Merry Marwig
VP Global Communications and Advocacy
Privacy4Cars
https://privacy4cars.com

01 May 2026

Chair Michael Marcotte
House Committee on Commerce and Economic Development
115 State Street
Montpelier, VT 06633

Subject: Written Testimony in Support of S.71, the Vermont Data Privacy and Online Surveillance Act

Dear Chair Marcotte and Members of the Committee,

Thank you for the opportunity to testify in support of S.71, the Vermont Data Privacy and Online Surveillance Act. My name is Merry Marwig. I am VP of Global Communications and Advocacy at Privacy4Cars, a world-leading authority on vehicle privacy and data security, and I have spent seven years working in data privacy and the last two in automotive privacy.

Let me start with a story that illustrates why this bill matters. A consumer named Michael Terrana requested the data that a data broker had on his driving behavior. The report showed that nearly every day around 5:30 p.m., there was a “near-miss collision, small object.” The explanation turned out to be simple: when he pulled into his driveway after work, his cats ran up to greet his car.[1] These excited cats became “near-miss collisions” in his dataset, a risk score that now follows Michael everywhere, and may have cost him hundreds of dollars in raised insurance rates.

For most Vermonters, a car is a necessity, not a convenience. Vermont has roughly one vehicle per resident[2], and Vermonters drive 20% more than the national average[3]. Cars play an enormous role in your constituents’ everyday lives.

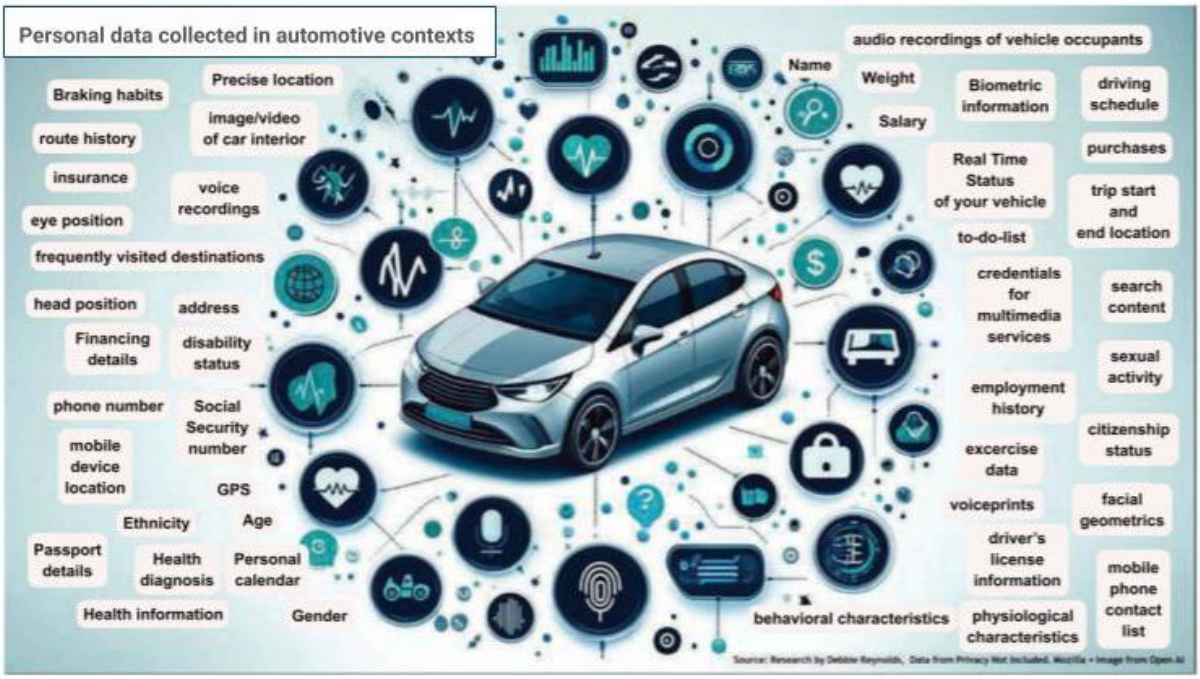
And yet, cars today are among the most data-intensive consumer products on the market. The concept that vehicles are mainly mechanical things—four wheels and a seat—is outdated.

---

[1] "Car Insurers Found a New Way to Rip You Off," YouTube, September 23, 2025, at 1:03. Available at: https://youtu.be/X6UW4CFz71s?t=63
[2] https://www.healthvermont.gov/stats/data-reporting-topic/population-data and https://vermontvehicle.org/
[3] https://vermontbiz.com/news/2016/january/28/vermonters-drive-20-percent-more-us-average-are-seeking-out-alternatives

Electronics and software represent approximately 40% of the cost of manufacturing a vehicle today, expected to surpass 50% by 2030.[4] The nonprofit Mozilla Foundation rated automobiles as the worst product category for privacy they have ever reviewed, worse than dating apps and worse than fertility trackers.[5]

The reality is that a multitude of players in the automotive ecosystem can collect, share, sell, buy, and use highly sensitive personal data: manufacturers, third-party service providers, telematics companies, finance companies, data brokers, and insurance companies. And we are not just talking about braking habits and route history. We are talking about frequently visited destinations, driving schedules, search content, health diagnoses, exercise data, even citizenship status and ethnicity.[6]



Source: Image by Debbie "The Data Diva" Reynolds, originally prepared for the IoT Board of Advisors, a federal initiative under the auspices of the US Department of Commerce and the National Institute of Standards and Technologies, 2024.

[4]Deloitte, "Automotive Electronics Cost as a Percentage of Total Car Cost Worldwide from 1970 to 2030," April 2019, via Statista. See also McKinsey & Company, "Mapping the Automotive Software and Electronics Landscape Through 2030," January 2023.

[5]Mozilla Foundation, "It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy," Privacy Not Included, September 6, 2023. Available at: https://www.mozillafoundation.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

[6]Infographic: "Personal Data Collected in Automotive Contexts," prepared by Debbie Reynolds for the IoT Board of Advisors, U.S. Department of Commerce / National Institute of Standards and Technology (NIST).

And what are the harms that can stem from this data? A multitude that include but are not limited to:

Financial harms:

- *Insurance premium increases* - One driver's premium jumped 80% after an automaker shared hundreds of entries of their driving data with a data broker.[7]
- *Insurance denial or cancellation* -- Another driver claimed the data sharing significantly impacted his ability to find automobile insurance coverage at all, and that when he finally did find it, his rate nearly doubled.[8]
- *Inaccurate risk scoring* -- A driver complained their driving data in the report is "so decontextualized that it can hardly be called accurate."[9] Again, think of the cat story from above.

Privacy violations:

- *Undisclosed surveillance*
- *Loss of control over personal data* – When consumers request the reports data brokers compile about them, many consumers are alarmed to discover the extensive files documenting granular details of their driving history, data they had no idea was being collected, recorded, or shared.
- *Enrollment without meaningful consent*
- *Data persistence in resold vehicles* -- Over 80% of used vehicles sold today have prior drivers and passengers' personal data still stored on the car.[10]

Physical Safety harms:

- *Abuse and stalking* -- Abusive people have tracked a vehicle's real-time location, viewed footage from interior and exterior cameras, and in some cases controlled the vehicle remotely such as honking the horn in the early morning hours, or cranking the heat to dangerous levels in the middle of summer. One survivor of abuse said, "My ex would unlock my car's trunk at 3:49 AM, forcing me to get out of bed to secure my vehicle. I lived in constant fear of what he might do next through the car app."

Identity Theft and Data Breach Exposure - this is a great example of why data minimization (similar to Maryland's) is so important:

---

[7] https://gmauthority.com/blog/2026/01/ftc-says-gm-and-onstar-were-watching-and-selling-your-every-move/
[8] https://natlawreview.com/article/ftc-makes-statement-automaker-faces-class-action
[9] https://www.carcomplaints.com/news/2025/gm-onstar-class-action-lawsuit.shtml
[10] Privacy4cars.com/CISO

- *Mass data breaches* impacting millions of people
- *Extractable digital identities* from cars as devices
- *Lifetime risk* - The data collected in car contexts represent some of the most intimate data of our lives, especially the location data.

Inferential Harms and Discrimination

- *Sensitive life information derived from location data* - Your religious beliefs, sexual orientation, health information, and more.
- *Relationship and lifestyle inferences* -- who you may spend time with based on where your car is parked.
- *Law enforcement access without warrants*
- *National security exposure* - Data brokers have sold members of military's location data to foreign and adversarial governments.

Systemic/Market harms:

- *Deceptive user experience patterns* – in 2025, the California Privacy Protection Agency took enforcement action against an automaker for deceptive design patterns that inhibited consumer's ability to exercise their privacy rights.
- And very importantly — *Asymmetric power* – Consumers have little or no control over their personal data in car contexts today. You can't buy a modern car that doesn't collect data. Consent mechanisms are opaque, privacy choices are limited, and without a private right of action, consumers have no practical way to push back. And without a private right of action, that lack of power – that asymmetric power – is cemented.

So, when we think about this Act, we need to think about connected cars as one of the most intimate surveillance devices consumers engage with today, one they are paying for not only with money, but also, unbeknownst to many, with their personal data.

Your Act covers online surveillance, and it is important to understand that people access the internet increasingly not just through web browsers on computers, but through IoT devices. I recommend including in your universal opt-out mechanism language, a "System for Recognizing Universal Opt-Out Mechanisms" similar to Colorado's formal review process (Colorado Code of Regulations: 4 CCR 904-3-5.07.). I say this because the current widely adopted universal opt-out mechanism, Global Privacy Control (GPC), only works in browser-based settings, not when consumers access the internet with an IoT device. There is a Universal Opt Out Mechanism that exists today that works for IoT devices including vehicles, smartphones, laptops, tablets,

routers, the apps that run on them[11]. A formal review process can help ensure Opt Out Mechanisms stay current with the way Vermont consumers access the internet.

Cars are one of the largest, most expensive IoT devices a Vermonter will ever own. Geolocation data — one of the most invasive data types — shows where you are, where you live, where you work, who you might be with, places you go like medical visits, religious institutions, political or union activities. Should these highly sensitive details of our lives be sold? This Act says no. And I commend you for that.

I strongly support this Act. Its sensitive data definitions, its prohibition on selling geolocation data, its requirement in § 2415d(a)(5) that controllers name the specific entities they have sold data to. These are real protections.

That is important because today, many major car brands face legal action over personal data practices: class actions, consumer arbitrations, state Attorney General investigations, and as of January 2025, an FTC consent order banning an automaker from collecting and disclosing driving data to consumer reporting agencies for five years.[12] The common thread: consumers did not know what personal data of theirs was being collected, companies did not clearly disclose what they were doing, and their position was that there were not clear laws telling them they had to. That is exactly why what you are doing here matters.

In addition to supporting the bill, I want to flag three automotive-specific gaps that could undermine these protections, and offer simple fixes for each:

> **First,** the absence of vehicle-specific disclosures at the right time in the vehicle lifecycle.
>
> **Second,** an entity-level GLBA exemption that lets auto finance and insurance companies sidestep the bill entirely.
>
> **Third,** franchise relationships that create hidden, unregulated data pipelines.

Automotive-Specific Gap 1: Vehicle Lifecycle — Disclosure and Consent Concerns

The Problem: *The bill requires notice but does not address multi-controller transactions, like vehicle sales involving manufacturers, dealers, lenders, and third-party service providers, and does not specify when that notice is required.*

Part of the problem today is that consumers are not being properly informed. Privacy notices are buried in paperwork, written in legalese, and voluminous. A 2024-model car I examined had twelve different documents explaining its data practices. Reading them all would take an

---

[11] https://practicalprivacy.wyrick.com/blog/shortlisted-the-colorado-attorney-general-identifies-three-potential-universal-opt-out-mechanisms-for-upcoming-cpa-opt-out-requirement

[12] Federal Trade Commission, "FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent," Press Release, January 16, 2025. Order finalized January 14, 2026.

average reader approximately five and a half hours, approximately the same time a fast reader could get through George Orwell's *1984*. Which feels appropriate.

Example of the reading level and reading time

UNIQUE DOCUMENTS **12**	WORDS **66,144**	READ TIME** **329 min**
Main Privacy Policy Last Updated: 9/25/2024	5,321 Reading Level: 17th Grade***	27 min
Main TOS Last Updated: Undated	2,808 Reading Level: 15th Grade***	14 min
Vehicle Owners Privacy Policy Same As Main Privacy Policy	Same Reading Level: Same	Same
Vehicle Owners TOS Same As Main TOS	Same Reading Level: Same	Same
Connected Services/Telematics Privacy Policy Last Updated: 9/25/2024	3,475 Reading Level: 18th Grade***	17 min
Connected Services/Telematics TOS Last Updated: 05/01/2018	12,669 Reading Level: 15th Grade***	63 min
Sirius XM: Main Privacy Policy Last Updated: 6/30/2023	10,996 Reading Level: 12th Grade***	55 min
Sirius XM: Main TOS Last Updated: 1/19/2018	3,843 Reading Level: 11th Grade***	19 min
Android Auto: Main Privacy Policy Last Updated: 10/4/2023	9,362 Reading Level: 8th Grade***	47 min
Android Auto: Main TOS Last Updated: 1/5/2022	3,492 Reading Level: 11th Grade***	17 min
Apple Carplay: Main Privacy Policy Last Updated: 12/22/2022	4,069 Reading Level: 13th Grade***	20 min
Apple Carplay: Main TOS Last Updated: 11/20/2009	3,404 Reading Level: 15th Grade***	17 min
Amazon Alexa: Main Privacy Policy Last Updated: 8/11/2023	3,634 Reading Level: 11th Grade***	18 min
Amazon Alexa: Main TOS Last Updated: 9/14/2022	3,071 Reading Level: 12th Grade***	15 min

* Estimate based on public disclosures made in the Privacy Policy (PP) and Terms Of Service (TOS) of the vehicle's OEM (Original Equipment Manufacturer) and third party service providers. For full disclosure and information go to the links provided.

** Average time to read entire document(s) at 200 words per minute.

*** Flesch–Kincaid Grade Level (FKGL): a readability test designed to indicate how difficult a passage in English is to understand. It is comparable to the proficiency an average student has to achieve at that grade of education in the United States. The lower the number, the easier it is to comprehend a text. In the USA, several States require by law that auto insurance documents have a FKGL of 9th grade or below (14-15 years old).

13

Vermont law already requires every traditional new vehicle purchase to go through a franchised dealer. The dealer is not optional; it is legally mandated by Vermont state law. So does it not

[13] Privacy notice volume analysis of a 2024-model connected vehicle, illustrating twelve separate privacy documents and estimated reading time, screenshot taken from VehiclePrivacyReport.com.

make sense that a consumer receives a vehicle-specific privacy disclosure prior to and at that point of transaction, before they commit to a purchase? This would let consumers comparison shop on data practices, perhaps choosing a brand that collects less personal data or does not sell or share it. California already has a "Notice at Collection" regulation (Cal. Code Regs. Tit. 11, § 7012) that includes automotive examples as a model.[14]

The disclosure needs to be prominent and simple. At minimum, consumers should quickly understand: whether sensitive data will be collected (geolocation, biometrics, data from their smartphone); whether the vehicle can transmit data through its own cellular connection (telematics); and the third-parties the manufacturer shares data with, such as affiliates including their captive lender and dealers, data brokers, and insurers.

The timing of this disclosure is critical. Cars are expensive, difficult purchases to back out of. If a consumer discovers after purchase that the manufacturer's data practices are misaligned with their privacy preferences and personal security risk tolerance, the remedy is impractical. One cannot easily just buy a new car. Requiring consumers to go online or call the manufacturer ahead of a purchase to get this information would create excessive burden, make transactions at dealerships even more time-consuming, and be outright ineffective. The notice needs to be prior to and at the point of transaction.

Then after purchase, the consumer should receive a plain-language notice informing them of what rights they have under Vermont law and what choices they can make about the data their vehicle collects, stores, sells, and shares.

Timing also matters when vehicles change hands. When a consumer trades in a vehicle, returns a lease, returns a rental, or a vehicle is repossessed, companies should have a duty to protect the personal data stored on that vehicle. Today, over 80% of pre-owned or pre-used vehicles for sale still contain the prior drivers and passengers unencrypted personal data: contacts, call logs, navigation history, garage door codes, saved passwords, and more.[15] Other states have already acted. Illinois requires repossession agencies to delete personal information from vehicles upon repossession.[16] New Jersey requires motor vehicle dealers to offer to delete a consumer's personal information when taking possession of a vehicle for resale or lease.[17] Many companies are already voluntarily deleting personal data from vehicles when they change

[14]Cal. Code Regs. Tit. 11, § 7012 — Notice at Collection of Personal Information. See subsections (g)(1)–(2) and illustrative examples regarding vehicles and car rental businesses.

[15]Privacy4Cars research and analysis. See also Andrea Amico, "Why Auto Financiers Must Address Vehicle Data Privacy Now," Non Prime Times, December 2023.

[16]Illinois Senate Bill SB800 (Public Act 103-0501), amending the Collateral Recovery Act, effective January 1, 2024. Requires licensed repossession agencies to delete personal information stored in vehicles upon repossession.

[17]New Jersey Assembly Bill A4723 (P.L. 2023, c.314), signed January 16, 2024. Requires motor vehicle dealers to offer to delete a consumer's personal information from the vehicle's computer system when taking possession for resale or lease.

hands, because it is the right thing to do. We believe it makes sense to extend those pragmatic, simple protections to all Vermont residents through your law.

Recommended Fix: *Require plain-language, vehicle-specific privacy disclosures before and at point of sale, after purchase, and at every change of vehicle possession. Require companies to protect and delete personal data when they take possession of a vehicle.*

Automotive-Specific Gap 2: The GLBA Exemption Gap

The Problem: *The bill's entity-level GLBA exemption creates unintended consequences in automotive contexts. Auto dealers, auto lenders, and auto insurers can all claim this exemption. That is a loophole so large you could drive all of Vermont's cars and trucks through it.*

Let me illustrate how this works. Suppose Michael finances his car through the manufacturer's captive finance company, which is a bank, fully exempt under this bill as written (see § 2415c(a)(14)). The manufacturer collects Michael's driving data every day through the connected vehicle platform: where he drives, how hard he brakes, how fast he accelerates, and more.

That driving data flows from the manufacturer to the finance company without being classified as a sale under this bill, because they are affiliates under the same corporate parent. Once inside the finance company, the bill does not apply.

So now the finance company has Michael's loan application information, his income, credit score, Social Security number, *and now his daily driving behavior*. It blends them. Late payments plus hard braking plus low income equals a "high-risk driver/borrower" score. That score could affect his next loan approval, his interest rate, or trigger an early review of his current loan. Did Michael ever know about this use of his data? No. Did he consent to it? No.

This is the same data the bill rightly classifies as sensitive in other contexts. The data did not change. The harm did not change. Only the legal classification changed. And some captive finance companies have already written into their privacy policies that they reserve the right to use vehicle data for repossession. This is not theoretical; it is currently common practice.

Now consider auto insurance: 100% of Vermont drivers must carry auto insurance. It is a mandatory product. And under the current language, we are allowing auto insurers to collect and use whatever vehicle data they want because they are GLBA-exempt. Remember Michael's cats? That data practice would be perfectly permissible under this bill as written.

Recommended Fix: *A one-sentence addition to the statute: automotive retailers, automotive lenders, and automotive insurers do not qualify for the entity-level GLBA exemption for data collected from or about vehicles.*

Automotive-Specific Gap 3: The Franchise Coercion Problem

The Problem: *Franchised dealers operate under contracts dictated by auto manufacturers. Those agreements increasingly mandate that dealers use the manufacturer's dealer management systems, enroll customers in connected services, sync customer data upstream, and transmit deal data to manufacturer platforms. The dealer cannot refuse without risking critical items to their business including vehicle allocation, incentives, or the franchise itself.*

If the dealer is exempt or falls below this Act's applicability thresholds, the franchise agreement becomes an unregulated data pipeline. The manufacturer extracts consumer data through the dealer without triggering any Vermont disclosure or consent obligation. The consumer never knows. This also puts local Vermont dealers in an impossible position; they are contractually compelled to participate in data practices they may not even fully understand, and that may violate your state's law.

Recommended Fix: *One sentence: a franchise agreement may not require a dealer to collect, process, or disclose personal data in a manner that violates this Act. That makes manufacturer data mandates that conflict with Vermont law unenforceable. And it protects local dealers, too. It de-risks them from being forced into practices that would violate your law.*

Closing

This bill is strong. The sensitive data definitions and the sale prohibition are real protections. But the automotive ecosystem exposes three gaps:

1. Consumers are not meaningfully informed before the point of sale, after sale, or when vehicles change hands.
2. The GLBA entity-level exemption lets auto finance captives and insurers ingest sensitive vehicle data without oversight.
3. Franchise relationships let manufacturers extract data through dealers without accountability.

The good news is that the fixes are simple. Three additions, each requiring just one sentence of statutory language:

1. Require vehicle-specific disclosures throughout the lifecycle of the vehicle.
2. Close the GLBA entity-level exemption for automotive data.
3. Bar franchise agreements from overriding this Act.

These are pragmatic fixes – including the formal review process of Universal Opt Out Mechanisms mentioned earlier - that close real gaps without reworking the structure of your bill.

Sincerely,

Merry Marwig

Merry Marwig
VP Global Communications & Advocacy
Privacy4Cars
merry@privacy4cars.com
https://privacy4cars.com