Commission (2024). FTC Takes Action Against Data Brokers for Selling Sensitive Location Data. FTC enforcement actions filed January 2024 against data brokers for selling precise geolocation data revealing visits to medical facilities including reproductive health clinics. Available at: https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-takes-action-against-data-broker. Cited in testimony of Falko Schilling, ACLU of Vermont, before the House Committee on Commerce and Economic Development, April 30, 2026.

* * *