HOUSE OF REPRESENTATIVES
2 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0002
(207) 287-1400
TTY: MAINE RELAY 711

Tiffany Roberts
35 Buttonwood Road
South Berwick, ME 03908
Home: (207) 210-3287
Tiffany.Roberts@legislature.maine.gov

April 10, 2025

Testimony of Rep. Tiffany Roberts presenting

LD 1227, An Act to Repeal the Requirement That Motor Vehicle Manufacturers Equip Vehicles with a Standardized Data Access Platform

Before the Joint Standing Committee on Housing and Economic Development

Good afternoon, Senator Curry, Representative Gere, and esteemed members of the Joint Standing Committee on Housing and Economic Development. I am Tiffany Roberts, and I represent House District 149, which includes parts of North and South Berwick. I am pleased to be here today to present **LD 1227, An Act to Repeal the Requirement That Motor Vehicle Manufacturers Equip Vehicles with a Standardized Data Access Platform**.

Thank you for the opportunity to present testimony for LD 1227, a narrowly focused bill to repeal Section 1810 subsection 6 of the Right to Repair law passed via ballot initiative in 2023. This section mandates a mobile-based, interoperable platform giving unrestricted access to vehicle-generated data, a provision that now threatens consumer privacy, vehicle cybersecurity, and Maine's compliance with federal law. I respectfully ask this committee to support the repeal itself and the emergency clause because the stakes are not theoretical. They are immediate and profound.

Let's be clear about what's at stake: This subsection is already being challenged in federal court, and the lawsuit identifies it as unconstitutional and impossible to comply with.

This is not what voters were told they were voting for. They were not told that the law could expose their personal data, including location, driving behavior, and usage patterns, to unlicensed third parties. They were not told that their taxpayer dollars would be used to defend a lawsuit against the State over this very provision.

Let's begin with how this law section has been portrayed to the public. A radio ad across Maine celebrated this moment immediately after Subsection 6 was enacted in early January. It said:

"Guess what? Thanks to voters like you all across the state, we finally got the right to repair our vehicles where we choose... The right to repair means you finally get access to your repair data

from your vehicle so you can fix it where you want. And if Big Auto tries their old tricks and doesn't give you access to your car's data, guess what? The new law says they owe you $10,000."

This ad, paid for by the Maine Right to Repair Committee, directs consumers to contact the Attorney General to enforce penalties. Even though, as the pending lawsuit makes clear, the access platform required under Subsection 6 does not exist, and no 'independent entity' has been established to securely administer this access, as required under Subsection 2 of the same statute. And when I say I access, I mean access to our data.

In January, the Alliance for Automotive Innovation filed suit in federal court, asserting that Subsection 6 of the Data Law is unenforceable because it violates due process and is preempted by the federal Vehicle Safety Act. Their complaint calls out Subsection 6 specifically as 'unconstitutionally vague' and 'impossible to comply with,' noting that no standardized platform exists, and no cybersecurity framework has been put in place to protect against remote tampering with critical vehicle systems such as braking or steering. Further, the Bureau of Industry and Security and the National Highway Traffic Safety Administration (NHTSA) have warned that open telematics access introduces risks of remote hijacking and systemic failure.

The complaint states plainly that:
"Subsection 6 requires vehicle manufacturers to use a standardized access platform that does not exist, administered by an independent entity that has not been designated, to provide secure access to all telematics data. Because it is impossible for manufacturers to comply, enforcement would deprive them of due process."

The lawsuit also argues that this provision poses a conflict with federal safety law, saying:
"A failure to maintain adequate cybersecurity controls would give rise to a safety-related defect," which could trigger federal recalls under the Vehicle Safety Act.

The very language at the heart of the pending lawsuit centers on Subsection 6. We have opened a door with no lock and no guard on the other side.

To be frank, many of us in this room saw this coming. Some chose not to believe it. This is one of those rare times when I don't like being right.

But here we are.

So I ask you plainly: Is this what people voted for?

We spend hours in this building debating how to protect consumer data in a digital world, yet because of this law, sensitive location, behavioral, and diagnostic data from connected vehicles can be accessed without vetting, consent, or regulation. We have no statewide privacy law, no regulation on who can access this data, no oversight of what can be done with it, and now, a legal mandate to make it accessible.

The 2023 Citizen's Voter Guide did not explain that Subsection 6 would allow real-time remote access to data streams that include GPS, speed, diagnostic codes, and potentially biometric information. This data must also be bi-directional, or in plain terms, send information to and from your vehicle.

Let me repeat: an unauthorized, unregulated business or person with unrestricted access to you and your vehicle's data to take data from and send data to.

Voters were not told that no standards or rules exist in Maine to govern who can access this data, how it can be stored, or what happens when it's misused, if anything.

This is a case where the ballot initiative process got ahead of the policy reality.

Some will say this repeal guts the intent of Question 4. I disagree.

The Government Accountability Office (GAO), the Federal Trade Commission (FTC), and the industry's own MOU all confirm that independent shops already have access to the same diagnostic data as dealers. The industry already complies with a national Memorandum of Understanding on repair access. This repeal targets the unrestricted, mobile-based data stream, not the ability to change your brakes or fix your transmission.

Some will say this is about manufacturer control. I would offer it's about consumer protection.

Should we wait for the courts? But while we wait, this law is in effect, and the Attorney General has issued guidance requiring dealerships to disclose the mobile access requirement to consumers starting January 5, 2025.

We must also address a central myth: this access is urgently needed for vehicle repairs. The so-called 'repair data' at the center of this law includes far more than diagnostics. It includes behavioral and location data that no mechanic needs to replace a water pump or perform a brake job.

Six of eight automakers interviewed said they do not provide dealerships with telematics data, and the two that do, provide a similar level of access to independent repair shops. Even the federal GAO and NHTSA confirm that today's diagnostics don't require telematics.

If this is about preparing for future tools, then there's no harm in waiting until it can be done safely.

Another misconception or false narrative is that there is no issue because the Massachusetts law has been ruled on. As I stated before, the law passed in Massachusetts is not the same as ours, starting with the supposed "entity" that oversees this section.

We may also hear today that there haven't been any breaches, which is the point. We can't wait until someone's brakes fail because of compromised firmware. The cybersecurity risks are well-documented and very real.

This narrow repeal does not undo the voters' will; your Right to Repair stays intact. It removes the legally flawed and risky access provision.

I added the emergency clause to LD 1227 because every day this law stays in effect without basic safeguards exposes Mainers to real cybersecurity risks. The Bureau of Industry and Security at the U.S. Department of Commerce recently proposed rules highlighting how connected vehicles can be exploited to exfiltrate sensitive data or enable remote manipulation by

foreign adversaries. It's not hard to see how Maine's law falls squarely into that danger zone by requiring real-time, direct data access with no security framework.

This is not a repeal of the right to repair. It is a repeal of a dangerous and misleading provision that was never ready for implementation. Every day, this section stays in law, creating legal exposure for the State of Maine and real vulnerability for our citizens' personal information. We are already spending taxpayer dollars defending a law we knew, or should have known, would not survive federal scrutiny.

Section 1810(6) is a legal and cybersecurity liability. This will cost Maine time, money, and credibility. Regardless of our decisions on the entire law, we must deal with this one reckless section.

Let's press pause on unregulated access before we press our luck with data privacy, safety, and federal law.

We have a choice: we can take corrective action now, or we can let an unworkable, unsecure, and legally vulnerable policy remain on the books and hope the courts bail us out. I believe it's our job to fix it.

Let's protect consumers, uphold cybersecurity best practices, and ensure that what we pass into law is enforceable, defensible, and grounded in reality.

Thank you for your time and attention. I am happy to take questions.